

# *ZyWALL 2Plus*

*Internet Security Appliance*

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

Version 4.00

5/2006

Edition 1

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Zy" is in a smaller font size than "XEL", and the "X" is significantly larger and more prominent.



# Copyright

Copyright © 2006 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.

# Certifications

## 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.

### Viewing Certifications

- 1 Go to <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.

## Registration

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.

# 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) 333 8250	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
		+48 (22) 333 8251		
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 Arte, 21 5ª planta 28033 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>3</b>
<b>Certifications</b> .....	<b>4</b>
<b>Safety Warnings</b> .....	<b>6</b>
<b>ZyXEL Limited Warranty</b> .....	<b>7</b>
<b>Customer Support</b> .....	<b>8</b>
<b>Table of Contents</b> .....	<b>11</b>
<b>List of Figures</b> .....	<b>27</b>
<b>List of Tables</b> .....	<b>37</b>
<b>Preface</b> .....	<b>43</b>
<b>Chapter 1</b>	
<b>Getting to Know Your ZyWALL</b> .....	<b>45</b>
1.1 ZyWALL Internet Security Appliance Overview .....	45
1.2 Physical Features .....	45
1.2.1 Non-Physical Features .....	46
1.3 Applications for the ZyWALL .....	50
1.3.1 Secure Broadband Internet Access via Cable or DSL Modem .....	50
1.3.2 VPN Application .....	51
1.3.3 Front Panel Lights .....	52
<b>Chapter 2</b>	
<b>Introducing the Web Configurator</b> .....	<b>53</b>
2.1 Web Configurator Overview .....	53
2.2 Accessing the ZyWALL Web Configurator .....	53
2.3 Resetting the ZyWALL .....	54
2.3.1 Procedure To Use The Reset Button .....	55
2.3.2 Uploading a Configuration File Via Console Port .....	55
2.4 Navigating the ZyWALL Web Configurator .....	55
2.4.1 Router Mode .....	56
2.4.2 Bridge Mode .....	58
2.4.3 Navigation Panel .....	61
2.4.4 System Statistics.....	64
2.4.5 DHCP Table Screen .....	65

2.4.6 VPN Status .....	66
<b>Chapter 3</b>	
<b>Wizard Setup .....</b>	<b>69</b>
3.1 Wizard Setup Overview .....	69
3.2 Internet Access .....	69
3.2.1 ISP Parameters .....	69
3.2.1.1 Ethernet .....	69
3.2.1.2 PPPoE Encapsulation .....	71
3.2.1.3 PPTP Encapsulation .....	72
3.2.2 Internet Access Wizard: Second Screen .....	74
3.2.3 Internet Access Wizard: Registration.....	75
3.3 VPN Wizard Gateway Setting .....	78
3.4 VPN Wizard Network Setting .....	80
3.5 VPN Wizard IKE Tunnel Setting (IKE Phase 1) .....	82
3.6 VPN Wizard IPSec Setting (IKE Phase 2) .....	83
3.7 VPN Wizard Status Summary .....	84
3.8 VPN Wizard Setup Complete .....	87
<b>Chapter 4</b>	
<b>Registration .....</b>	<b>89</b>
4.1 myZyXEL.com overview .....	89
4.1.1 Content Filtering Subscription Service .....	89
4.2 Registration .....	89
4.3 Service .....	91
<b>Chapter 5</b>	
<b>LAN Screens .....</b>	<b>93</b>
5.1 LAN, WAN and the ZyWALL .....	93
5.2 IP Address and Subnet Mask .....	93
5.2.1 Private IP Addresses .....	94
5.3 DHCP .....	95
5.3.1 IP Pool Setup .....	95
5.4 RIP Setup .....	95
5.5 Multicast .....	95
5.6 WINS .....	96
5.7 LAN .....	96
5.8 LAN Static DHCP .....	98
5.9 LAN IP Alias .....	100
<b>Chapter 6</b>	
<b>Bridge Screens .....</b>	<b>103</b>
6.1 Bridge .....	103

6.1.1 Bridge Loop .....	103
6.2 Spanning Tree Protocol (STP) .....	104
6.2.1 Rapid STP .....	104
6.2.2 STP Terminology .....	104
6.2.3 How STP Works .....	105
6.2.4 STP Port States .....	105
6.3 Configuring Bridge .....	105
<b>Chapter 7</b>	
<b>WAN Screens .....</b>	<b>109</b>
7.1 WAN Overview .....	109
7.2 TCP/IP Priority (Metric) .....	109
7.3 WAN Route .....	109
7.4 WAN IP Address Assignment .....	111
7.5 DNS Server Address Assignment .....	111
7.6 WAN MAC Address .....	112
7.7 WAN .....	112
7.7.1 WAN Ethernet Encapsulation .....	112
7.7.2 PPPoE Encapsulation .....	115
7.7.3 PPTP Encapsulation .....	119
7.8 Traffic Redirect .....	122
7.9 Configuring Traffic Redirect .....	122
7.10 Configuring Dial Backup .....	123
7.11 Advanced Modem Setup .....	127
7.11.1 AT Command Strings .....	127
7.11.2 DTR Signal .....	127
7.11.3 Response Strings .....	127
7.12 Configuring Advanced Modem Setup .....	127
<b>Chapter 8</b>	
<b>Firewall Screens .....</b>	<b>131</b>
8.1 Firewall Overview .....	131
8.2 Firewall Connection Directions .....	132
8.3 Security Considerations .....	133
8.4 Firewall Rules Example .....	133
8.5 Firewall Default Rule (Router Mode) .....	135
8.6 Firewall Default Rule (Bridge Mode) .....	136
8.7 Firewall Rule Summary .....	138
8.7.1 Firewall Edit Rule .....	139
8.8 Anti-Probing .....	142
8.9 Denial of Service Attacks .....	143
8.10 Firewall Thresholds .....	144
8.10.1 Threshold Values .....	144

8.11 Threshold Screen .....	145
8.12 Service .....	146
8.12.1 Firewall Edit Custom Service .....	148
8.13 Solving the Asymmetrical Route Problem Example .....	149
8.14 My Service Firewall Rule Example .....	150

## **Chapter 9**

### **Content Filtering Screens ..... 155**

9.1 Content Filtering Overview .....	155
9.1.1 Restrict Web Features .....	155
9.1.2 Create a Filter List .....	155
9.1.3 Customize Web Site Access .....	155
9.2 Content Filter General .....	155
9.3 Category Based Content Filtering .....	157
9.4 Content Filter Categories .....	158
9.5 Content Filter Customization .....	165
9.6 Customizing Keyword Blocking URL Checking .....	167
9.6.1 Domain Name or IP Address URL Checking .....	167
9.6.2 Full Path URL Checking .....	167
9.6.3 File Name URL Checking .....	167
9.7 Content Filtering Cache .....	168

## **Chapter 10**

### **Content Filtering Reports ..... 171**

10.1 Checking Content Filtering Activation .....	171
10.2 Viewing Content Filtering Reports .....	171
10.3 Web Site Submission .....	176

## **Chapter 11**

### **IPSec VPN ..... 179**

11.1 IPSec VPN Overview .....	179
11.1.1 IKE SA .....	180
11.1.1.1 ZyWALL and Remote IPSec Router .....	183
11.1.1.2 IKE SA Proposal .....	183
11.1.1.3 Authentication Key and Extended Authentication (X-Auth) .....	183
11.1.2 IPSec SAs Using IKE SAs .....	185
11.1.2.1 IPSec SA Proposal .....	185
11.1.2.2 Local and Remote Network .....	186
11.1.2.3 IPSec SA Properties .....	186
11.1.3 IPSec SA Using Manual Keys .....	186
11.1.4 Additional IPSec VPN Topics .....	187
11.1.4.1 Active Protocols, Encryption Algorithms, and Authentication Algorithms .....	187

11.1.4.2 Encapsulation .....	189
11.1.4.3 VPN, NAT, and NAT Traversal .....	190
11.1.4.4 SA Life Time .....	191
11.1.4.5 IPSec High Availability .....	191
11.2 VPN Rules (IKE) .....	192
11.3 VPN Rules (IKE) Gateway Policy Edit .....	194
11.4 VPN Rules (IKE): Network Policy Edit .....	200
11.5 VPN Rules (IKE): Network Policy Move .....	204
11.6 VPN Rules (Manual) .....	205
11.7 VPN Rules (Manual): Edit .....	207
11.8 VPN SA Monitor .....	210
11.9 VPN Global Setting .....	211
11.10 Telecommuter VPN/IPSec Examples .....	213
11.10.1 Telecommuters Sharing One VPN Rule Example .....	213
11.10.2 Telecommuters Using Unique VPN Rules Example .....	214
11.11 VPN and Remote Management .....	215
<b>Chapter 12</b>	
<b>Certificates.....</b>	<b>217</b>
12.1 Certificates Overview .....	217
12.1.1 Advantages of Certificates .....	218
12.2 Self-signed Certificates .....	218
12.3 Configuration Summary .....	218
12.4 My Certificates .....	219
12.5 My Certificate Import .....	221
12.5.1 Certificate File Formats .....	221
12.6 My Certificate Create .....	222
12.7 My Certificate Details .....	224
12.8 Trusted CAs .....	227
12.9 Trusted CA Import .....	229
12.10 Trusted CA Details .....	230
12.11 Trusted Remote Hosts .....	232
12.12 Verifying a Trusted Remote Host's Certificate .....	234
12.12.1 Trusted Remote Host Certificate Fingerprints .....	234
12.13 Trusted Remote Hosts Import .....	235
12.14 Trusted Remote Host Certificate Details .....	236
12.15 Directory Servers .....	239
12.16 Directory Server Add or Edit .....	240
<b>Chapter 13</b>	
<b>Authentication Server.....</b>	<b>243</b>
13.1 Authentication Server Overview .....	243
13.2 Local User Database .....	243

13.3 RADIUS .....	243
13.3.1 Types of RADIUS Messages .....	244
13.4 Local User Database .....	244
13.5 RADIUS .....	246
<b>Chapter 14</b>	
<b>Network Address Translation (NAT) .....</b>	<b>249</b>
14.1 NAT Overview .....	249
14.1.1 NAT Definitions .....	249
14.1.2 What NAT Does .....	250
14.1.3 How NAT Works .....	250
14.1.4 NAT Application .....	251
14.1.5 Port Restricted Cone NAT .....	252
14.1.6 NAT Mapping Types .....	252
14.2 Using NAT .....	253
14.2.1 SUA (Single User Account) Versus NAT .....	253
14.3 NAT Overview .....	254
14.4 NAT Address Mapping .....	255
14.4.1 NAT Address Mapping Edit .....	256
14.5 Port Forwarding .....	258
14.5.1 Default Server IP Address .....	258
14.5.2 Port Forwarding: Services and Port Numbers .....	258
14.5.3 Configuring Servers Behind Port Forwarding (Example) .....	258
14.5.4 Port Translation .....	259
14.6 Port Forwarding Screen .....	260
14.7 Port Forwarding WAN to LAN HTTP Rule Example .....	261
14.8 Port Triggering .....	262
<b>Chapter 15</b>	
<b>Static Route .....</b>	<b>265</b>
15.1 IP Static Route .....	265
15.2 IP Static Route Screen .....	265
15.2.1 IP Static Route Edit .....	266
<b>Chapter 16</b>	
<b>Bandwidth Management .....</b>	<b>269</b>
16.1 Bandwidth Management Overview .....	269
16.2 Bandwidth Classes and Filters .....	269
16.3 Proportional Bandwidth Allocation .....	270
16.4 Application-based Bandwidth Management .....	270
16.5 Subnet-based Bandwidth Management .....	270
16.6 Application and Subnet-based Bandwidth Management .....	271
16.7 Scheduler .....	271



16.7.1 Priority-based Scheduler .....	271
16.7.2 Fairness-based Scheduler .....	271
16.7.3 Maximize Bandwidth Usage .....	271
16.7.4 Reserving Bandwidth for Non-Bandwidth Class Traffic .....	272
16.7.5 Maximize Bandwidth Usage Example .....	272
16.7.5.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth	273
16.7.5.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth ...	273
16.8 Bandwidth Borrowing .....	274
16.8.1 Bandwidth Borrowing Example .....	274
16.9 Maximize Bandwidth Usage With Bandwidth Borrowing .....	275
16.10 Configuring Summary .....	275
16.11 Configuring Class Setup .....	277
16.11.1 Bandwidth Manager Class Configuration .....	278
16.11.2 Bandwidth Management Statistics .....	281
16.12 Configuring Monitor .....	282
<b>Chapter 17</b>	
<b>DNS.....</b>	<b>285</b>
17.1 DNS Overview .....	285
17.2 DNS Server Address Assignment .....	285
17.3 DNS Servers .....	285
17.4 Address Record .....	286
17.4.1 DNS Wildcard .....	286
17.5 Name Server Record .....	286
17.5.1 Private DNS Server .....	286
17.6 System Screen .....	287
17.6.1 Adding an Address Record .....	288
17.6.2 Inserting a Name Server record .....	289
17.7 DNS Cache .....	291
17.8 Configure DNS Cache .....	291
17.9 Configuring DNS DHCP .....	292
17.10 Dynamic DNS .....	294
17.10.1 DYNDNS Wildcard .....	294
17.10.2 High Availability .....	294
17.11 Configuring Dynamic DNS .....	294
<b>Chapter 18</b>	
<b>Remote Management.....</b>	<b>297</b>
18.1 Remote Management Overview .....	297
18.1.1 Remote Management Limitations .....	297
18.1.2 System Timeout .....	298
18.2 Introduction to HTTPS .....	298

18.3 WWW .....	299
18.4 HTTPS Example .....	300
18.4.1 Internet Explorer Warning Messages .....	301
18.4.2 Netscape Navigator Warning Messages .....	301
18.4.3 Avoiding the Browser Warning Messages .....	302
18.4.4 Login Screen .....	303
18.5 SSH .....	306
18.6 How SSH Works .....	306
18.7 SSH Implementation on the ZyWALL .....	307
18.7.1 Requirements for Using SSH .....	307
18.8 Configuring SSH .....	307
18.9 Secure Telnet Using SSH Examples .....	308
18.9.1 Example 1: Microsoft Windows .....	308
18.9.2 Example 2: Linux .....	309
18.10 Secure FTP Using SSH Example .....	310
18.11 Telnet .....	311
18.12 Configuring TELNET .....	311
18.13 FTP .....	312
18.14 SNMP .....	313
18.14.1 Supported MIBs .....	315
18.14.2 SNMP Traps .....	315
18.14.3 REMOTE MANAGEMENT: SNMP .....	315
18.15 DNS .....	317
18.16 Introducing Vantage CNM .....	317
18.17 Configuring CNM .....	318
<b>Chapter 19</b>	
<b>UPnP.....</b>	<b>321</b>
19.1 Universal Plug and Play Overview .....	321
19.1.1 How Do I Know If I'm Using UPnP? .....	321
19.1.2 NAT Traversal .....	321
19.1.3 Cautions with UPnP .....	321
19.1.4 UPnP and ZyXEL .....	322
19.2 Configuring UPnP .....	322
19.3 Displaying UPnP Port Mapping .....	323
19.4 Installing UPnP in Windows Example .....	324
19.4.1 Installing UPnP in Windows Me .....	325
19.4.2 Installing UPnP in Windows XP .....	326
19.5 Using UPnP in Windows XP Example .....	326
19.5.1 Auto-discover Your UPnP-enabled Network Device .....	327
19.5.2 Web Configurator Easy Access .....	328

<b>Chapter 20</b>	
<b>ALG Screen.....</b>	<b>333</b>
20.1 ALG Introduction .....	333
20.1.1 ALG and NAT .....	333
20.1.2 ALG and the Firewall .....	333
20.2 FTP .....	334
20.3 H.323 .....	334
20.4 RTP .....	334
20.4.1 H.323 ALG Details .....	334
20.5 SIP .....	335
20.5.1 STUN .....	335
20.5.2 SIP ALG Details .....	335
20.5.3 SIP Signaling Session Timeout .....	336
20.5.4 SIP Audio Session Timeout .....	336
20.6 ALG Screen .....	336
<b>Chapter 21</b>	
<b>Logs Screens.....</b>	<b>339</b>
21.1 Configuring View Log .....	339
21.2 Log Description Example .....	340
21.2.1 Certificate Not Trusted Log Note .....	341
21.3 Configuring Log Settings .....	342
21.4 Configuring Reports .....	345
21.4.1 Viewing Web Site Hits .....	347
21.4.2 Viewing Protocol/Port .....	347
21.4.3 Viewing Host IP Address .....	348
21.4.4 Reports Specifications .....	349
<b>Chapter 22</b>	
<b>Maintenance .....</b>	<b>351</b>
22.1 Maintenance Overview .....	351
22.2 General Setup .....	351
22.2.1 General Setup and System Name .....	351
22.2.2 General Setup .....	351
22.3 Configuring Password .....	352
22.4 Time and Date .....	353
22.5 Pre-defined NTP Time Servers List .....	356
22.5.1 Resetting the Time .....	356
22.5.2 Time Server Synchronization .....	356
22.6 Introduction To Transparent Bridging .....	358
22.7 Transparent Firewalls .....	358
22.8 Configuring Device Mode (Router) .....	359
22.9 Configuring Device Mode (Bridge) .....	360

22.10 F/W Upload Screen .....	361
22.11 Backup and Restore .....	363
22.11.1 Backup Configuration .....	364
22.11.2 Restore Configuration .....	364
22.11.3 Back to Factory Defaults .....	366
22.12 Restart Screen .....	366
<b>Chapter 23</b>	
<b>Introducing the SMT .....</b>	<b>367</b>
23.1 Introduction to the SMT .....	367
23.2 Accessing the SMT via the Console Port .....	367
23.2.1 Initial Screen .....	367
23.2.2 Entering the Password .....	368
23.3 Navigating the SMT Interface .....	368
23.3.1 Main Menu .....	369
23.3.2 SMT Menus Overview .....	371
23.4 Changing the System Password .....	373
23.5 Resetting the ZyWALL .....	374
<b>Chapter 24</b>	
<b>SMT Menu 1 - General Setup.....</b>	<b>375</b>
24.1 Introduction to General Setup .....	375
24.2 Configuring General Setup .....	375
24.2.1 Configuring Dynamic DNS .....	377
24.2.1.1 Editing DDNS Host .....	377
<b>Chapter 25</b>	
<b>WAN and Dial Backup Setup.....</b>	<b>381</b>
25.1 Introduction to WAN and Dial Backup Setup .....	381
25.2 WAN Setup .....	381
25.3 Dial Backup .....	382
25.4 Configuring Dial Backup in Menu 2 .....	382
25.5 Advanced WAN Setup .....	383
25.6 Remote Node Profile (Backup ISP) .....	385
25.7 Editing PPP Options .....	387
25.8 Editing TCP/IP Options .....	388
25.9 Editing Login Script .....	390
25.10 Remote Node Filter .....	391
<b>Chapter 26</b>	
<b>LAN Setup.....</b>	<b>393</b>
26.1 Introduction to LAN Setup .....	393
26.2 Accessing the LAN Menus .....	393

26.3 LAN Port Filter Setup .....	393
26.4 TCP/IP and DHCP Ethernet Setup Menu .....	394
26.4.1 IP Alias Setup .....	397
<b>Chapter 27</b>	
<b>Internet Access .....</b>	<b>399</b>
27.1 Introduction to Internet Access Setup .....	399
27.2 Ethernet Encapsulation .....	399
27.3 Configuring the PPTP Client .....	401
27.4 Configuring the PPPoE Client .....	401
27.5 Basic Setup Complete .....	402
<b>Chapter 28</b>	
<b>Remote Node Setup .....</b>	<b>403</b>
28.1 Introduction to Remote Node Setup .....	403
28.2 Remote Node Setup .....	403
28.3 Remote Node Profile Setup .....	403
28.3.1 Ethernet Encapsulation .....	404
28.3.2 PPPoE Encapsulation .....	405
28.3.2.1 Outgoing Authentication Protocol .....	406
28.3.2.2 Nailed-Up Connection .....	406
28.3.2.3 Metric .....	407
28.3.3 PPTP Encapsulation .....	407
28.4 Edit IP .....	408
28.5 Remote Node Filter .....	410
28.6 Traffic Redirect .....	411
<b>Chapter 29</b>	
<b>IP Static Route Setup .....</b>	<b>413</b>
29.1 IP Static Route Setup .....	413
<b>Chapter 30</b>	
<b>Network Address Translation (NAT) .....</b>	<b>415</b>
30.1 Using NAT .....	415
30.1.1 SUA (Single User Account) Versus NAT .....	415
30.1.2 Applying NAT .....	415
30.2 NAT Setup .....	417
30.2.1 Address Mapping Sets .....	417
30.2.1.1 SUA Address Mapping Set .....	418
30.2.1.2 User-Defined Address Mapping Sets .....	419
30.2.1.3 Ordering Your Rules .....	420
30.3 Configuring a Server Behind NAT .....	422
30.4 General NAT Examples .....	424

30.4.1 Internet Access Only .....	424
30.4.2 Example 2: Internet Access with a Default Server .....	426
30.4.3 Example 3: Multiple Public IP Addresses With Inside Servers .....	426
30.4.4 Example 4: NAT Unfriendly Application Programs .....	430
30.5 Trigger Port Forwarding .....	432
30.5.1 Two Points To Remember About Trigger Ports .....	432
<b>Chapter 31</b>	
<b>Introducing the ZyWALL Firewall .....</b>	<b>435</b>
31.1 Accessing the Firewall Settings .....	435
31.2 Firewall SMT Menus .....	435
31.2.1 Activating the Firewall .....	435
<b>Chapter 32</b>	
<b>Filter Configuration .....</b>	<b>437</b>
32.1 Introduction to Filters .....	437
32.1.1 The Filter Structure of the ZyWALL .....	438
32.2 Packet Filtering Versus Firewall .....	440
32.2.1 Packet Filtering .....	440
32.2.1.1 When To Use Filtering .....	440
32.2.2 Firewall .....	440
32.2.2.1 When To Use The Firewall .....	441
32.3 Configuring a Filter Set .....	441
32.3.1 Configuring a Filter Rule .....	443
32.3.2 Configuring a TCP/IP Filter Rule .....	443
32.3.3 Configuring a Generic Filter Rule .....	446
32.4 Example Filter .....	448
32.5 Filter Types and NAT .....	450
32.6 Firewall Versus Filters .....	451
32.7 Applying a Filter .....	451
32.7.1 Applying LAN Filters .....	451
32.7.2 Applying Remote Node Filters .....	452
<b>Chapter 33</b>	
<b>SNMP Configuration .....</b>	<b>453</b>
33.1 SNMP Configuration .....	453
33.2 SNMP Traps .....	454
<b>Chapter 34</b>	
<b>System Information &amp; Diagnosis .....</b>	<b>455</b>
34.1 Introduction to System Status .....	455
34.2 System Status .....	455
34.3 System Information and Console Port Speed .....	457

34.3.1 System Information .....	457
34.3.2 Console Port Speed .....	458
34.4 Log and Trace .....	459
34.4.1 Viewing Error Log .....	459
34.4.2 Syslog Logging .....	460
34.4.3 Call-Triggering Packet .....	463
34.5 Diagnostic .....	463
34.5.1 WAN DHCP .....	464
<b>Chapter 35</b>	
<b>Firmware and Configuration File Maintenance .....</b>	<b>467</b>
35.1 Introduction .....	467
35.2 Filename Conventions .....	467
35.3 Backup Configuration .....	468
35.3.1 Backup Configuration .....	468
35.3.2 Using the FTP Command from the Command Line .....	469
35.3.3 Example of FTP Commands from the Command Line .....	470
35.3.4 GUI-based FTP Clients .....	470
35.3.5 File Maintenance Over WAN .....	470
35.3.6 Backup Configuration Using TFTP .....	471
35.3.7 TFTP Command Example .....	471
35.3.8 GUI-based TFTP Clients .....	472
35.3.9 Backup Via Console Port .....	472
35.4 Restore Configuration .....	473
35.4.1 Restore Using FTP .....	473
35.4.2 Restore Using FTP Session Example .....	475
35.4.3 Restore Via Console Port .....	475
35.5 Uploading Firmware and Configuration Files .....	476
35.5.1 Firmware File Upload .....	476
35.5.2 Configuration File Upload .....	477
35.5.3 FTP File Upload Command from the DOS Prompt Example .....	478
35.5.4 FTP Session Example of Firmware File Upload .....	478
35.5.5 TFTP File Upload .....	478
35.5.6 TFTP Upload Command Example .....	479
35.5.7 Uploading Via Console Port .....	479
35.5.8 Uploading Firmware File Via Console Port .....	479
35.5.9 Example Xmodem Firmware Upload Using HyperTerminal .....	480
35.5.10 Uploading Configuration File Via Console Port .....	480
35.5.11 Example Xmodem Configuration Upload Using HyperTerminal .....	481
<b>Chapter 36</b>	
<b>System Maintenance Menus 8 to 10 .....</b>	<b>483</b>
36.1 Command Interpreter Mode .....	483

36.1.1 Command Syntax .....	483
36.1.2 Command Usage .....	484
36.2 Call Control Support .....	485
36.2.1 Budget Management .....	485
36.2.2 Call History .....	486
36.3 Time and Date Setting .....	487
<b>Chapter 37</b>	
<b>Remote Management .....</b>	<b>491</b>
37.1 Remote Management .....	491
37.1.1 Remote Management Limitations .....	493
<b>Chapter 38</b>	
<b>Call Scheduling .....</b>	<b>495</b>
38.1 Introduction to Call Scheduling .....	495
<b>Chapter 39</b>	
<b>Troubleshooting .....</b>	<b>499</b>
39.1 Problems Starting Up the ZyWALL .....	499
39.2 Problems with the LAN Interface .....	499
39.3 Problems with the WAN Interface .....	500
39.4 Problems Accessing the ZyWALL .....	500
39.4.1 Pop-up Windows, JavaScripts and Java Permissions .....	501
39.4.1.1 Internet Explorer Pop-up Blockers .....	501
39.4.1.2 JavaScripts .....	504
39.4.1.3 Java Permissions .....	506
39.5 Packet Flow .....	508
<b>Appendix A</b>	
<b>Product Specifications .....</b>	<b>509</b>
<b>Appendix B</b>	
<b>Wall-mounting Instructions.....</b>	<b>515</b>
<b>Appendix C</b>	
<b>Setting up Your Computer's IP Address.....</b>	<b>517</b>
<b>Appendix D</b>	
<b>IP Subnetting.....</b>	<b>533</b>
<b>Appendix E</b>	
<b>Common Services.....</b>	<b>541</b>
<b>Appendix F</b>	
<b>VPN Setup.....</b>	<b>545</b>



---

<b>Appendix G</b>	
<b>Importing Certificates .....</b>	<b>557</b>
<b>Appendix H</b>	
<b>Command Interpreter.....</b>	<b>569</b>
<b>Appendix I</b>	
<b>Firewall Commands .....</b>	<b>571</b>
<b>Appendix J</b>	
<b>NetBIOS Filter Commands .....</b>	<b>577</b>
<b>Appendix K</b>	
<b>Certificates Commands .....</b>	<b>579</b>
<b>Appendix L</b>	
<b>Brute-Force Password Guessing Protection.....</b>	<b>583</b>
<b>Appendix M</b>	
<b>Boot Commands .....</b>	<b>585</b>
<b>Appendix N</b>	
<b>Log Descriptions.....</b>	<b>587</b>
<b>Index.....</b>	<b>607</b>



# List of Figures

Figure 1 Secure Internet Access via Cable, DSL or Wireless Modem .....	51
Figure 2 VPN Application .....	51
Figure 3 Front Panel .....	52
Figure 4 Change Password Screen .....	54
Figure 5 Replace Certificate Screen .....	54
Figure 6 Example Xmodem Upload .....	55
Figure 7 Web Configurator HOME Screen in Router Mode .....	56
Figure 8 Web Configurator HOME Screen in Bridge Mode .....	59
Figure 9 Home: Show Statistics .....	64
Figure 10 Home: DHCP Table .....	66
Figure 11 Home: VPN Status .....	67
Figure 12 ISP Parameters: Ethernet Encapsulation .....	70
Figure 13 ISP Parameters: PPPoE Encapsulation .....	71
Figure 14 ISP Parameters: PPTP Encapsulation .....	73
Figure 15 Internet Access Wizard: Second Screen .....	74
Figure 16 Internet Access Setup Complete .....	75
Figure 17 Internet Access Wizard: Registration .....	75
Figure 18 Internet Access Wizard: Registration in Progress .....	76
Figure 19 Internet Access Wizard: Status .....	77
Figure 20 Internet Access Wizard: Registration Failed .....	77
Figure 21 Internet Access Wizard: Registered Device .....	77
Figure 22 Internet Access Wizard: Activated Services .....	78
Figure 23 Gateway and Network Policies .....	78
Figure 24 IPSec Fields Summary .....	79
Figure 25 VPN Wizard: Gateway Setting .....	79
Figure 26 VPN Wizard: Network Setting .....	80
Figure 27 VPN Wizard: IKE Tunnel Setting .....	82
Figure 28 VPN Wizard: IPSec Setting .....	83
Figure 29 VPN Wizard: VPN Status .....	85
Figure 30 VPN Wizard Setup Complete .....	87
Figure 31 Registration .....	90
Figure 32 Registration: Registered Device .....	91
Figure 33 Registration: Service .....	92
Figure 34 LAN and WAN .....	93
Figure 35 LAN .....	97
Figure 36 LAN Static DHCP .....	99
Figure 37 Physical Network & Partitioned Logical Networks .....	100
Figure 38 LAN IP Alias .....	100

Figure 39 Bridge Loop: Bridge Connected to Wired LAN .....	103
Figure 40 Bridge .....	106
Figure 41 WAN Route .....	110
Figure 42 WAN: Ethernet Encapsulation .....	113
Figure 43 WAN: PPPoE Encapsulation .....	116
Figure 44 WAN: PPTP Encapsulation .....	119
Figure 45 Traffic Redirect WAN Setup .....	122
Figure 46 Traffic Redirect LAN Setup .....	122
Figure 47 Traffic Redirect .....	123
Figure 48 Dial Backup .....	124
Figure 49 Advanced Setup .....	128
Figure 50 Default Firewall Action .....	131
Figure 51 Blocking All LAN to WAN IRC Traffic Example .....	133
Figure 52 Limited LAN to WAN IRC Traffic Example .....	134
Figure 53 Default Rule (Router Mode) .....	135
Figure 54 Default Rule (Bridge Mode) .....	137
Figure 55 Rule Summary .....	138
Figure 56 Firewall Edit Rule .....	140
Figure 57 Anti-Probing .....	142
Figure 58 ZyWALL Firewall Application .....	143
Figure 59 Three-Way Handshake .....	144
Figure 60 Firewall Threshold .....	145
Figure 61 Firewall Service .....	147
Figure 62 Firewall Edit Custom Service .....	148
Figure 63 IP Alias .....	149
Figure 64 My Service Firewall Rule Example: Service .....	150
Figure 65 My Service Firewall Rule Example: Edit Custom Service .....	150
Figure 66 My Service Firewall Rule Example: Rule Summary .....	151
Figure 67 My Service Firewall Rule Example: Rule Edit .....	151
Figure 68 My Service Firewall Rule Example: Rule Configuration .....	152
Figure 69 My Service Firewall Rule Example: Rule Summary .....	153
Figure 70 Content Filter: General .....	156
Figure 71 Content Filtering Lookup Procedure .....	158
Figure 72 Content Filter: Categories .....	159
Figure 73 Content Filter: Customization .....	165
Figure 74 Content Filter: Cache .....	168
Figure 75 myZyXEL.com: Login .....	172
Figure 76 myZyXEL.com: Welcome .....	172
Figure 77 myZyXEL.com: Service Management .....	173
Figure 78 Blue Coat: Login .....	173
Figure 79 Content Filtering Reports Main Screen .....	174
Figure 80 Blue Coat: Report Home .....	174
Figure 81 Global Report Screen Example .....	175

Figure 82 Requested URLs Example .....	176
Figure 83 Web Page Review Process Screen .....	177
Figure 84 VPN: High-Level Example .....	179
Figure 85 VPN: IKE SA and IPSec SA .....	180
Figure 86 IKE SA: Main Negotiation Mode .....	181
Figure 87 IKE SA: Aggressive Negotiation Mode .....	182
Figure 88 VPN Example: NAT Traversal .....	190
Figure 89 IPSec High Availability .....	192
Figure 90 Gateway and Network Policies .....	192
Figure 91 IPSec Fields Summary .....	193
Figure 92 VPN Rules (IKE) .....	193
Figure 93 VPN Rules (IKE): Gateway Policy: Edit .....	195
Figure 94 VPN Rules (IKE): Network Policy Edit .....	201
Figure 95 VPN Rules (IKE): Network Policy Move .....	205
Figure 96 VPN Rules (Manual) .....	206
Figure 97 VPN Rules (Manual): Edit .....	208
Figure 98 VPN: SA Monitor .....	211
Figure 99 VPN: Global Setting .....	212
Figure 100 Telecommuters Sharing One VPN Rule Example .....	213
Figure 101 Telecommuters Using Unique VPN Rules Example .....	214
Figure 102 VPN for Remote Management Example .....	216
Figure 103 Certificate Configuration Overview .....	218
Figure 104 My Certificates .....	219
Figure 105 My Certificate Import .....	221
Figure 106 My Certificate Create .....	222
Figure 107 My Certificate Details .....	225
Figure 108 Trusted CAs .....	228
Figure 109 Trusted CA Import .....	229
Figure 110 Trusted CA Details .....	230
Figure 111 Trusted Remote Hosts .....	233
Figure 112 Remote Host Certificates .....	234
Figure 113 Certificate Details .....	235
Figure 114 Trusted Remote Host Import .....	236
Figure 115 Trusted Remote Host Details .....	237
Figure 116 Directory Servers .....	239
Figure 117 Directory Server Add .....	240
Figure 118 Local User Database .....	245
Figure 119 RADIUS .....	246
Figure 120 How NAT Works .....	250
Figure 121 NAT Application With IP Alias .....	251
Figure 122 Port Restricted Cone NAT Example .....	252
Figure 123 NAT Overview .....	254
Figure 124 NAT Address Mapping .....	255

Figure 125 NAT Address Mapping Edit .....	257
Figure 126 Multiple Servers Behind NAT Example .....	259
Figure 127 Port Translation Example .....	259
Figure 128 Port Forwarding .....	260
Figure 129 Port Forwarding .....	262
Figure 130 Trigger Port Forwarding Process: Example .....	263
Figure 131 Port Triggering .....	264
Figure 132 Example of Static Routing Topology .....	265
Figure 133 IP Static Route .....	266
Figure 134 IP Static Route Edit .....	267
Figure 135 Subnet-based Bandwidth Management Example .....	270
Figure 136 Bandwidth Management: Summary .....	276
Figure 137 Bandwidth Management: Class Setup .....	277
Figure 138 Bandwidth Management: Edit Class .....	279
Figure 139 Bandwidth Management: Statistics .....	281
Figure 140 Bandwidth Management: Monitor .....	282
Figure 141 Private DNS Server Example .....	287
Figure 142 System DNS .....	287
Figure 143 System DNS: Add Address Record .....	289
Figure 144 System DNS: Insert Name Server Record .....	290
Figure 145 DNS Cache .....	291
Figure 146 DNS DHCP .....	293
Figure 147 DDNS .....	295
Figure 148 HTTPS Implementation .....	299
Figure 149 WWW .....	299
Figure 150 Security Alert Dialog Box (Internet Explorer) .....	301
Figure 151 Security Certificate 1 (Netscape) .....	302
Figure 152 Security Certificate 2 (Netscape) .....	302
Figure 153 Login Screen (Internet Explorer) .....	303
Figure 154 Login Screen (Netscape) .....	304
Figure 155 Replace Certificate .....	304
Figure 156 Device-specific Certificate .....	305
Figure 157 Common ZyWALL Certificate .....	305
Figure 158 SSH Communication Example .....	306
Figure 159 SSH .....	308
Figure 160 SSH Example 1: Store Host Key .....	309
Figure 161 SSH Example 2: Test .....	309
Figure 162 SSH Example 2: Log in .....	310
Figure 163 Secure FTP: Firmware Upload Example .....	310
Figure 164 Telnet Configuration on a TCP/IP Network .....	311
Figure 165 Telnet .....	311
Figure 166 FTP .....	312
Figure 167 SNMP Management Model .....	314

Figure 168 SNMP .....	316
Figure 169 DNS .....	317
Figure 170 CNM .....	318
Figure 171 UPnP .....	322
Figure 172 UPnP Ports .....	323
Figure 173 H.323 ALG Example .....	334
Figure 174 SIP ALG Example .....	335
Figure 175 ALG .....	336
Figure 176 View Log .....	339
Figure 177 myZyXEL.com: Download Center .....	341
Figure 178 myZyXEL.com: Certificate Download .....	342
Figure 179 Log Settings .....	343
Figure 180 Reports .....	346
Figure 181 Web Site Hits Report Example .....	347
Figure 182 Protocol/Port Report Example .....	348
Figure 183 Host IP Address Report Example .....	349
Figure 184 General Setup .....	352
Figure 185 Password Setup .....	353
Figure 186 Time and Date .....	354
Figure 187 Synchronization in Process .....	357
Figure 188 Synchronization is Successful .....	357
Figure 189 Synchronization Fail .....	357
Figure 190 Device Mode (Router Mode) .....	359
Figure 191 Device Mode (Bridge Mode) .....	360
Figure 192 Firmware Upload .....	362
Figure 193 Firmware Upload In Process .....	362
Figure 194 Network Temporarily Disconnected .....	363
Figure 195 Firmware Upload Error .....	363
Figure 196 Backup and Restore .....	364
Figure 197 Configuration Upload Successful .....	365
Figure 198 Network Temporarily Disconnected .....	365
Figure 199 Configuration Upload Error .....	365
Figure 200 Reset Warning Message .....	366
Figure 201 Restart Screen .....	366
Figure 202 Initial Screen .....	368
Figure 203 Password Screen .....	368
Figure 204 Main Menu (Router Mode) .....	370
Figure 205 Main Menu (Bridge Mode) .....	370
Figure 206 Menu 23: System Password .....	373
Figure 207 Menu 1: General Setup (Router Mode) .....	375
Figure 208 Menu 1: General Setup (Bridge Mode) .....	376
Figure 209 Menu 1.1: Configure Dynamic DNS .....	377
Figure 210 Menu 1.1.1: DDNS Host Summary .....	378

Figure 211 Menu 1.1.1: DDNS Edit Host .....	379
Figure 212 MAC Address Cloning in WAN Setup .....	381
Figure 213 Menu 2: Dial Backup Setup .....	383
Figure 214 Menu 2.1: Advanced WAN Setup .....	384
Figure 215 Menu 11.2: Remote Node Profile (Backup ISP) .....	386
Figure 216 Menu 11.2.1: Remote Node PPP Options .....	388
Figure 217 Menu 11.2.2: Remote Node Network Layer Options .....	389
Figure 218 Menu 11.2.3: Remote Node Script .....	391
Figure 219 Menu 11.2.4: Remote Node Filter .....	392
Figure 220 Menu 3: LAN Setup .....	393
Figure 221 Menu 3.1: LAN Port Filter Setup .....	394
Figure 222 Menu 3: TCP/IP and DHCP Setup .....	394
Figure 223 Menu 3.2: TCP/IP and DHCP Ethernet Setup .....	395
Figure 224 Menu 3.2.1: IP Alias Setup .....	397
Figure 225 Menu 4: Internet Access Setup (Ethernet) .....	399
Figure 226 Internet Access Setup (PPTP) .....	401
Figure 227 Internet Access Setup (PPPoE) .....	402
Figure 228 Menu 11: Remote Node Setup .....	403
Figure 229 Menu 11.1: Remote Node Profile for Ethernet Encapsulation .....	404
Figure 230 Menu 11.1: Remote Node Profile for PPPoE Encapsulation .....	406
Figure 231 Menu 11.1: Remote Node Profile for PPTP Encapsulation .....	408
Figure 232 Menu 11.1.2: Remote Node Network Layer Options for Ethernet Encapsulation 409	
Figure 233 Menu 11.1.4: Remote Node Filter (Ethernet Encapsulation) .....	411
Figure 234 Menu 11.1.4: Remote Node Filter (PPPoE or PPTP Encapsulation) .....	411
Figure 235 Menu 11.1.5: Traffic Redirect Setup .....	412
Figure 236 Menu 12: IP Static Route Setup .....	413
Figure 237 Menu 12. 1: Edit IP Static Route .....	414
Figure 238 Menu 4: Applying NAT for Internet Access .....	416
Figure 239 Menu 11.1.2: Applying NAT to the Remote Node .....	416
Figure 240 Menu 15: NAT Setup .....	417
Figure 241 Menu 15.1: Address Mapping Sets .....	418
Figure 242 Menu 15.1.255: SUA Address Mapping Rules .....	418
Figure 243 Menu 15.1.1 Address Mapping Rules .....	419
Figure 244 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set .....	421
Figure 245 Menu 15.2.1: NAT Server Sets .....	422
Figure 246 15.2.x: NAT Server Configuration .....	423
Figure 247 Menu 15.2: NAT Server Setup .....	424
Figure 248 Server Behind NAT Example .....	424
Figure 249 NAT Example 1 .....	425
Figure 250 Menu 4: Internet Access & NAT Example .....	425
Figure 251 NAT Example 2 .....	426
Figure 252 Menu 15.2: Specifying an Inside Server .....	426



Figure 253 NAT Example 3 .....	427
Figure 254 Example 3: Menu 11.1.2 .....	428
Figure 255 Example 3: Menu 15.1.1.1 .....	428
Figure 256 Example 3: Final Menu 15.1.1 .....	429
Figure 257 Example 3: Menu 15.2 .....	430
Figure 258 NAT Example 4 .....	430
Figure 259 Example 4: Menu 15.1.1.1: Address Mapping Rule .....	431
Figure 260 Example 4: Menu 15.1.1: Address Mapping Rules .....	432
Figure 261 Menu 15.3: Trigger Port Setup .....	433
Figure 262 Menu 21: Filter and Firewall Setup .....	435
Figure 263 Menu 21.2: Firewall Setup .....	436
Figure 264 Outgoing Packet Filtering Process .....	437
Figure 265 Filter Rule Process .....	439
Figure 266 Menu 21: Filter and Firewall Setup .....	441
Figure 267 Menu 21.1: Filter Set Configuration .....	442
Figure 268 Menu 21.1.1.1: TCP/IP Filter Rule .....	444
Figure 269 Executing an IP Filter .....	446
Figure 270 Menu 21.1.1.1: Generic Filter Rule .....	447
Figure 271 Telnet Filter Example .....	448
Figure 272 Example Filter: Menu 21.1.3.1 .....	449
Figure 273 Example Filter Rules Summary: Menu 21.1.3 .....	450
Figure 274 Protocol and Device Filter Sets .....	451
Figure 275 Filtering LAN Traffic .....	452
Figure 276 Filtering Remote Node Traffic .....	452
Figure 277 Menu 22: SNMP Configuration .....	453
Figure 278 Menu 24: System Maintenance .....	455
Figure 279 Menu 24.1: System Maintenance: Status .....	456
Figure 280 Menu 24.2: System Information and Console Port Speed .....	457
Figure 281 Menu 24.2.1: System Maintenance: Information .....	458
Figure 282 Menu 24.2.2: System Maintenance: Change Console Port Speed .....	459
Figure 283 Menu 24.3: System Maintenance: Log and Trace .....	459
Figure 284 Examples of Error and Information Messages .....	460
Figure 285 Menu 24.3.2: System Maintenance: Syslog Logging .....	460
Figure 286 Call-Triggering Packet Example .....	463
Figure 287 Menu 24.4: System Maintenance: Diagnostic .....	464
Figure 288 Telnet into Menu 24.5 .....	469
Figure 289 FTP Session Example .....	470
Figure 290 System Maintenance: Backup Configuration .....	472
Figure 291 System Maintenance: Starting Xmodem Download Screen .....	472
Figure 292 Backup Configuration Example .....	473
Figure 293 Successful Backup Confirmation Screen .....	473
Figure 294 Telnet into Menu 24.6 .....	474
Figure 295 Restore Using FTP Session Example .....	475

Figure 296 System Maintenance: Restore Configuration .....	475
Figure 297 System Maintenance: Starting Xmodem Download Screen .....	475
Figure 298 Restore Configuration Example .....	475
Figure 299 Successful Restoration Confirmation Screen .....	476
Figure 300 Telnet Into Menu 24.7.1: Upload System Firmware .....	477
Figure 301 Telnet Into Menu 24.7.2: System Maintenance .....	477
Figure 302 FTP Session Example of Firmware File Upload .....	478
Figure 303 Menu 24.7.1 As Seen Using the Console Port .....	480
Figure 304 Example Xmodem Upload .....	480
Figure 305 Menu 24.7.2 As Seen Using the Console Port .....	481
Figure 306 Example Xmodem Upload .....	481
Figure 307 Command Mode in Menu 24 .....	483
Figure 308 Valid Commands .....	484
Figure 309 Call Control .....	485
Figure 310 Budget Management .....	486
Figure 311 Call History .....	487
Figure 312 Menu 24: System Maintenance .....	488
Figure 313 Menu 24.10 System Maintenance: Time and Date Setting .....	488
Figure 314 Menu 24.11 – Remote Management Control .....	492
Figure 315 Schedule Setup .....	495
Figure 316 Schedule Set Setup .....	496
Figure 317 Applying Schedule Set(s) to a Remote Node (PPPoE) .....	497
Figure 318 Applying Schedule Set(s) to a Remote Node (PPTP) .....	498
Figure 319 Pop-up Blocker .....	502
Figure 320 Internet Options: Privacy .....	502
Figure 321 Internet Options: Privacy .....	503
Figure 322 Pop-up Blocker Settings .....	504
Figure 323 Internet Options: Security .....	505
Figure 324 Security Settings - Java Scripting .....	506
Figure 325 Security Settings - Java .....	507
Figure 326 Java (Sun) .....	508
Figure 327 Console/Dial Backup Cable DB-9 End Pin Layout .....	512
Figure 328 Ethernet Cable Pin Assignments .....	513
Figure 329 Wall-mounting Example .....	515
Figure 330 WIndows 95/98/Me: Network: Configuration .....	518
Figure 331 Windows 95/98/Me: TCP/IP Properties: IP Address .....	519
Figure 332 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	520
Figure 333 Windows XP: Start Menu .....	521
Figure 334 Windows XP: Control Panel .....	521
Figure 335 Windows XP: Control Panel: Network Connections: Properties .....	522
Figure 336 Windows XP: Local Area Connection Properties .....	522
Figure 337 Windows XP: Internet Protocol (TCP/IP) Properties .....	523
Figure 338 Windows XP: Advanced TCP/IP Properties .....	524

Figure 339 Windows XP: Internet Protocol (TCP/IP) Properties .....	525
Figure 340 Macintosh OS 8/9: Apple Menu .....	526
Figure 341 Macintosh OS 8/9: TCP/IP .....	526
Figure 342 Macintosh OS X: Apple Menu .....	527
Figure 343 Macintosh OS X: Network .....	528
Figure 344 Red Hat 9.0: KDE: Network Configuration: Devices .....	529
Figure 345 Red Hat 9.0: KDE: Ethernet Device: General .....	529
Figure 346 Red Hat 9.0: KDE: Network Configuration: DNS .....	530
Figure 347 Red Hat 9.0: KDE: Network Configuration: Activate .....	530
Figure 348 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 .....	531
Figure 349 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 .....	531
Figure 350 Red Hat 9.0: DNS Settings in resolv.conf .....	531
Figure 351 Red Hat 9.0: Restart Ethernet Card .....	532
Figure 352 Red Hat 9.0: Checking TCP/IP Properties .....	532
Figure 353 VPN Rules .....	546
Figure 354 Headquarters Gateway Policy Edit .....	547
Figure 355 Branch Office Gateway Policy Edit .....	548
Figure 356 Headquarters VPN Rule .....	549
Figure 357 Branch Office VPN Rule .....	549
Figure 358 Headquarters Network Policy Edit .....	550
Figure 359 Branch Office Network Policy Edit .....	551
Figure 360 VPN Rule Configured .....	552
Figure 361 VPN Dial .....	552
Figure 362 VPN Tunnel Established .....	552
Figure 363 VPN Log Example .....	554
Figure 364 IKE/IPSec Debug Example .....	555
Figure 365 Security Certificate .....	557
Figure 366 Login Screen .....	558
Figure 367 Certificate General Information before Import .....	558
Figure 368 Certificate Import Wizard 1 .....	559
Figure 369 Certificate Import Wizard 2 .....	559
Figure 370 Certificate Import Wizard 3 .....	560
Figure 371 Root Certificate Store .....	560
Figure 372 Certificate General Information after Import .....	561
Figure 373 ZyWALL Trusted CA Screen .....	562
Figure 374 CA Certificate Example .....	563
Figure 375 Personal Certificate Import Wizard 1 .....	564
Figure 376 Personal Certificate Import Wizard 2 .....	564
Figure 377 Personal Certificate Import Wizard 3 .....	565
Figure 378 Personal Certificate Import Wizard 4 .....	565
Figure 379 Personal Certificate Import Wizard 5 .....	566
Figure 380 Personal Certificate Import Wizard 6 .....	566
Figure 381 Access the ZyWALL Via HTTPS .....	566

Figure 382 SSL Client Authentication .....	567
Figure 383 ZyWALL Secure Login Screen .....	567
Figure 384 Option to Enter Debug Mode .....	585
Figure 385 Boot Module Commands .....	586
Figure 386 Displaying Log Categories Example .....	604
Figure 387 Displaying Log Parameters Example .....	605

# List of Tables

Table 1 Front Panel Lights .....	52
Table 2 Web Configurator HOME Screen in Router Mode .....	56
Table 3 Web Configurator HOME Screen in Bridge Mode .....	59
Table 4 Bridge and Router Mode Features Comparison .....	61
Table 5 Screens Summary .....	62
Table 6 Home: Show Statistics .....	65
Table 7 Home: DHCP Table .....	66
Table 8 Home: VPN Status .....	67
Table 9 ISP Parameters: Ethernet Encapsulation .....	70
Table 10 ISP Parameters: PPPoE Encapsulation .....	71
Table 11 ISP Parameters: PPTP Encapsulation .....	73
Table 12 Internet Access Wizard: Registration .....	76
Table 13 VPN Wizard: Gateway Setting .....	79
Table 14 VPN Wizard: Network Setting .....	81
Table 15 VPN Wizard: IKE Tunnel Setting .....	82
Table 16 VPN Wizard: IPSec Setting .....	84
Table 17 VPN Wizard: VPN Status .....	85
Table 18 Registration .....	90
Table 19 Service .....	92
Table 20 LAN .....	97
Table 21 LAN Static DHCP .....	99
Table 22 LAN IP Alias .....	101
Table 23 STP Path Costs .....	104
Table 24 STP Port States .....	105
Table 25 Bridge .....	106
Table 26 WAN Route .....	110
Table 27 Private IP Address Ranges .....	111
Table 28 Example of Network Properties for LAN Servers with Fixed IP Addresses .....	112
Table 29 WAN: Ethernet Encapsulation .....	113
Table 30 WAN: PPPoE Encapsulation .....	117
Table 31 WAN: PPTP Encapsulation .....	120
Table 32 Traffic Redirect .....	123
Table 33 Dial Backup .....	125
Table 34 Advanced Setup .....	128
Table 35 Blocking All LAN to WAN IRC Traffic Example .....	134
Table 36 Limited LAN to WAN IRC Traffic Example .....	135
Table 37 Default Rule (Router Mode) .....	136
Table 38 Default Rule (Bridge Mode) .....	137

Table 39 Rule Summary .....	138
Table 40 Firewall Edit Rule .....	141
Table 41 Anti-Probing .....	143
Table 42 Firewall Threshold .....	145
Table 43 Firewall Service .....	147
Table 44 Firewall Edit Custom Service .....	148
Table 45 Content Filter: General .....	156
Table 46 Content Filter: Categories .....	159
Table 47 Content Filter: Customization .....	166
Table 48 Content Filter: Cache .....	169
Table 49 VPN Example: Matching ID Type and Content .....	184
Table 50 VPN Example: Mismatching ID Type and Content .....	184
Table 51 VPN: Types of Encryption and Authentication in ESP and AH .....	188
Table 52 VPN: Transport and Tunnel Mode Encapsulation .....	189
Table 53 VPN: NAT Compatibility with Active Protocol and Encapsulation .....	190
Table 54 VPN Rules (IKE) .....	193
Table 55 VPN Rules (IKE): Gateway Policy: Edit .....	196
Table 56 VPN Rules (IKE): Network Policy Edit .....	202
Table 57 VPN Rules (IKE): Network Policy Move .....	205
Table 58 VPN Rules (Manual) .....	206
Table 59 VPN Rules (Manual) Edit .....	208
Table 60 VPN: SA Monitor .....	211
Table 61 VPN: Global Setting .....	212
Table 62 Telecommuters Sharing One VPN Rule Example .....	214
Table 63 Telecommuters Using Unique VPN Rules Example .....	215
Table 64 My Certificates .....	219
Table 65 My Certificate Import .....	222
Table 66 My Certificate Create .....	223
Table 67 My Certificate Details .....	226
Table 68 Trusted CAs .....	228
Table 69 Trusted CA Import .....	229
Table 70 Trusted CA Details .....	231
Table 71 Trusted Remote Hosts .....	233
Table 72 Trusted Remote Host Import .....	236
Table 73 Trusted Remote Host Details .....	237
Table 74 Directory Servers .....	240
Table 75 Directory Server Add .....	241
Table 76 Local User Database .....	246
Table 77 RADIUS .....	247
Table 78 NAT Definitions .....	249
Table 79 NAT Application With IP Alias .....	251
Table 80 NAT Mapping Types .....	253
Table 81 NAT Overview .....	254

Table 82 NAT Address Mapping .....	256
Table 83 NAT Address Mapping Edit .....	257
Table 84 Port Forwarding .....	261
Table 85 Port Triggering .....	264
Table 86 IP Static Route .....	266
Table 87 IP Static Route Edit .....	267
Table 88 Application and Subnet-based Bandwidth Management Example .....	271
Table 89 Maximize Bandwidth Usage Example .....	272
Table 90 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example .....	273
Table 91 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example .....	273
Table 92 Bandwidth Borrowing Example .....	274
Table 93 Bandwidth Management: Summary .....	276
Table 94 Bandwidth Management: Class Setup .....	277
Table 95 Bandwidth Management: Edit Class .....	279
Table 96 Services and Port Numbers .....	281
Table 97 Bandwidth Management: Statistics .....	282
Table 98 Bandwidth Management: Monitor .....	283
Table 99 System DNS .....	288
Table 100 System DNS: Add Address Record .....	289
Table 101 System DNS: Insert Name Server Record .....	290
Table 102 DNS Cache .....	292
Table 103 DNS DHCP .....	293
Table 104 DDNS .....	295
Table 105 WWW .....	300
Table 106 How SSH Works .....	306
Table 107 SSH .....	308
Table 108 Telnet .....	312
Table 109 FTP .....	313
Table 110 SNMP Traps .....	315
Table 111 SNMP .....	316
Table 112 DNS .....	317
Table 113 CNM .....	318
Table 114 UPnP .....	322
Table 115 UPnP Ports .....	323
Table 116 ALG .....	337
Table 117 View Log .....	339
Table 118 Example Log Description .....	340
Table 119 Log Settings .....	344
Table 120 Reports .....	346
Table 121 Web Site Hits Report .....	347
Table 122 Protocol/ Port Report .....	348
Table 123 Host IP Address Report .....	349
Table 124 Report Specifications .....	349

Table 125 General Setup .....	352
Table 126 Password Setup .....	353
Table 127 Time and Date .....	354
Table 128 Default Time Servers .....	356
Table 129 MAC-address-to-port Mapping Table .....	358
Table 130 Device Mode (Router Mode) .....	359
Table 131 Device Mode (Bridge Mode) .....	360
Table 132 Firmware Upload .....	362
Table 133 Restore Configuration .....	364
Table 134 Main Menu Commands .....	368
Table 135 Main Menu Summary .....	371
Table 136 SMT Menus Overview .....	371
Table 137 Menu 1: General Setup (Router Mode) .....	375
Table 138 Menu 1: General Setup (Bridge Mode) .....	376
Table 139 Menu 1.1: Configure Dynamic DNS .....	377
Table 140 Menu 1.1.1: DDNS Host Summary .....	378
Table 141 Menu 1.1.1: DDNS Edit Host .....	379
Table 142 MAC Address Cloning in WAN Setup .....	382
Table 143 Menu 2: Dial Backup Setup .....	383
Table 144 Advanced WAN Port Setup: AT Commands Fields .....	384
Table 145 Advanced WAN Port Setup: Call Control Parameters .....	385
Table 146 Menu 11.2: Remote Node Profile (Backup ISP) .....	386
Table 147 Menu 11.2.1: Remote Node PPP Options .....	388
Table 148 Menu 11.2.2: Remote Node Network Layer Options .....	389
Table 149 Menu 11.2.3: Remote Node Script .....	391
Table 150 Menu 3.2: DHCP Ethernet Setup Fields .....	395
Table 151 Menu 3.2: LAN TCP/IP Setup Fields .....	396
Table 152 Menu 3.2.1: IP Alias Setup .....	397
Table 153 Menu 4: Internet Access Setup (Ethernet) .....	400
Table 154 New Fields in Menu 4 (PPTP) Screen .....	401
Table 155 New Fields in Menu 4 (PPPoE) screen .....	402
Table 156 Menu 11.1: Remote Node Profile for Ethernet Encapsulation .....	404
Table 157 Fields in Menu 11.1 (PPPoE Encapsulation Specific) .....	407
Table 158 Menu 11.1: Remote Node Profile for PPTP Encapsulation .....	408
Table 159 Remote Node Network Layer Options Menu Fields .....	409
Table 160 Menu 11.1.5: Traffic Redirect Setup .....	412
Table 161 Menu 12. 1: Edit IP Static Route .....	414
Table 162 Applying NAT in Menus 4 & 11.1.2 .....	417
Table 163 SUA Address Mapping Rules .....	418
Table 164 Fields in Menu 15.1.1 .....	420
Table 165 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set .....	421
Table 166 15.2.x: NAT Server Configuration .....	423
Table 167 NAT Example 3 .....	427



Table 168 Menu 15.3: Trigger Port Setup .....	433
Table 169 Abbreviations Used in the Filter Rules Summary Menu .....	442
Table 170 Rule Abbreviations Used .....	443
Table 171 Menu 21.1.1.1: TCP/IP Filter Rule .....	444
Table 172 Generic Filter Rule Menu Fields .....	447
Table 173 SNMP Configuration Menu Fields .....	453
Table 174 SNMP Traps .....	454
Table 175 System Maintenance: Status Menu Fields .....	456
Table 176 Fields in System Maintenance: Information .....	458
Table 177 System Maintenance Menu Syslog Parameters .....	460
Table 178 System Maintenance Menu Diagnostic .....	464
Table 179 Filename Conventions .....	468
Table 180 General Commands for GUI-based FTP Clients .....	470
Table 181 General Commands for GUI-based TFTP Clients .....	472
Table 182 Valid Commands .....	484
Table 183 Budget Management .....	486
Table 184 Call History .....	487
Table 185 Menu 24.10 System Maintenance: Time and Date Setting .....	489
Table 186 Menu 24.11 – Remote Management Control .....	492
Table 187 Schedule Set Setup .....	496
Table 188 Troubleshooting the Start-Up of Your ZyWALL .....	499
Table 189 Troubleshooting the LAN Interface .....	499
Table 190 Troubleshooting the WAN Interface .....	500
Table 191 Troubleshooting Accessing the ZyWALL .....	500
Table 192 Device Specifications .....	509
Table 193 Performance .....	509
Table 194 Firmware Features .....	510
Table 195 Feature Specifications .....	511
Table 196 Console Cable Pin Assignments .....	512
Table 197 Console Cable Pin Assignments .....	512
Table 198 Power Adaptor Specifications .....	513
Table 199 Classes of IP Addresses .....	533
Table 200 Allowed IP Address Range By Class .....	534
Table 201 “Natural” Masks .....	534
Table 202 Alternative Subnet Mask Notation .....	535
Table 203 Two Subnets Example .....	535
Table 204 Subnet 1 .....	536
Table 205 Subnet 2 .....	536
Table 206 Subnet 1 .....	537
Table 207 Subnet 2 .....	537
Table 208 Subnet 3 .....	537
Table 209 Subnet 4 .....	538
Table 210 Eight Subnets .....	538

Table 211 Class C Subnet Planning .....	538
Table 212 Class B Subnet Planning .....	539
Table 213 Commonly Used Services .....	541
Table 214 Firewall Commands .....	571
Table 215 NetBIOS Filter Default Settings .....	578
Table 216 Certificates Commands .....	579
Table 217 Brute-Force Password Guessing Protection Commands .....	583
Table 218 System Maintenance Logs .....	587
Table 219 System Error Logs .....	588
Table 220 Access Control Logs .....	589
Table 221 TCP Reset Logs .....	589
Table 222 Packet Filter Logs .....	590
Table 223 ICMP Logs .....	590
Table 224 CDR Logs .....	591
Table 225 PPP Logs .....	591
Table 226 UPnP Logs .....	591
Table 227 Content Filtering Logs .....	592
Table 228 Attack Logs .....	592
Table 229 Remote Management Logs .....	594
Table 230 IPsec Logs .....	594
Table 231 IKE Logs .....	595
Table 232 PKI Logs .....	598
Table 233 Certificate Path Verification Failure Reason Codes .....	599
Table 234 802.1X Logs .....	600
Table 235 ACL Setting Notes .....	601
Table 236 ICMP Notes .....	601
Table 237 Syslog Logs .....	603
Table 238 RFC-2408 ISAKMP Payload Types .....	603

# 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 connection information and instructions on getting started.
- 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 right angle bracket ( > ). For example, “In Windows, click **Start > Settings > 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 

# 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 and certificates. 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, DHCP server and many other powerful features.

### 1.2 Physical Features

#### 4-port LAN Switch

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

#### WAN

The Ethernet WAN port connects to the Internet via broadband modem or router.

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

All of the ZyWALL's Ethernet ports are 10/100 Mbps auto-negotiating. This allows 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 if the WAN 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.

## Reset Button

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

## 1.2.1 Non-Physical Features

### 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 change your existing network configuration.

### 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 user name 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 and disable web proxies. The ZyWALL can block or allow access to web sites that you specify. It 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.

## **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.

## **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, interfaces via its single physical Ethernet LAN interface with the ZyWALL itself as the gateway for each network.

## **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 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 where it relays IP address assignment from another DHCP server to the clients.

## **Full Network Management**

The embedded web configurator is an all-platform, web-based utility that allows you to easily manage and configure the ZyWALL. 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.

## **Upgradable Firmware**

The firmware of the ZyWALL can be upgraded.

## **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.

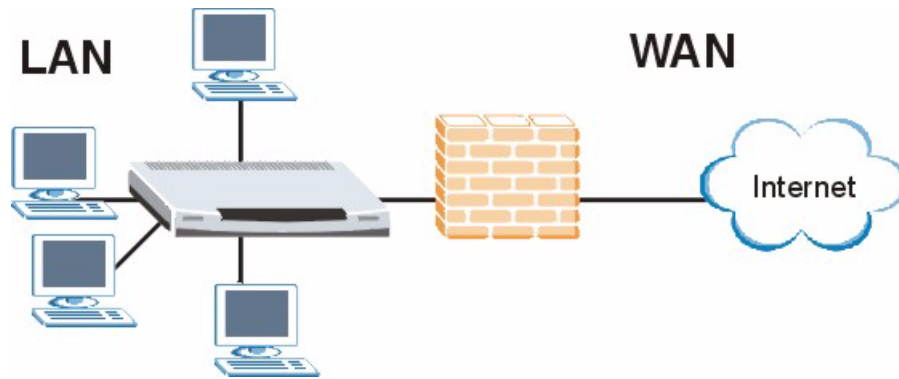
# **1.3 Applications for the ZyWALL**

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 with an Ethernet port to the ZyWALL for broadband Internet access. The ZyWALL guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

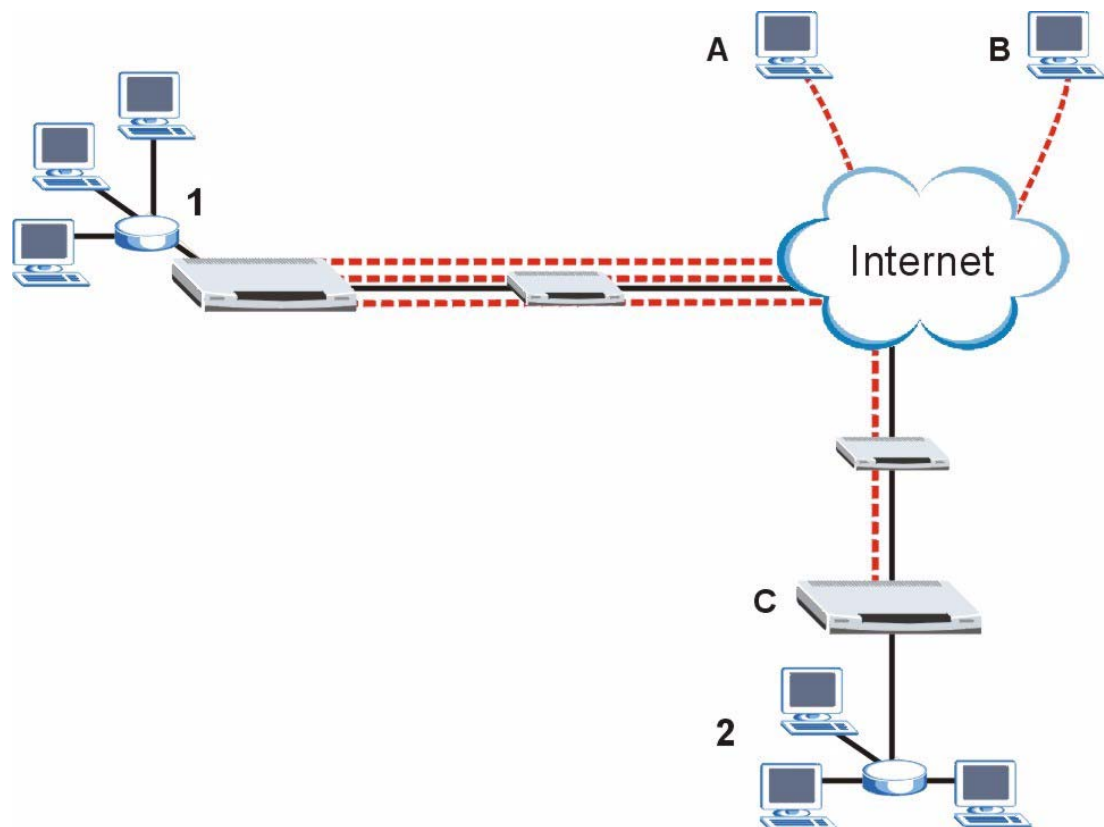
**Figure 1** Secure Internet Access via Cable, DSL or Wireless Modem



### 1.3.2 VPN Application

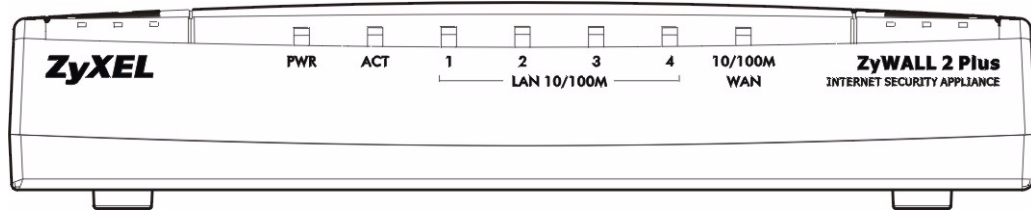
ZyWALL VPN is an ideal cost-effective way to connect branch offices and business partners over the Internet without the need (and expense) for leased lines between sites. In the following diagram, **A** is a VPN Client for secure remote management, **B** is a VPN client for remote access, and **C** is a remote IPSec router. The LAN is marked **1** and the remote network is marked **2**. The dotted lines show VPN tunnels.

**Figure 2** VPN Application



### 1.3.3 Front Panel Lights

Figure 3 Front Panel



The following table describes the lights.

Table 1 Front Panel Lights

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The ZyWALL is turned off.
	Green	On	The ZyWALL is turned on.
	Red	Flashing	The ZyWALL is performing system tests.
		On	The power to the ZyWALL is too low.
ACT	Green	Off	The backup port is not connected.
		On	The backup port is connected.
		Flashing	The backup port is sending or receiving packets.
LAN 10/100M 1-4		Off	The LAN 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.	
WAN 10/100M		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.	

# 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.

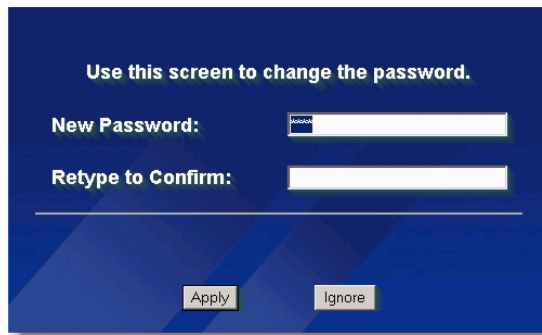
In order to use the web configurator you need to allow:

- 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

- 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 4** 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 5** 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 7 on page 56](#)).

**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

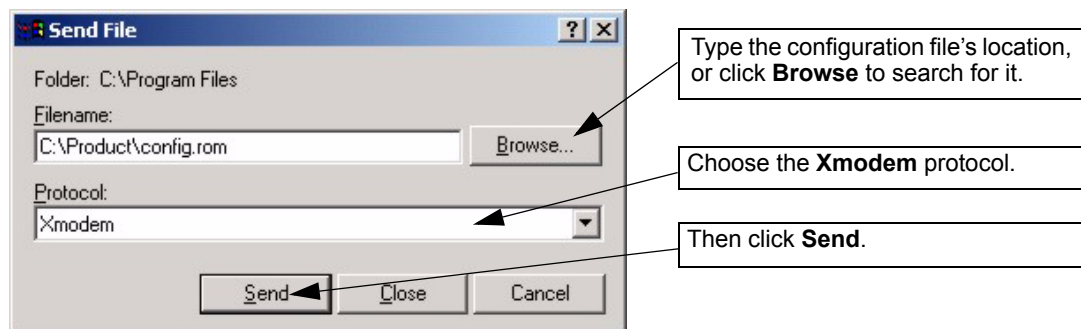
Make sure the **SYS LED** is on (not blinking) before you begin this procedure.

- 1 Press the **RESET** button for ten seconds, and then release it. The ZyWALL restarts with the defaults restored. 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 ZyWALL restarts with the defaults restored.
- 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 6** 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.

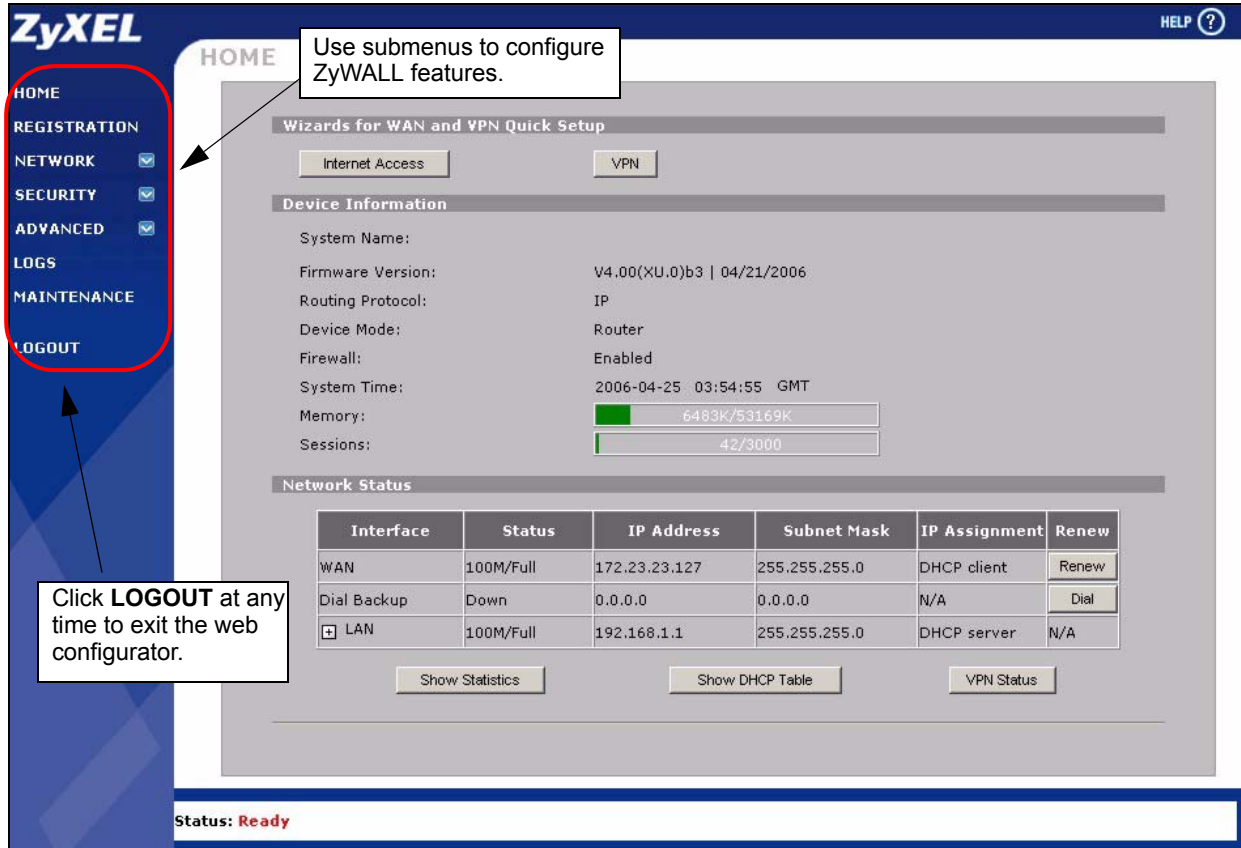
**Note:** Follow the instructions you see in the **HOME** screen or click the  icon.

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.

**Figure 7** Web Configurator HOME Screen in Router Mode



The following table describes the labels in this screen.

**Table 2** Web Configurator HOME Screen in Router Mode

LABEL	DESCRIPTION
Wizards for WAN and VPN Quick Setup	
Internet Access	Click <b>Internet Access</b> to use the initial configuration wizard. This configures the WAN port to connect to the Internet.
VPN	Click <b>VPN</b> to configure a Virtual Private Network (VPN) policy for secure communications between sites.
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.



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

LABEL	DESCRIPTION
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>
Network Status	
Interface	This is the port type. Click "+" to expand or "-" to collapse the LAN drop-down lists.
Status	<p>For the LAN ports, this displays the port speed and duplex setting. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect.</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>
IP Address	This shows the port's IP address.
Subnet Mask	This shows the port's subnet mask.
IP Assignment	<p>For the WAN, <b>DHCP client</b> displays if the ZyWALL gets its IP address automatically. <b>Static</b> displays if the ZyWALL was a manually entered static (fixed) IP address.</p> <p>For the LAN, <b>DHCP server</b> displays when the ZyWALL is set to automatically give IP address information to the computers connected to the LAN. <b>DHCP relay</b> displays when the ZyWALL is set to forward IP address assignment requests to another DHCP server. <b>Static</b> displays if the LAN port is using a manually entered static (fixed) IP address. In this case, you must have another DHCP server on your LAN, or else the computers must be manually configured.</p> <p>This shows <b>N/A</b> for the dial backup port.</p>

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

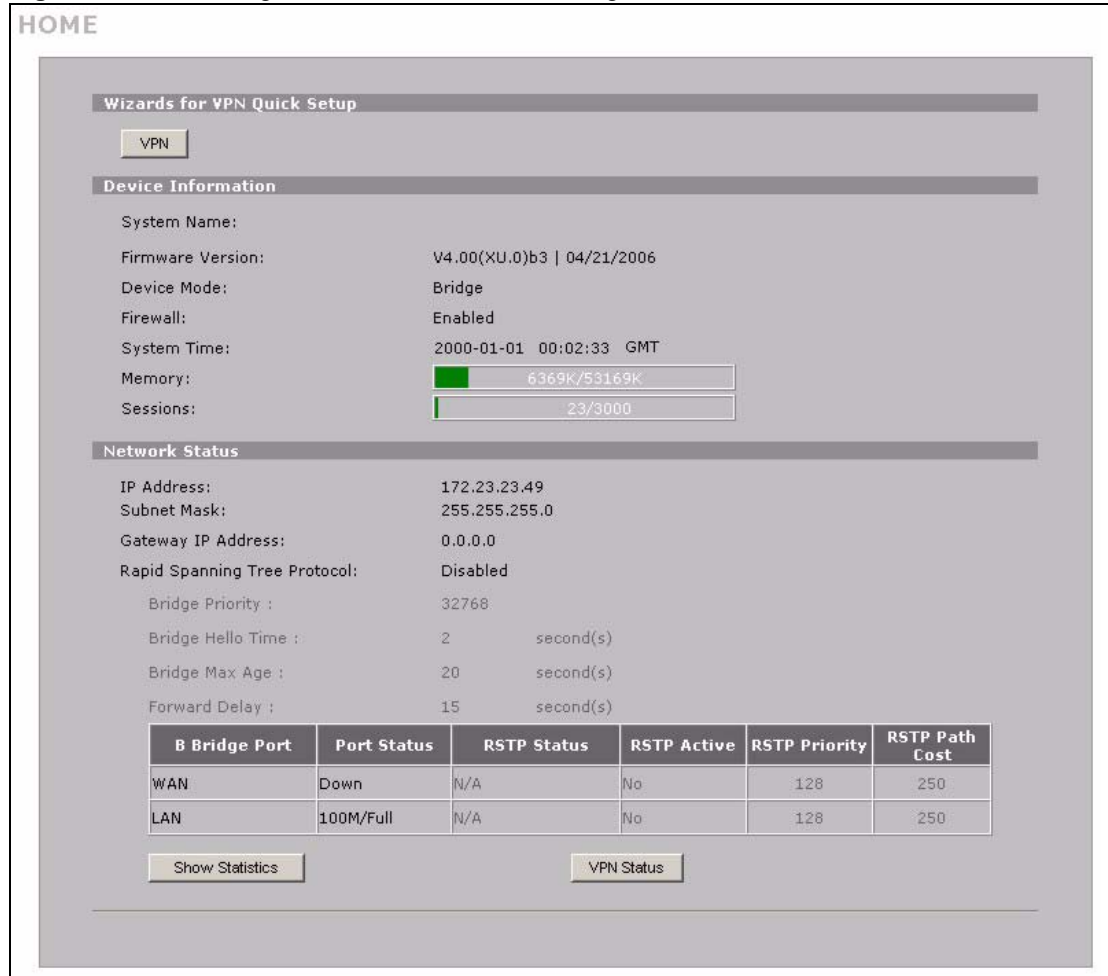
LABEL	DESCRIPTION
Renew	If you are using Ethernet encapsulation and the WAN port is configured to get the IP address automatically from the ISP, click <b>Renew</b> to release the WAN port's dynamically assigned IP address and get the IP address afresh. Click <b>Dial</b> to dial up the PPTP, PPPoE or dial backup connection.
Show Statistics	Click <b>Show Statistics</b> to see performance statistics such as the number of packets sent and number of packets received for each port.
Show DHCP Table	Click <b>Show DHCP Table</b> to show a list of the computers to which the ZyWALL has assigned IP address information.
VPN Status	Click <b>VPN Status</b> to display the active VPN (secure) connections.

## 2.4.2 Bridge Mode

The following screen displays when the ZyWALL is set to bridge mode. While in bridge mode, the ZyWALL does not get an IP address from a DHCP server. The LAN and WAN interfaces 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 8** Web Configurator HOME Screen in Bridge Mode

The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
Wizards for VPN Quick Setup	
VPN	Click <b>VPN</b> to configure a Virtual Private Network (VPN) policy for secure communications between sites.
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.
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.

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

LABEL	DESCRIPTION
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. The gateway is usually the device that connects the ZyWALL to the Internet.
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>LAN</b> .
Port Status	<p>This displays the port speed and duplex setting. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect.</p> <p>For the WAN port, it displays <b>Down</b> when the link is not ready or has failed.</p>
RSTP Status	This is the RSTP status of the corresponding port.
RSTP Active	This shows whether or not RSTP is active on the corresponding port.
RSTP Priority	This is the RSTP priority of the corresponding port.
RSTP Path Cost	This is the cost of transmitting a frame from the root bridge to the corresponding port.

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

LABEL	DESCRIPTION
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.
VPN Status	Click <b>VPN Status</b> to display the active VPN (secure) 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 4** 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
Bridge	O	
Firewall	O	O
Content Filter	O	O
VPN	O	O
Certificates	O	O
Authentication Server	O	O
NAT		O
Static Route		O
Bandwidth Management	O	O
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 5** Screens Summary

LINK	TAB	FUNCTION
HOME		This screen shows the ZyWALL's general device and network status information. Use this screen to access the wizards, statistics and DHCP table.
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.
BRIDGE	Bridge	Use this screen to change the bridge settings on the ZyWALL.
WAN	Route	This screen allows you to configure WAN traffic redirect and dial backup route priority.
	WAN	Use this screen to configure the WAN 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.
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.
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.

**Table 5** Screens Summary (continued)

LINK	TAB	FUNCTION
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 VPN users.
ADVANCED		
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.
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 the DNS information that the ZyWALL assigns to the DHCP clients.
	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.

**Table 5** Screens Summary (continued)

LINK	TAB	FUNCTION
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.
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.

**Figure 9** Home: Show Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	25	1146	0	0	192	0:02:31
Dial Backup	Down	0	0	0	0	0	0:00:00
LAN	100M/Full	348	401	0	354	406	0:32:41

System Up Time : 0:32:46

Poll Interval(s) :



The following table describes the labels in this screen.

**Table 6** Home: Show Statistics

LABEL	DESCRIPTION
Port	These are the ZyWALL's interfaces.
Status	For the LAN, 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.
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 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows computers to obtain TCP/IP configuration (including IP addresses, subnet masks, gateways, and some network information like the IP addresses of DNS servers) 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 the ZyWALL's DHCP service is disabled, you must have another DHCP server on your LAN, or else the computers must be manually configured.

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

**Figure 10** Home: DHCP Table

The screenshot shows the 'HOME - DHCP TABLE' interface. At the top, there is a dropdown menu labeled 'Interface' with 'LAN' selected. Below this is a table with the following data:

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	tw11	00:00:e8:7c:14:80	<input type="checkbox"/>

At the bottom of the interface, there are two buttons: 'Apply' and 'Refresh'.

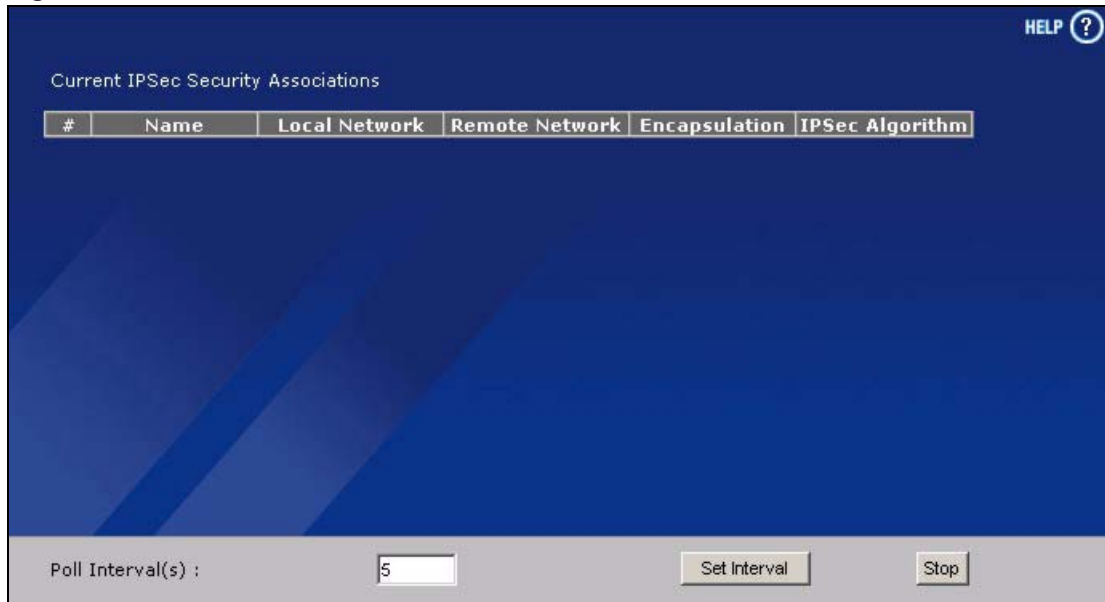
The following table describes the labels in this screen.

**Table 7** Home: DHCP Table

LABEL	DESCRIPTION
Interface	Select an interface 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)). 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.

## 2.4.6 VPN Status

Click **VPN Status** in the **HOME** screen to open the following screen. This screen provides read-only information about the active VPN connections. The **Poll Interval(s)** field is configurable.

**Figure 11** Home: VPN Status

The following table describes the labels in this screen.

**Table 8** 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 the 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 12** ISP Parameters: Ethernet Encapsulation

The following table describes the labels in this screen.

**Table 9** 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 DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

**Figure 13** ISP Parameters: PPPoE Encapsulation

The screenshot shows the 'WIZARD - Internet Access' configuration window. It is divided into two main sections: 'ISP Parameters for Internet Access' and 'WAN IP Address Assignment'.  
 In the 'ISP Parameters for Internet Access' section, there is a dropdown menu for 'Encapsulation' set to 'PPP over Ethernet'. Below it are text input fields for 'Service Name' (marked as optional), 'User Name', 'Password', and 'Retype to Confirm'. There is also a checkbox for 'Nailed-Up' and an 'Idle Timeout' field set to '100 (Seconds)'.  
 In the 'WAN IP Address Assignment' section, there is a dropdown menu for 'IP Address Assignment' set to 'Static'. Below it are four text input fields for 'My WAN IP Address', 'First DNS Server', and 'Second DNS Server', each containing the IP address '0 . 0 . 0 . 0'.  
 An 'Apply' button is located at the bottom right of the configuration area.

The following table describes the labels in this screen.

**Table 10** 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.

**Table 10** ISP Parameters: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
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	
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.



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

**Figure 14** 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: PPTP

User Name: [ ]

Password: [ ]

Retype to Confirm: [ ]

Nailed-Up

Idle Timeout: 100 (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**

IP Address Assignment: Static

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

First DNS Server: 0 . 0 . 0 . 0

Second DNS Server: 0 . 0 . 0 . 0

Apply

The following table describes the labels in this screen.

**Table 11** 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.

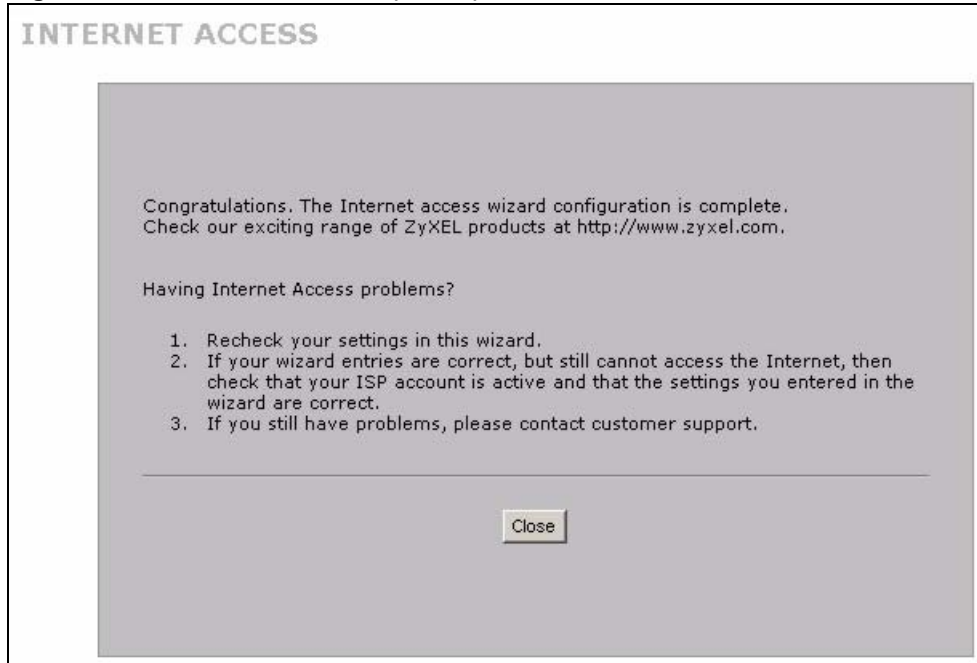
**Table 11** ISP Parameters: PPTP Encapsulation

LABEL	DESCRIPTION
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your xDSL modem.
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 trial application. Otherwise, click **Skip** to display the congratulations screen and click **Close** to complete the Internet access setup.

**Figure 15** Internet Access Wizard: Second Screen

**Figure 16** Internet Access Setup Complete

### 3.2.3 Internet Access Wizard: Registration

If you clicked **Next** in the previous screen (see [Figure 15 on page 74](#)), 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 17** 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 12** Internet Access Wizard: Registration

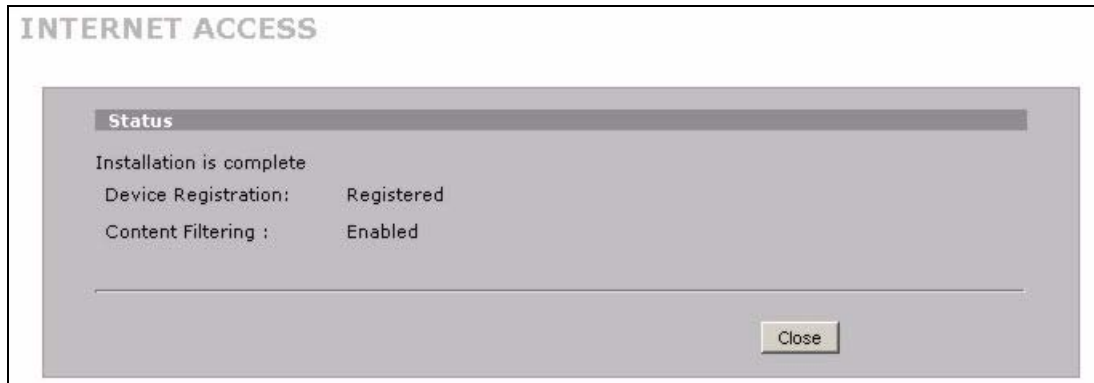
LABEL	DESCRIPTION
Device Registration	If you select <b>Existing myZyXEL.com account</b> , only the <b>User Name</b> and <b>Password</b> fields are available.
New myZyXEL.com account	If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account 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 18** Internet Access Wizard: Registration in Progress



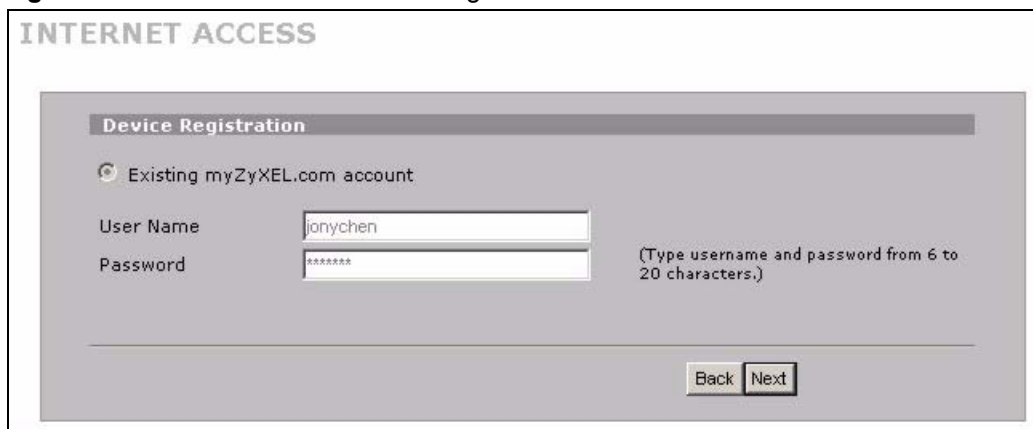
Click **Close** to leave the wizard screen when the registration and activation are done.

**Figure 19** Internet Access Wizard: Status

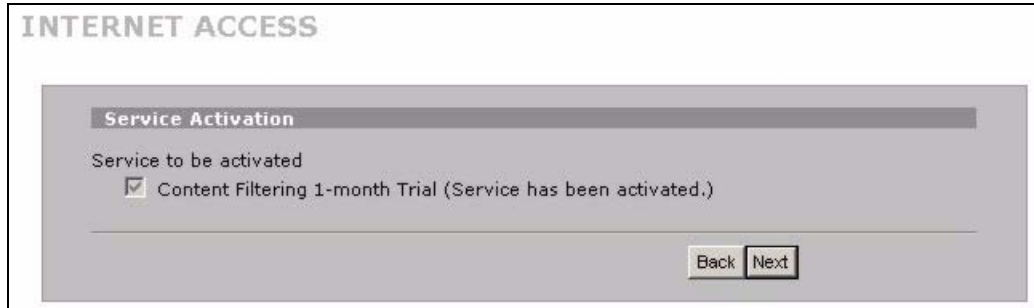
The following screen appears if the registration was not successful. Click **Return** to go back to the **Device Registration** screen and check your settings.

**Figure 20** 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 21** Internet Access Wizard: Registered Device

**Figure 22** Internet Access Wizard: Activated Services



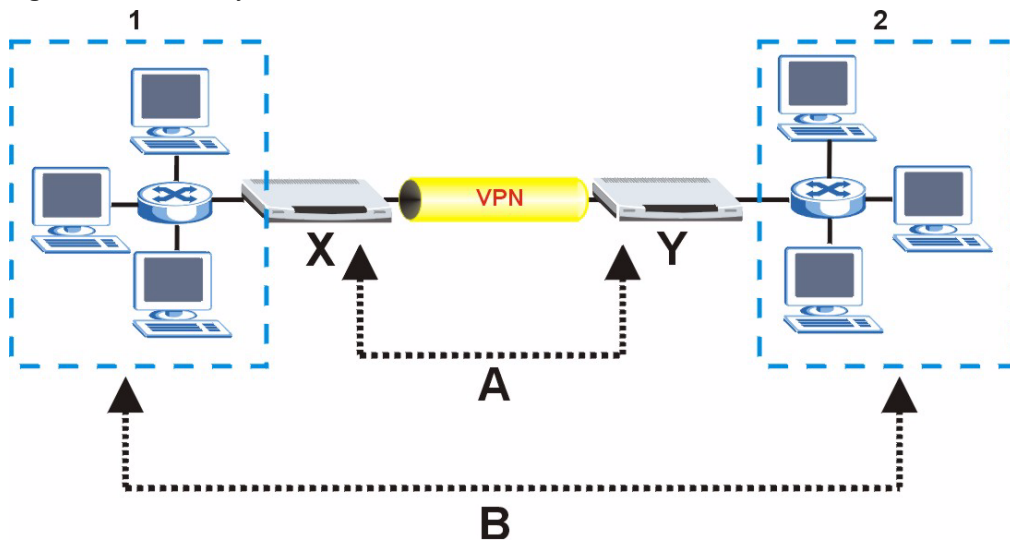
### 3.3 VPN Wizard Gateway Setting

A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.

A gateway policy identifies the IPsec routers at either end of a VPN tunnel.

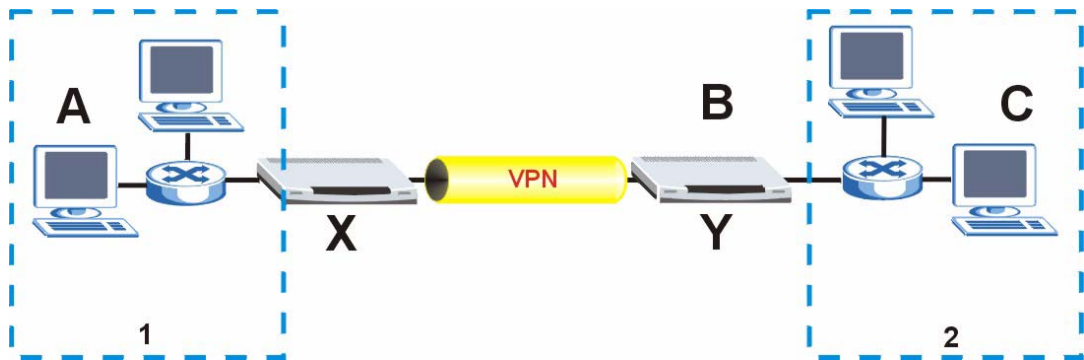
A network policy specifies which devices (behind the IPsec routers) can use the VPN tunnel. In the following diagram, **X** is your ZyWALL, **Y** is a remote IPsec router, the **A** arrows denote the gateway policy and the **B** arrows denote the network policy. The local network is marked **1**, and the remote network is marked **2**.

**Figure 23** Gateway and Network Policies



This figure helps explain the main fields in the wizard screens. In this figure, **X** is your ZyWALL, **Y** is a remote IPsec router, **A** denotes a local network IP address, **B** denotes a remote gateway address and **C** denotes a remote network address. The local network is marked **1**, and the remote network is marked **2**.

**Figure 24** IPSec Fields Summary



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.

**Note:** Your settings are not saved when you click **Back**.

**Figure 25** VPN Wizard: Gateway Setting

The screenshot shows a web-based configuration wizard titled "WIZARD - VPN". It is divided into two main sections: "Gateway Policy Property" and "Gateway Policy Setting".

- Gateway Policy Property:** Contains a "Name" field with the value "Test".
- Gateway Policy Setting:** Contains two fields: "My ZyWALL" with the value "0.0.0.0" and "Remote Gateway Address" with the value "BranchOffice.com".

A "Next" button is located at the bottom right of the form area.

The following table describes the labels in this screen.

**Table 13** 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.

**Table 13** VPN Wizard: Gateway Setting

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>The ZyWALL 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	<p>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.</p>
Next	<p>Click <b>Next</b> to continue.</p>

### 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 26** VPN Wizard: Network Setting



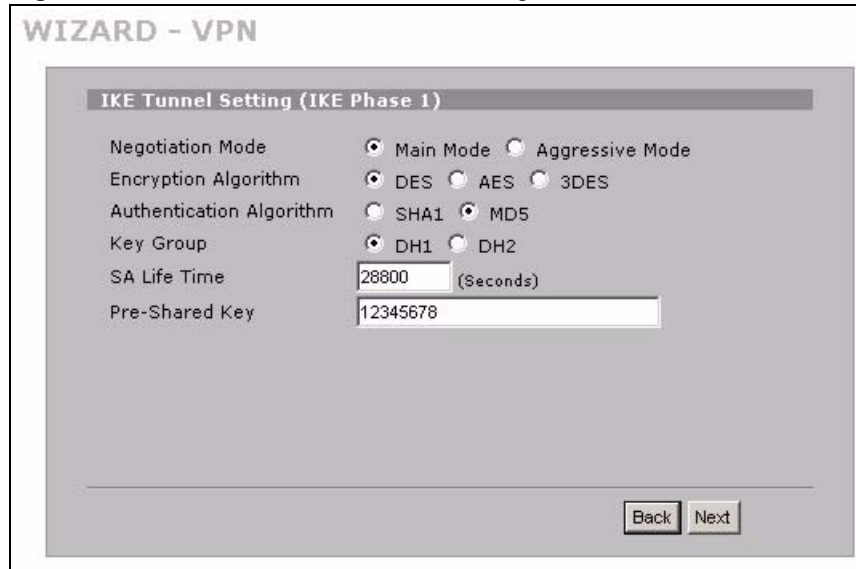
The following table describes the labels in this screen.

**Table 14** 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.
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 27 VPN Wizard: IKE Tunnel Setting



The following table describes the labels in this screen.

Table 15 VPN Wizard: IKE Tunnel Setting

LABEL	DESCRIPTION
Negotiation Mode	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.  <b>Note:</b> Multiple SAs (security associations) connecting through a secure gateway must have the same negotiation mode.
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 <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> .
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.
Key Group	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.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds.  A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.

**Table 15** VPN Wizard: IKE Tunnel Setting (continued)

LABEL	DESCRIPTION
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	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

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

**Figure 28** VPN Wizard: IPSec Setting

The screenshot shows the 'WIZARD - VPN' interface with the 'IPSec Setting (IKE Phase 2)' section. The settings are as follows:

- 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

At the bottom right, there are 'Back' and 'Next' buttons.

The following table describes the labels in this screen.

**Table 16** VPN Wizard: IPsec Setting

LABEL	DESCRIPTION
Encapsulation Mode	<p><b>Tunnel</b> is compatible with NAT, <b>Transport</b> is not.</p> <p>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).</p>
IPsec Protocol	<p>Select the security protocols used for an SA.</p> <p>Both <b>AH</b> and <b>ESP</b> increase ZyWALL processing requirements and communications latency (delay).</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 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.</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>
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>
Perfect Forward Secret (PFS)	<p>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.</p> <p>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).</p>
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 29** 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 17** 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 17** 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 30** 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 Content Filtering Subscription Service

The ZyWALL can use the content filtering subscription service. 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. See the chapter about content filtering for more information.

### 4.2 Registration

To register your ZyWALL with myXEL.com and activate the content filtering service, click **REGISTRATION** in the navigation panel to open the screen as shown next.

**Figure 31** Registration

The following table describes the labels in this screen.

**Table 18** 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.

**Table 18** Registration

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.

**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 32** Registration: Registered Device

**REGISTRATION**

**Registration**   **Service**

**Device Registration**

Existing myZyXEL.com account

User Name:

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

**Service Activation**

Content Filtering 1-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 33** Registration: Service

**REGISTRATION**

**Registration** **Service**

**Service Management**

Service	Status	Registration Type	Expiration Day
Content Filter Service	Active	Trial	2005-08-24

**License Upgrade**

License Key:

(Sync with myZyXEL.com to download license Info.)

The following table describes the labels in this screen.

**Table 19** 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.

### 5.1 LAN, WAN and the ZyWALL

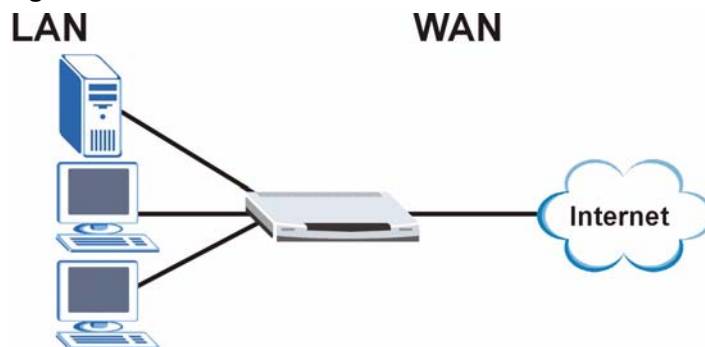
A network is a shared communication system to which many computers are attached.

The Local Area Network (LAN) includes the computers and networking devices in your home or office that you connect to the ZyWALL's LAN ports.

The Wide Area Network (WAN) is another network (most likely the Internet) that you connect to the ZyWALL's WAN port. See [Chapter 7 on page 109](#) for how to use the WAN screens to set up your WAN connection.

The LAN and the WAN are two separate networks. The ZyWALL controls the traffic that goes between them. The following graphic gives an example.

**Figure 34** LAN and WAN



### 5.2 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. If you select 192.168.1.0 as the network number; it 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.

## 5.2.1 Private IP Addresses

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

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

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

## 5.3 DHCP

The ZyWALL can use DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) to automatically assign IP addresses subnet masks, gateways, and some network information like the IP addresses of DNS servers to the computers on your LAN. You can alternatively have the ZyWALL relay DHCP information from another DHCP server. If you disable the ZyWALL's DHCP service, you must have another DHCP server on your LAN, or else the computers must be manually configured.

### 5.3.1 IP Pool Setup

The ZyWALL is pre-configured with a pool of IP addresses for the computers on your LAN. See [Appendix A on page 509](#) for the default IP pool range. Do not assign your LAN computers static IP addresses that are in the DHCP pool.

## 5.4 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**.

## 5.5 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.

## 5.6 WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network's computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name's IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have more than one WINS server. Samba can also serve as a WINS server.

## 5.7 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 20 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 20** 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.
DHCP WINS Server 1, 2	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
For DNS setup please click here	Click this link to go to the <b>DNS DHCP</b> screen to configure the DNS server information that the ZyWALL sends to the DHCP client devices on the LAN.
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.
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 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 > Static DHCP**. 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 consists of a table with three columns: '#', 'MAC Address', and 'IP Address'. The table has 32 rows, with rows 1-7 and 24-32 visible. Each row contains input fields for the MAC address and IP address. The IP address field is 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 21** 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.
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.

## 5.9 LAN IP Alias

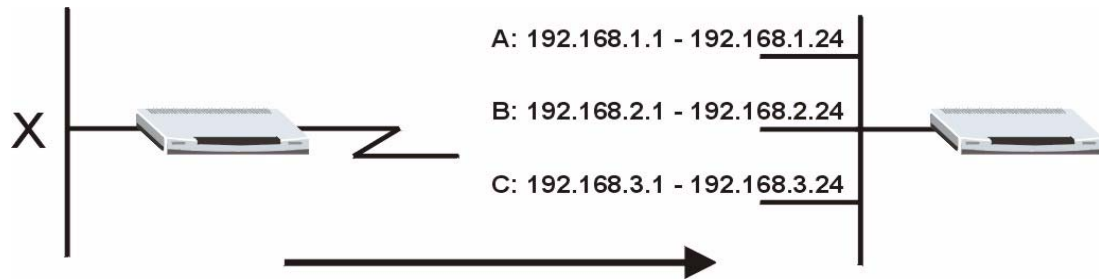
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network.

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.

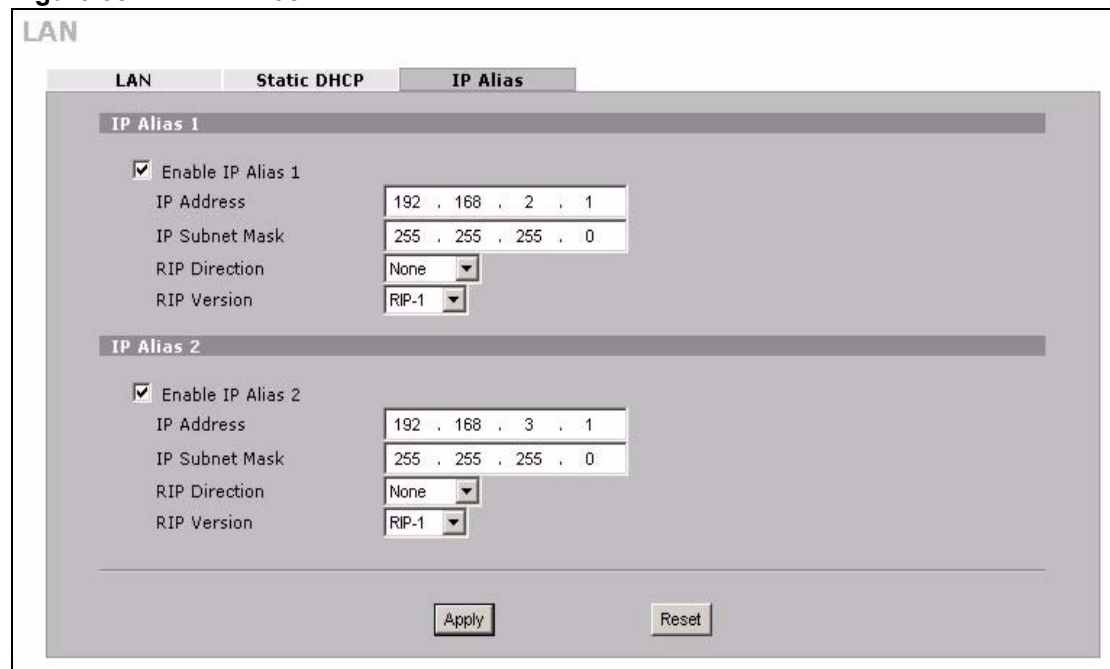
The following figure shows a LAN divided into subnets A, B, and C. The Ethernet interface is labeled X.

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



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

**Figure 38** LAN IP Alias



The following table describes the labels in this screen.

**Table 22** 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> .
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 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

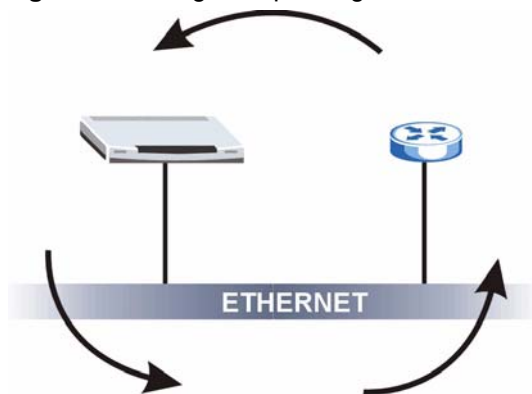
The ZyWALL can serve as a transparent firewall (also known as a bridge firewall) in order to provide firewall protection against denial of service attacks without. You do not need to change your existing network configuration to use the ZyWALL as a bridge firewall. The ZyWALL acts as a bridge between a switch and a wired LAN or between two routers and filters and inspects the packets.

#### 6.1.1 Bridge Loop

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.

The 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. So traffic will circle the network

**Figure 39** Bridge Loop: Bridge Connected to Wired LAN



You can prevent bridge loops by ensuring that your ZyWALL is not set to bridge mode while connected to two wired segments of the same LAN. If your network uses RSTP, you can set the ZyWALL to bridge mode while connected to two wired segments of the same LAN as long as you enable RSTP on the ZyWALL and the LAN's other networking devices.

## 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 23** 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 24** 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 Configuring 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 40** Bridge

The following table describes the labels in this screen.

**Table 25** Bridge

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

**Table 25** 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.



# CHAPTER 7

## WAN Screens

This chapter describes how to configure WAN settings.

### 7.1 WAN Overview

- Use the **WAN Route** screen to configure route priority.
- Use the **WAN** screen to configure the WAN port for Internet access.
- 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 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 priority of the WAN port route must always be higher than the dial-backup and traffic redirect route priorities.

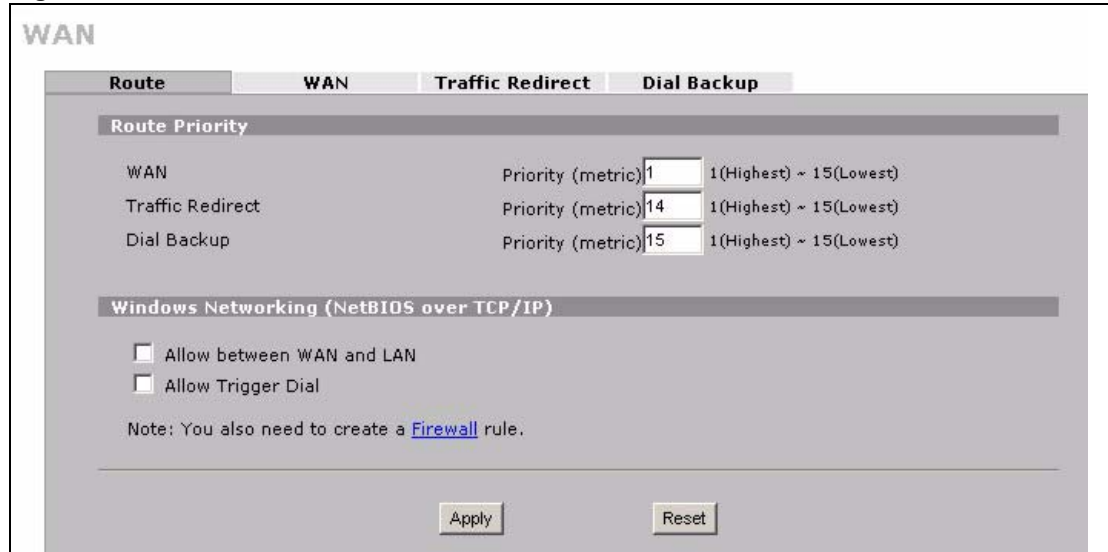
If the WAN port route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the WAN port route acts as the primary default route. If the WAN port route fails to connect to the Internet, the ZyWALL tries the traffic-redirect route next. 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 routes.

### 7.3 WAN Route

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

**Figure 41** WAN Route



The following table describes the labels in this screen.

**Table 26** WAN Route

LABEL	DESCRIPTION
Route Priority	
WAN 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 default priority of the routes is <b>WAN</b> , <b>Traffic Redirect</b> and then <b>Dial Backup</b> : 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"). The <b>Dial Backup</b> field is available only when you enable the corresponding dial backup feature in the <b>Dial Backup</b> screen.
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.
Allow between WAN and LAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow 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.

## 7.4 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 27** 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.

## 7.5 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 17.5.1 on page 286](#)).

## 7.6 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 28** 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)

## 7.7 WAN

To change your ZyWALL's WAN ISP, IP and MAC settings, click **NETWORK > WAN > WAN**. The screen differs by the encapsulation.

### 7.7.1 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 42** WAN: Ethernet Encapsulation

**WAN**

**Route**   **WAN**   **Traffic Redirect**   **Dial Backup**

**ISP Parameters for Internet Access**

Encapsulation: Ethernet

Service Type: RR-Toshiba

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

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

Retype to Confirm: \_\_\_\_\_

Login Server IP Address: 0 . 1 . 0 . 0

**WAN IP Address Assignment**

Get Automatically from ISP

Use Fixed IP Address

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

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

Gateway 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 from LAN

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

Apply   Reset

The following table describes the labels in this screen.

**Table 29** 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 29** 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 29** 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 clone 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>

## 7.7.2 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. 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.

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.

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

**Figure 43** WAN: PPPoE Encapsulation

**WAN**

**Route**   **WAN**   **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: 100 (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

Spooof WAN MAC Address from LAN

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

Apply   Reset

The following table describes the labels in this screen.

**Table 30** 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 14 on page 249</a> .

**Table 30** 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 clone 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>

### 7.7.3 PPTP Encapsulation

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

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

**Figure 44** WAN: PPTP Encapsulation

**WAN**

Route    **WAN**    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: 100 (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 from LAN

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

Apply    Reset

The following table describes the labels in this screen.

**Table 31** 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	



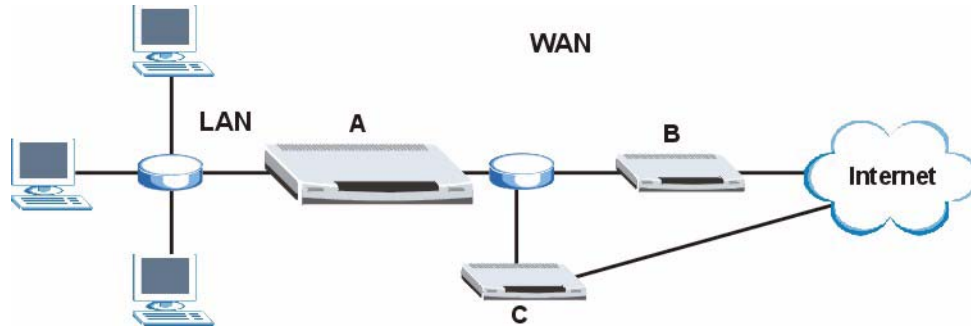
**Table 31** WAN: PPTP Encapsulation

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 14 on page 249</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 clone 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>

## 7.8 Traffic Redirect

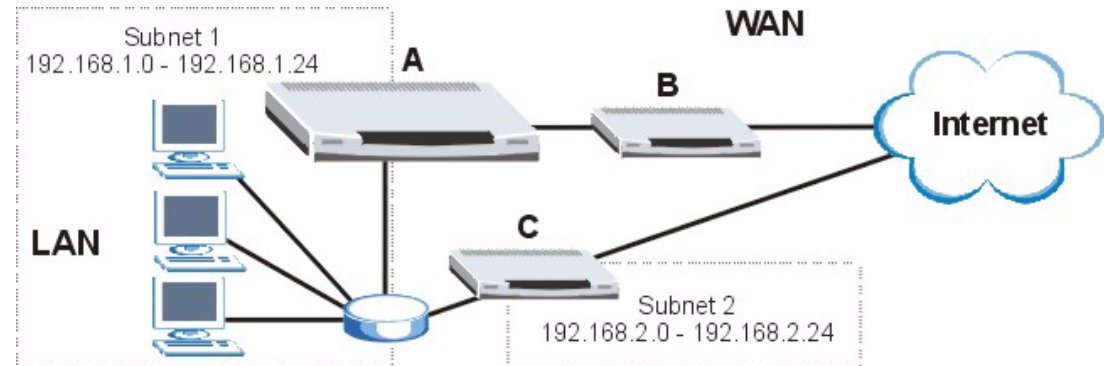
Traffic redirect forwards WAN traffic to a backup gateway when the ZyWALL cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyWALL still provides firewall protection. In the following figure, your ZyWALL is labeled **A**, the gateway is labeled **B** and the backup gateway is labeled **C**.

**Figure 45** Traffic Redirect WAN Setup



The following network topology allows you to avoid triangle route security issues (see [Section 8.13 on page 149](#)) when the backup gateway is connected to the LAN. 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). In the following figure, your ZyWALL is labeled **A**, the gateway is labeled **B** and the backup gateway is labeled **C**.

**Figure 46** Traffic Redirect LAN Setup



## 7.9 Configuring Traffic Redirect

To change your ZyWALL's traffic redirect settings, click **NETWORK > WAN > Traffic Redirect**. The screen appears as shown.

**Figure 47** Traffic Redirect

The screenshot shows the 'Traffic Redirect' configuration page. At the top, there are four tabs: 'Route', 'WAN', 'Traffic Redirect', and 'Dial Backup'. The 'Traffic Redirect' tab is selected. Below the tabs, there is a 'Traffic Redirect' section. It starts with an 'Active' checkbox, which is currently unchecked. Below this are several input fields: 'Backup Gateway IP Address' with the value '0 . 0 . 0 . 0', 'Check WAN IP Address' with the value '0 . 0 . 0 . 0', 'Fail Tolerance' with the value '2', 'Period' with the value '5' and '(Seconds)' to its right, and 'Timeout' with the value '3' and '(Seconds)' to its right. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 32** 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).
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.

## 7.10 Configuring Dial Backup

The dial backup port can be used in reserve for a traditional dial-up connection through an external analog modem if the WAN and traffic redirect connections fail.

Click **NETWORK > WAN > Dial Backup** to display the **Dial Backup** screen. Use this screen to configure the backup WAN dial-up connection.

**Figure 48** Dial Backup

**WAN**

Route    WAN    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 33** 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 33** 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 33** 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.

## 7.11 Advanced Modem Setup

### 7.11.1 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.

### 7.11.2 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`.

### 7.11.3 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.

## 7.12 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 49** Advanced Setup

**WAN - ADVANCED MODEM SETUP**

**AT Command Strings**

Dial: atdt

Drop: ~~~+++~ath

Answer: ata

Drop DTR When Hang Up

**AT Response Strings**

CLID: NMBR =

Called ID:

Speed: CONNECT

**Call Control**

Dial Timeout (sec): 60

Retry Count: 0

Retry Interval (sec): 10

Drop Timeout (sec): 20

Call Back Delay (sec): 15

Apply Cancel

The following table describes the labels in this screen.

**Table 34** 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 34** 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

## Firewall Screens

This chapter shows you how to configure your ZyWALL's firewall.

### 8.1 Firewall Overview

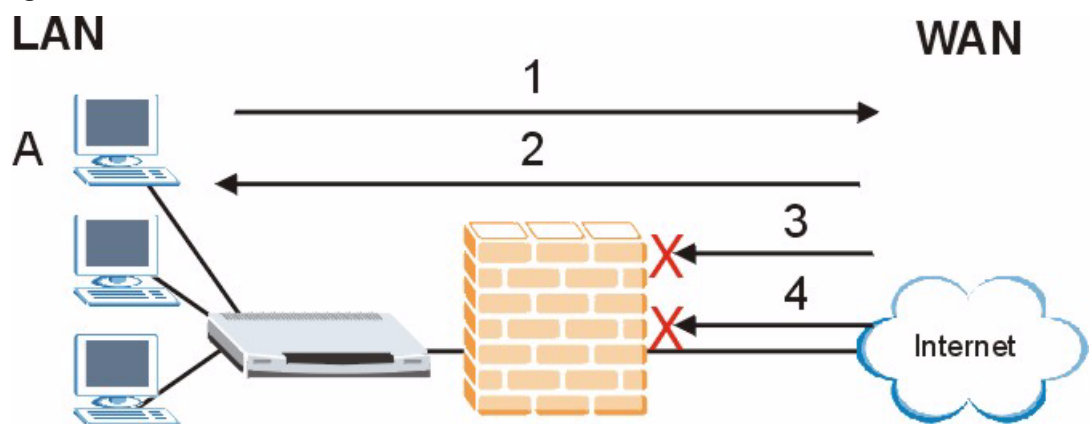
The networking term firewall is a system or group of systems that enforces an access-control policy between two networks. It is generally a mechanism used to protect a trusted network from an untrusted network.

The ZyWALL physically separates your private Local Area Network (LAN) of computers from the WAN (Wide Area Network) connection to the Internet and acts as a secure gateway for all data passing between the two networks. The ZyWALL protects against Denial of Service (DoS) attacks, prevents theft, destruction and modification of data, and logs events.

- Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN.
- By default the firewall allows traffic that originates from your LAN computers and blocks traffic that originates from the WAN.
- You should only need to configure firewall rules if you want to restrict what the LAN computers can access or allow access from the WAN.

The following figure illustrates the default firewall action. User A can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

**Figure 50** Default Firewall Action



Your customized rules take precedence and override the ZyWALL's default settings. The ZyWALL checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyWALL takes the action specified in the rule.

## 8.2 Firewall Connection Directions

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

By default, the ZyWALL allows packets traveling in the following directions.:

- LAN to LAN/ ZyWALL These rules specify which computers on the LAN can manage the ZyWALL and communicate between networks or subnets connected to the LAN interface.

**Note:** You can also configure the remote management settings to allow only a specific computer to manage the ZyWALL.

- LAN to WAN These rules specify which computers on the LAN can access which computers or services on the WAN. See [Section 8.4 on page 133](#) for an example.

By default, the ZyWALL drops packets traveling in the following directions.

- WAN to LAN These rules specify which computers on the WAN can access which computers or services on the LAN. For example, you may create rules to:
  - Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
  - Allow public access to a Web server on your protected network. You could also block certain IP addresses from accessing it.

**Note:** You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN. See [Section 14.5.3 on page 258](#) for an example.

- WAN to WAN/ ZyWALL By default the ZyWALL stops WAN computers from managing the ZyWALL or using the ZyWALL as a gateway to communicate with other computers on the WAN. You could configure one of these rules to allow a WAN computer to manage the ZyWALL.

**Note:** You also need to configure the remote management settings to allow a WAN computer to manage the ZyWALL.

## 8.3 Security Considerations

**Note:** Incorrectly configuring the firewall may block valid access or introduce security risks to the ZyWALL and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

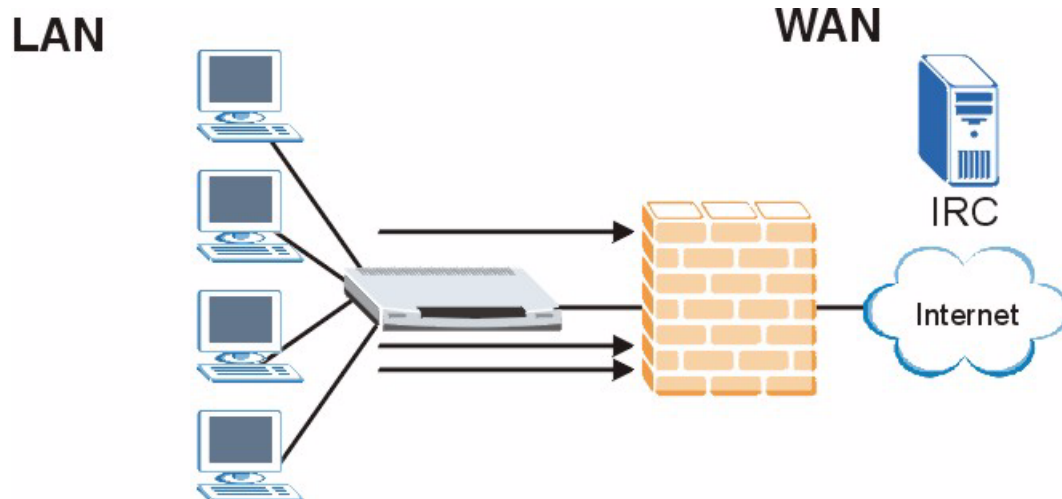
- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain 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 entering the information into the correct fields in the web configurator screens.

## 8.4 Firewall Rules Example

Suppose that your company decides to block all of the LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN firewall rule that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the firewall rule to always be in effect. The following figure shows the results of this rule.

**Figure 51** Blocking All LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

**Table 35** Blocking All LAN to WAN IRC Traffic Example

#	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	IRC	Drop
Default	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the firewall's default policy that allows all traffic from the LAN to go to the WAN.

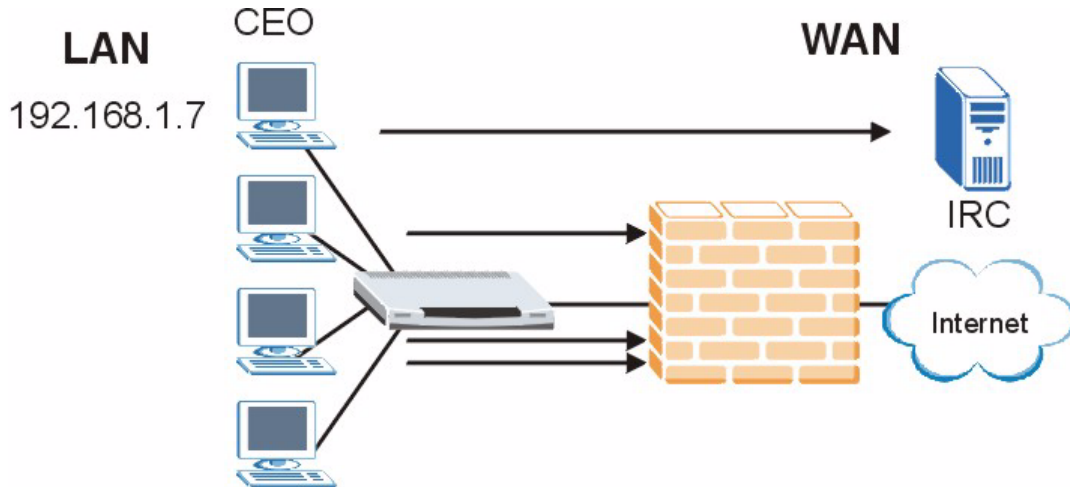
The ZyWALL applies the firewall rules in order. So for this example, when the ZyWALL receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that does not match the first firewall rule will match the default rule and the ZyWALL forwards it.

Now suppose that your company wants to let the CEO use IRC. You can configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

- has a static IP address,
- or you configure a static DHCP entry for it so the ZyWALL always assigns it the same IP address (see [Section 5.8 on page 98](#) for information on static DHCP).

Now you configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer (192.168.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the firewall rule to always be in effect. The following figure shows the results of your two custom rules.

**Figure 52** Limited LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

**Table 36** Limited LAN to WAN IRC Traffic Example

#	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	192.168.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	IRC	Drop
Default	Any	Any	Any	Any	Allow

- The first row allows the LAN computer at IP address 192.168.1.7 to access the IRC service on the WAN.
- The second row blocks LAN access to the IRC service on the WAN.
- The third row is (still) the firewall's default policy of allowing all traffic from the LAN to go to the WAN.

The rule for the CEO must come before the rule that blocks all LAN to WAN IRC traffic. If the rule that blocks all LAN to WAN IRC traffic came first, the CEO's IRC traffic would match that rule and the ZyWALL would drop it and not check any other firewall rules.

## 8.5 Firewall Default Rule (Router Mode)

Click **SECURITY > FIREWALL** to open the **Default Rule** screen. Use this screen to configure general firewall settings when the ZyWALL is set to router mode.

**Figure 53** 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 and WAN to WAN 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"/>
WAN to LAN	Drop	<input checked="" type="checkbox"/>
WAN to WAN / ZyWALL	Drop	<input checked="" type="checkbox"/>

Apply      Reset

The following table describes the labels in this screen.

**Table 37** 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	<p>If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged.</p> <p>Select this check box to have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection).</p> <p><b>Note:</b> Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use IP alias to put the ZyWALL and the backup gateway on separate subnets. See <a href="#">Section 8.13 on page 149</a> for an example.</p>
Packet Direction	<p>This is the direction of travel of packets.</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>Select the default action to take on packets that are traveling in the selected direction and do not match any of the firewall rules.</p> <p>Select <b>Drop</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select <b>Reject</b> to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.</p> <p>Select <b>Permit</b> to allow the passage of the packets.</p>
Log	Select the check box to create a log when the above action is taken.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.6 Firewall Default Rule (Bridge Mode)

Click **SECURITY > FIREWALL** to open the **Default Rule** screen. Use this screen to configure general firewall settings when the ZyWALL is set to bridge mode.



**Figure 54** Default Rule (Bridge Mode)

**FIREWALL**

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

Default Rule Setup

Enable Firewall

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

Apply | Reset

The following table describes the labels in this screen.

**Table 38** Default Rule (Bridge Mode)

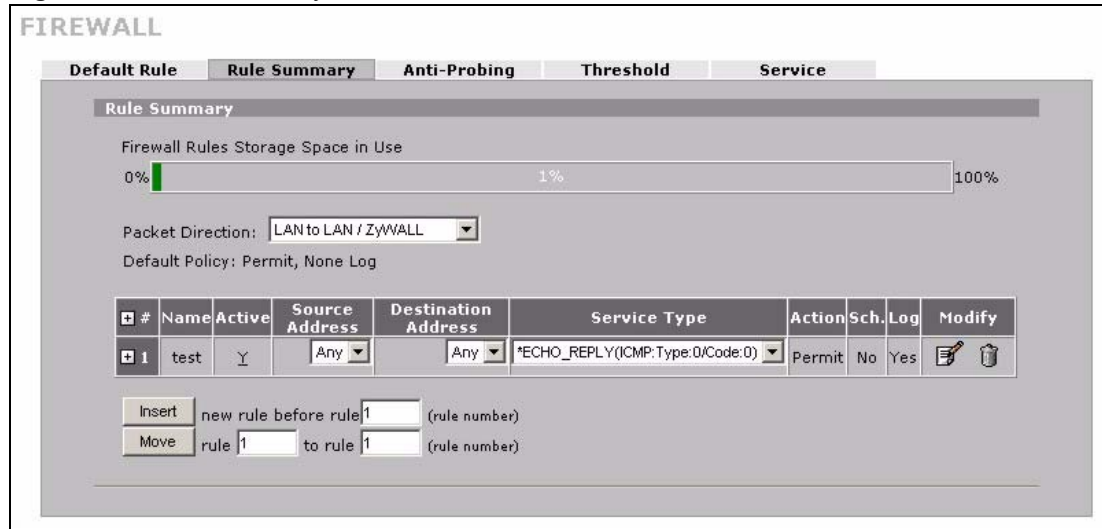
LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Packet Direction	This is the direction of travel of packets. Firewall rules are grouped based on the 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	Select the default action to take on packets that are traveling in the selected direction and do not match any of the firewall rules. Select <b>Drop</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select <b>Reject</b> to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select <b>Permit</b> to allow the passage of the packets.
Log	Select the check box to create a log when the above action is taken.
Log Broadcast Frame	Select the check box to create a log for any broadcast frames traveling in the selected direction. Many of these logs in a short time period could indicate a broadcast storm. A broadcast storm occurs when a packet triggers multiple responses from all hosts on a network or when computers attempt to respond to a host that never replies. As a result, duplicated packets are continuously created and circulated in the network, thus reducing network performance or even rendering it inoperable. A broadcast storm can be caused by an attack on the network, an incorrect network topology (such as a bridge loop) or a malfunctioning network device.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.7 Firewall Rule Summary

Click **SECURITY > FIREWALL > Rule Summary** 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 the order that they are listed.

**Figure 55** Rule Summary



The following table describes the labels in this screen.

**Table 39** 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 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.
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> .

**Table 39** Rule Summary

LABEL	DESCRIPTION
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="#">Appendix E on page 541</a> for a list of common services.
Action	This field displays whether the firewall silently discards packets ( <b>Drop</b> ), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender ( <b>Reject</b> ) or allows 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.

## 8.7.1 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 56** 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: 60px; margin-top: 10px;"></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 40** 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> .
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	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 <<. Next to the name of a service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type). For example, look at the DNS entry, (UDP/TCP:53) means UDP port 53 and TCP port 53. Click the <b>Service</b> link to go to the <b>Service</b> screen where you can configure custom service ports. See <a href="#">Appendix E on page 541</a> for a list of commonly used services and port numbers.
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.

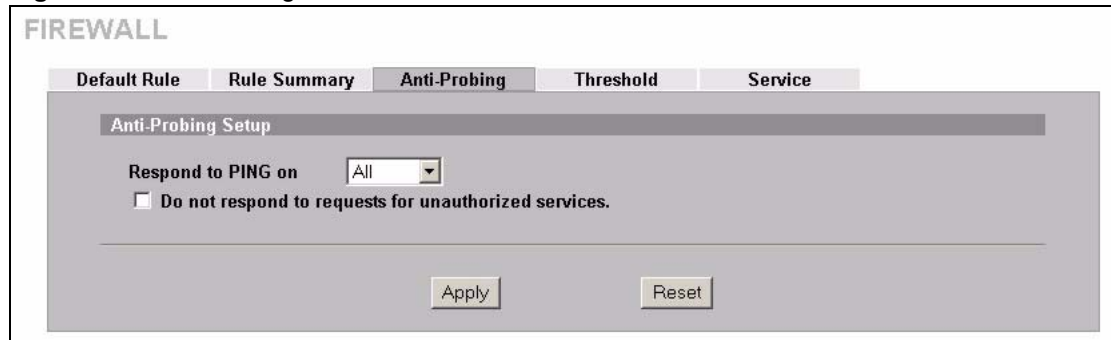
**Table 40** Firewall Edit Rule

LABEL	DESCRIPTION
Action for Matched Packets	<p>Use the drop-down list box to select what the firewall is to do with packets that match this rule.</p> <p>Select <b>Drop</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select <b>Reject</b> to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.</p> <p>Select <b>Permit</b> to allow the passage of the packets.</p> <p><b>Note:</b> You also need to configure NAT port forwarding (or full featured NAT address mapping rules) if you want to allow computers on the WAN to access devices on the LAN.</p> <p><b>Note:</b> You may also need to configure the remote management settings if you want to allow a WAN computer to manage the ZyWALL or restrict management from the LAN.</p>
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.

## 8.8 Anti-Probing

Click **SECURITY > FIREWALL > Anti-Probing** to open the following screen. Configure this screen to help keep the ZyWALL hidden from probing attempts. You can specify which of the ZyWALL's interfaces will respond to Ping requests and whether or not the ZyWALL is to respond to probing for unused ports.

**Figure 57** Anti-Probing



The following table describes the labels in this screen.

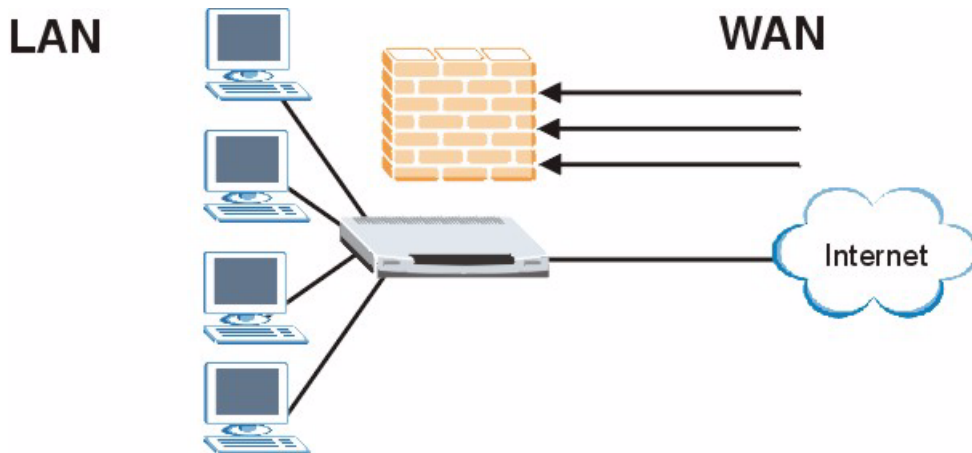
**Table 41** Anti-Probing

LABEL	DESCRIPTION
Respond to PING on	Select the interface that you want to reply to incoming Ping requests. Select <b>Disable</b> to have the ZyWALL not respond to any incoming 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. If this option is not selected, 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 rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the ZyWALL reacts based on the firewall rule to either 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.

## 8.9 Denial of Service Attacks

Denial 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 currently known DoS attacks.

**Figure 58** ZyWALL Firewall Application

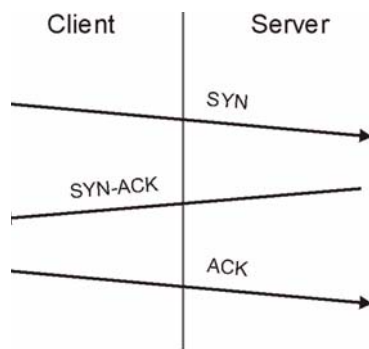


## 8.10 Firewall Thresholds

For DoS attacks, the ZyWALL uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all 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. 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.

**Figure 59** Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.

### 8.10.1 Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the ZyWALL has been receiving DoS attacks that are not recorded in the logs or the logs show that the ZyWALL is classifying normal traffic as DoS attacks. 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.

Reduce the threshold values 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).



If you often use P2P applications such as file sharing with eMule or eDonkey, 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 classify them as DoS attacks.

## 8.11 Threshold Screen

Click **SECURITY > FIREWALL > Threshold** to bring up the next screen. The global values specified for the threshold and timeout apply to all TCP connections.

**Figure 60** Firewall Threshold

**FIREWALL**

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

Disable DoS Attack Protection on  WAN  LAN

**Denial of Service Thresholds**

One Minute Low  sessions per minute  
 One Minute High  sessions per minute  
 Maximum Incomplete Low  sessions  
 Maximum Incomplete High  sessions  
 TCP Maximum Incomplete  sessions

**Action taken when TCP Maximum Incomplete reached threshold**

Delete the oldest half open session when new connection request comes.  
 Deny new connection request for  (1~256 minutes)

Apply Reset

The following table describes the labels in this screen.

**Table 42** 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	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.
One Minute Low	This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.

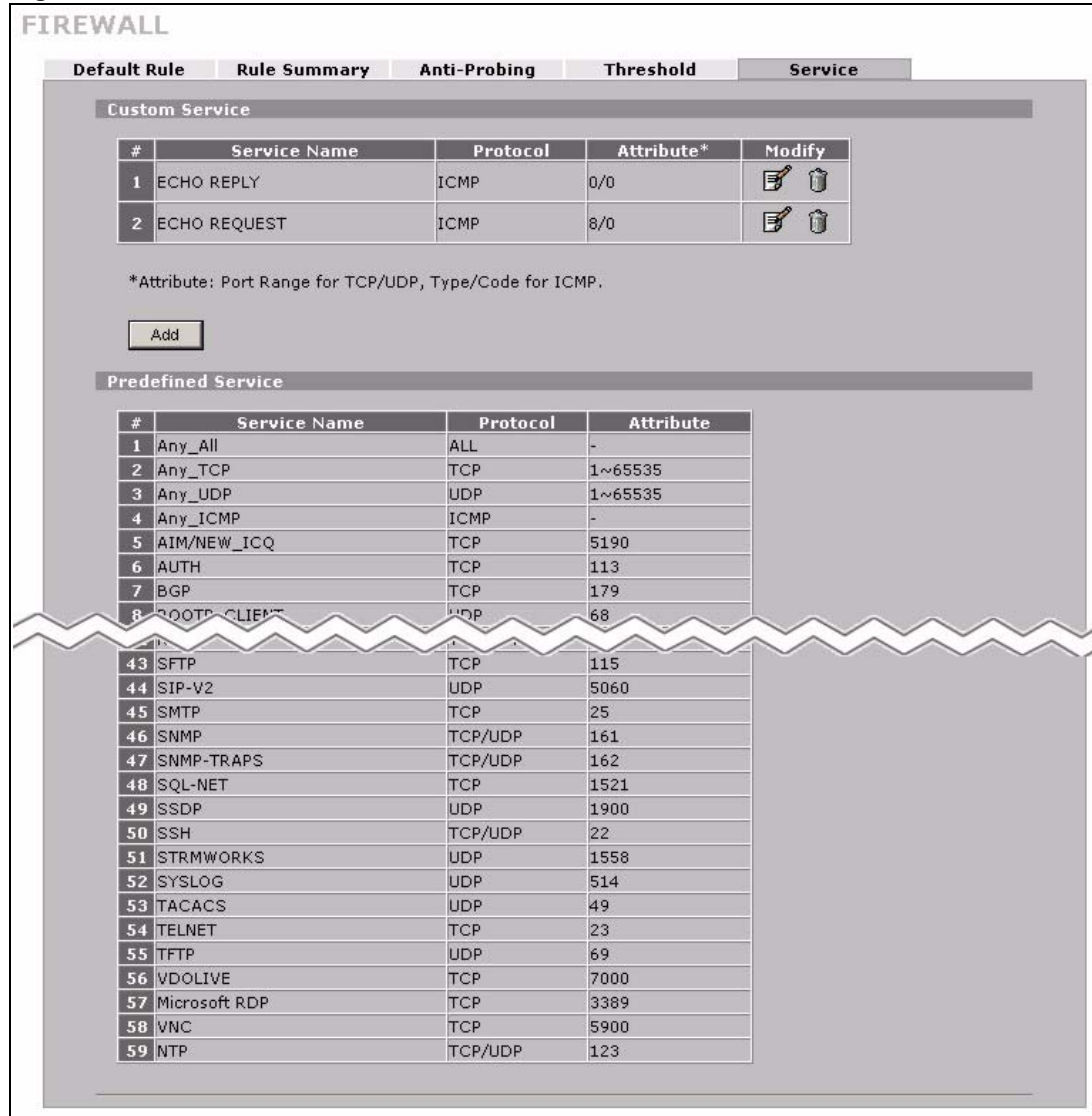
**Table 42** Firewall Threshold (continued)

LABEL	DESCRIPTION
One Minute High	<p>This is the rate of new half-open sessions per minute 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.</p> <p>For example, if you set the one minute high to 100, the ZyWALL starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low.</p>
Maximum Incomplete Low	<p>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.</p>
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>For example, if you set the maximum incomplete high to 100, the ZyWALL starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low.</p>
TCP Maximum Incomplete	<p>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.</p> <p>Specify 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. The ZyWALL sends alerts whenever the <b>TCP Maximum Incomplete</b> is exceeded.</p> <p>You also need to select the action that ZyWALL should take when the TCP maximum incomplete threshold is reached. You can have the ZyWALL either:</p> <p>Delete the oldest half open session when a new connection request comes.</p> <p>or</p> <p>Deny new connection requests for a the number of minutes that you specify (between 1 and 256).</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.

## 8.12 Service

Click **SECURITY > FIREWALL**, then the **Service** 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 61** Firewall Service



The following table describes the labels in this screen.

**Table 43** 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.

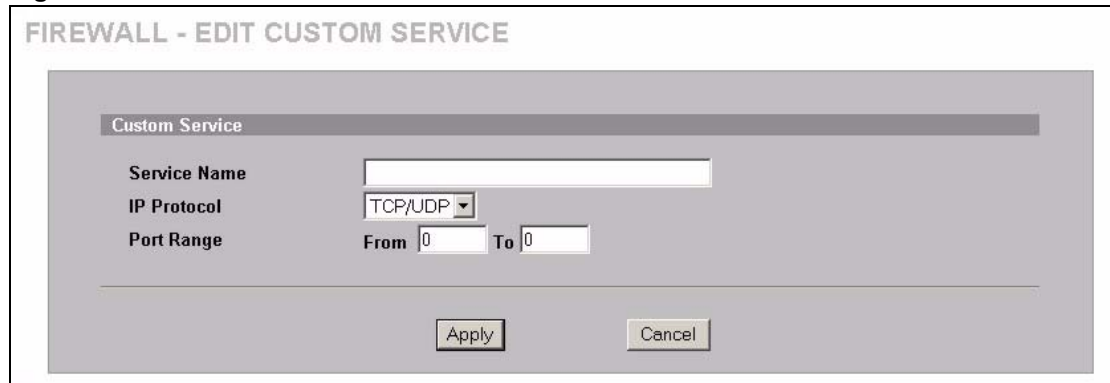
**Table 43** Firewall Service

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="#">Appendix E on page 541</a> for a list of common 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.

### 8.12.1 Firewall Edit Custom Service

Click the **Add** button under **Custom Service** to display the following screen. Use this screen to configure a custom service entry not is not predefined in the ZyWALL. See [Appendix E on page 541](#) for a list of commonly used services and port numbers.

**Figure 62** Firewall Edit Custom Service



The following table describes the labels in this screen.

**Table 44** Firewall Edit Custom Service

LABEL	DESCRIPTION
Service Name	Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the custom service. You cannot use the "(" character. Spaces are allowed.
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 44** 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.

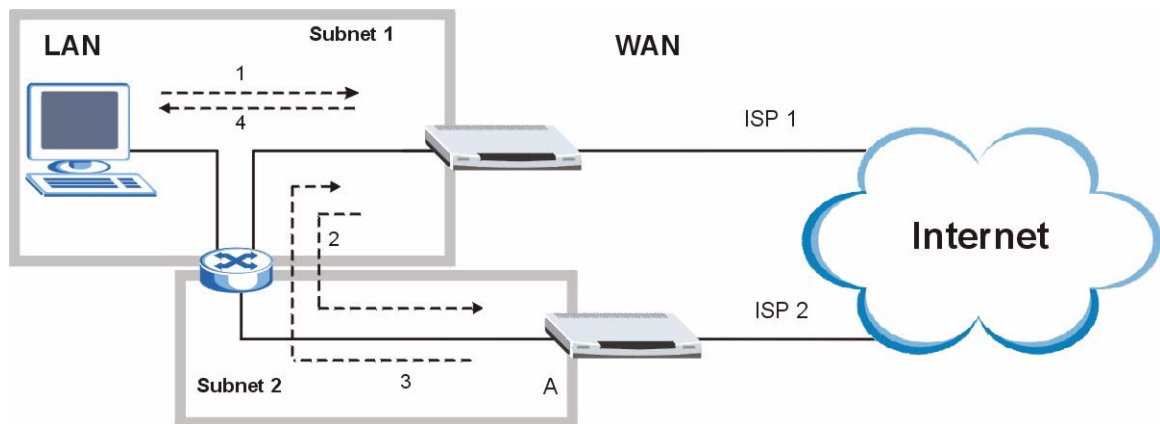
## 8.13 Solving the Asymmetrical Route Problem Example

If you have the ZyWALL allow asymmetrical route sessions, traffic from the WAN can go directly to a LAN computer without passing through the ZyWALL and its firewall protection.

Another solution is to use IP alias. 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.

This essentially lets you have multiple LAN networks on the same physical cables and ports. By putting your LAN and Gateway A 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 A, which is in Subnet 2.
- 3 The reply from the WAN goes to the ZyWALL.
- 4 The ZyWALL then sends it to the computer on the LAN in Subnet 1.

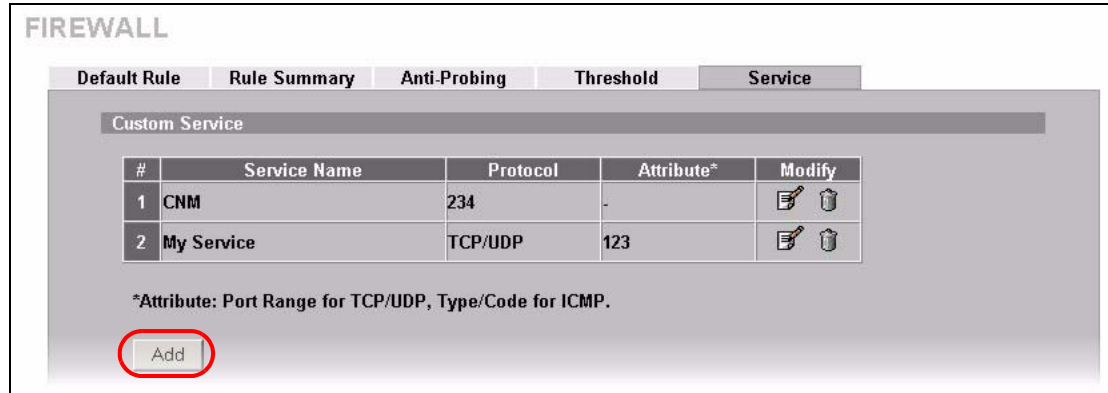
**Figure 63** IP Alias

## 8.14 My Service Firewall Rule Example

The following Internet firewall rule example allows a hypothetical My Service connection from the Internet.

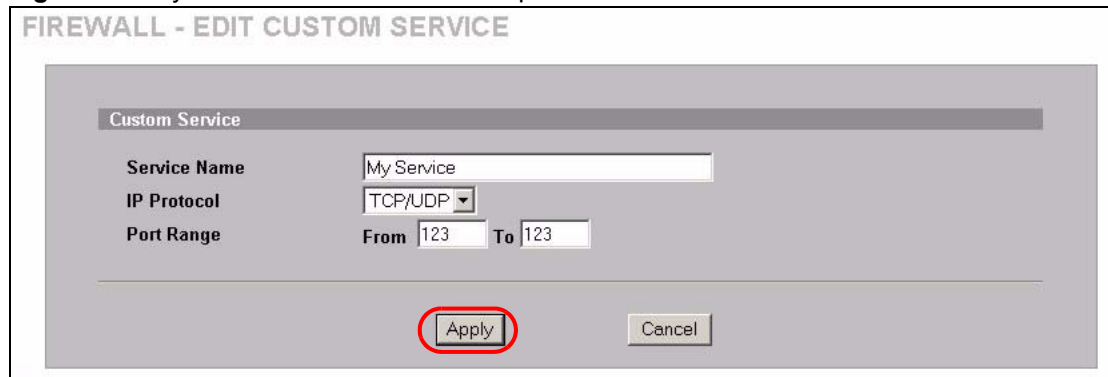
- 1 In the **Service** screen, click **Add** to open the **Edit Custom Service** screen.

**Figure 64** My Service Firewall Rule Example: Service



- 2 Configure it as follows and click **Apply**.

**Figure 65** My Service Firewall Rule Example: Edit Custom Service



- 3 Click **Rule Summary**. 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 66** My Service Firewall Rule 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	W2L_Rule_1	N	Any	Any	BOOTP_CLIENT(UDP:68)	Permit	No	No	
2	W2L_Rule_2	N	Any	Any	NetBIOS(TCP/UDP:137~139,445)	Permit	No	No	

Insert new rule before rule 1 (rule number)  
Move rule 1 to rule 1 (rule number)

- 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 fields as follows and click **Add**.

**Figure 67** My Service Firewall Rule Example: Rule Edit

**FIREWALL - EDIT RULE**

Rule Name: Ex1

**Edit Source Address**

Address Editor  
Address Type: Any Address  
Start IP Address: 0 . 0 . 0 . 0  
End IP Address: 0 . 0 . 0 . 0  
Subnet Mask: 0 . 0 . 0 . 0  
Add Modify

Source Address(es): Any  
Delete

**Edit Destination Address**

Address Editor  
Address Type: Range Address  
Start IP Address: 10 . 0 . 0 . 10  
End IP Address: 10 . 0 . 0 . 15  
Subnet Mask: 0 . 0 . 0 . 0  
Add Modify

Destination Address(es):  
Delete

- 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 68** My Service Firewall Rule Example: 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



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.

**Figure 69** My Service Firewall Rule 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 1 (rule number)

Move rule 1 to rule 1 (rule number)



# CHAPTER 9

## Content Filtering Screens

This chapter provides an overview of content filtering.

### 9.1 Content Filtering Overview

Content filtering allows you to block web features such as ActiveX controls, Java applets and cookies and disable web proxies. The ZyWALL can block or allow access to web sites that you specify. It 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.

#### 9.1.1 Restrict Web Features

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

#### 9.1.2 Create a Filter List

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

#### 9.1.3 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.

### 9.2 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 70** Content Filter: General

The following table describes the labels in this screen.

**Table 45** Content Filter: General

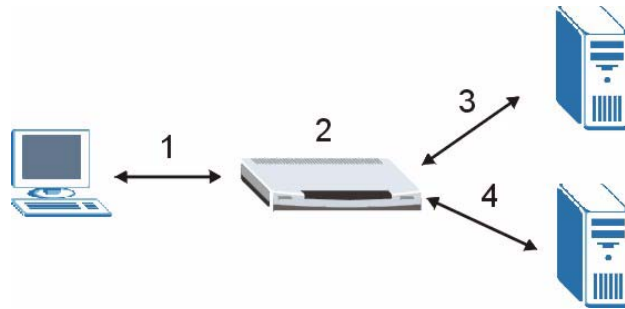
LABEL	DESCRIPTION
General Setup	
Enable Content Filter	Select this check box to enable the content filter.
Restrict Web Features	Select the check box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
Block ActiveX	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 45** 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.

### 9.3 Category Based Content Filtering

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 71** 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 9.7 on page 168](#)). 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.

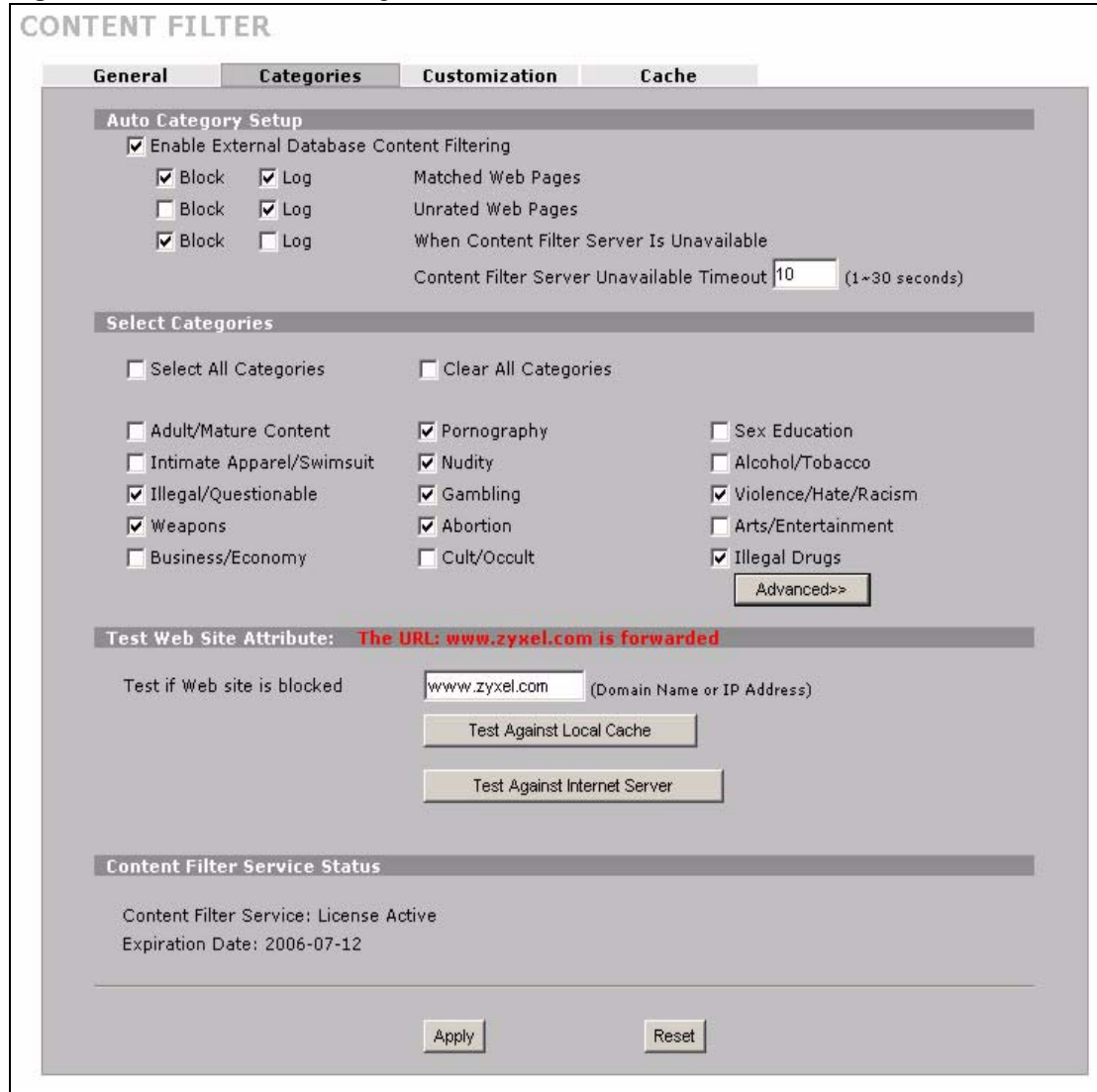
## 9.4 Content Filter Categories

Click **SECURITY > CONTENT FILTER > Categories** 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 89](#)) 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 10 on page 171](#) 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 77 on page 173](#)). Type your myZyXEL.com account password in the **Password** field. Click **Submit**.

**Figure 72** Content Filter: Categories



The following table describes the labels in this screen.

**Table 46** 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 46** 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 46** Content Filter: Categories (continued)

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

**Table 46** 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 46** 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 46** 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 10.1 on page 171</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.

## 9.5 Content Filter Customization

Click **SECURITY > CONTENT FILTER > Customization** 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 73** Content Filter: Customization

The screenshot displays the 'CONTENT FILTER' configuration page, specifically the 'Customization' tab. It is divided into three main sections: 'Web Site List Customization', 'Forbidden Web Site List', and 'Keyword Blocking'. Each section includes an 'Add' button and a 'Delete' button. The 'Trusted Web Sites' list contains 'www.zyxel.com.tw'. The 'Forbidden Web Sites' list contains 'www.playboy.com'. The 'Keyword List' contains 'bad' and 'sex'. At the bottom, there are 'Apply' and 'Reset' buttons.

**CONTENT FILTER**

General Categories **Customization** Cache

**Web Site List Customization**

Enable Web site customization.

Disable all Web traffic except for trusted Web sites.

Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites.

**Trusted Web Sites**

Add Trusted Web Site

Trusted Web Sites

www.zyxel.com.tw

Add Delete

**Forbidden Web Site List**

Add Forbidden Web Site

Forbidden Web Sites

www.playboy.com

Add Delete

**Keyword Blocking**

Block Web sites which contain these keywords.

Add Keyword

Keyword List

bad  
sex

Add Delete

Apply Reset

The following table describes the labels in this screen.

**Table 47** 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 9.6 on page 167</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 47** 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.

## 9.6 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.

### 9.6.1 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).

### 9.6.2 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.

### 9.6.3 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.

## 9.7 Content Filtering Cache

Click **SECURITY > CONTENT FILTER > Cache** 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 10.3 on page 176](#) for how to submit a web site that has been incorrectly categorized.

**Figure 74** 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 48** 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 10

## 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 89](#) on how to create a myZyXEL.com account, register your device and activate the subscription services using the **REGISTRATION** screens.

### 10.1 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.

### 10.2 Viewing Content Filtering Reports

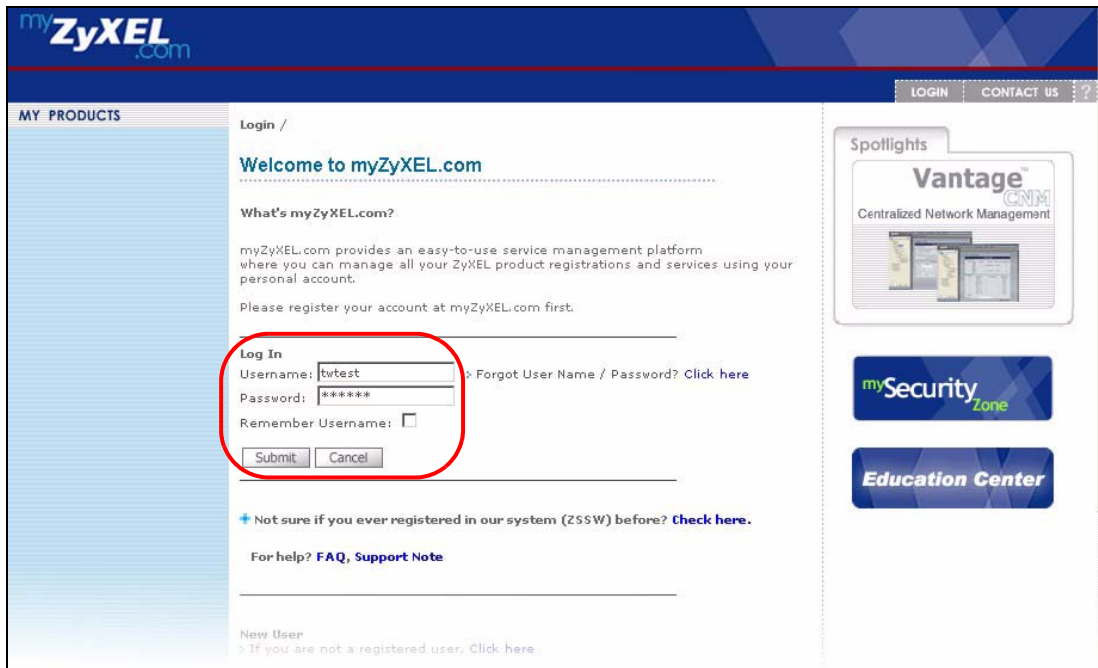
Content filtering reports are generated statistics and charts of access attempts to web sites belonging to the categories you selected in your device content filter screen.

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).

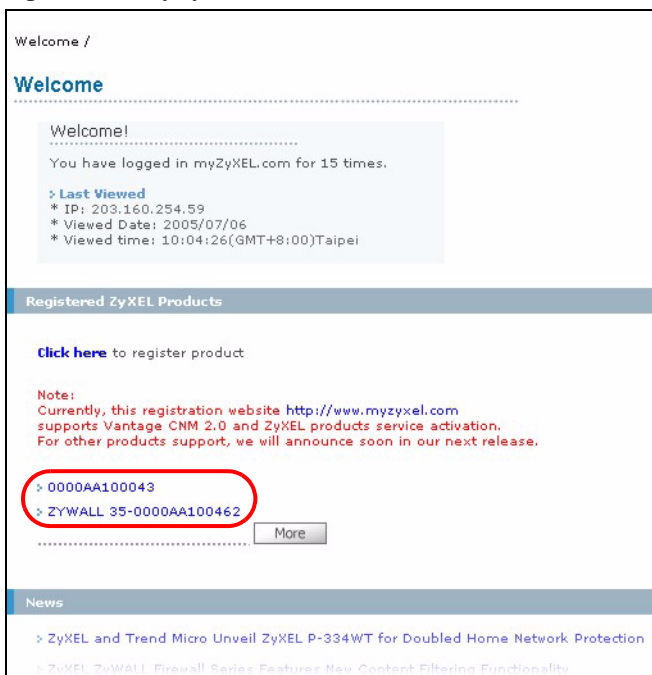
- 1 Go to <http://www.myZyXEL.com>.
- 2 Fill in your myZyXEL.com account information and click **Submit**.

**Figure 75** 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 77](#) on page 173).

**Figure 76** 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 77** 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 77 on page 173). Type your myZyXEL.com account password in the **Password** field.

**6** Click **Submit**.

**Figure 78** Blue Coat: Login

**ZyXEL** Powered By **Blue Coat** Technical Support

**System Login**

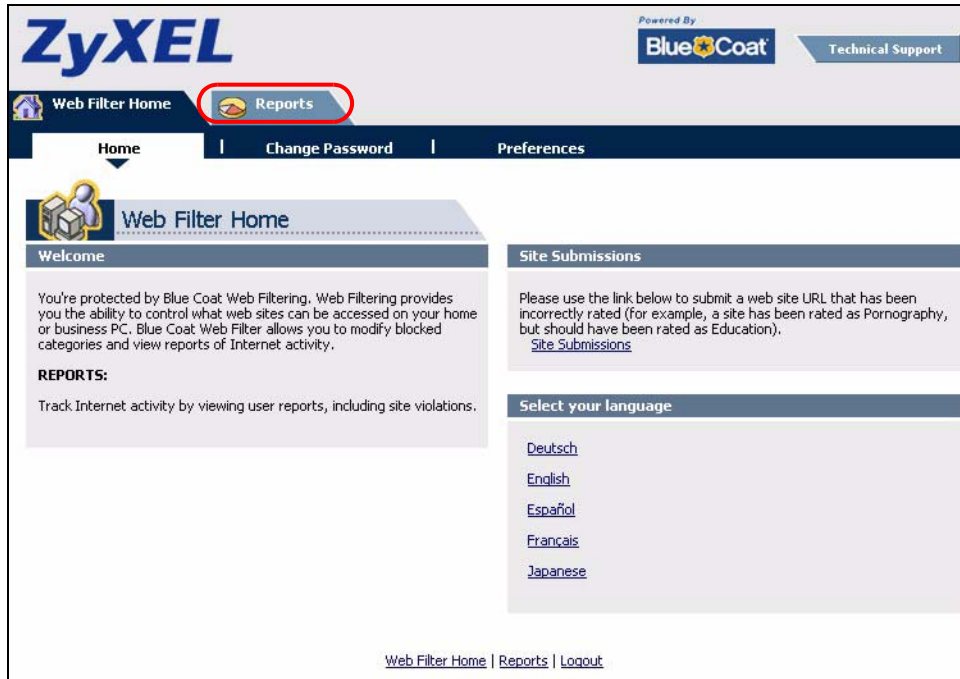
Welcome to your Blue Coat Web Filter Administration site. Please login using your Username and Password.

**Name**

**Password**

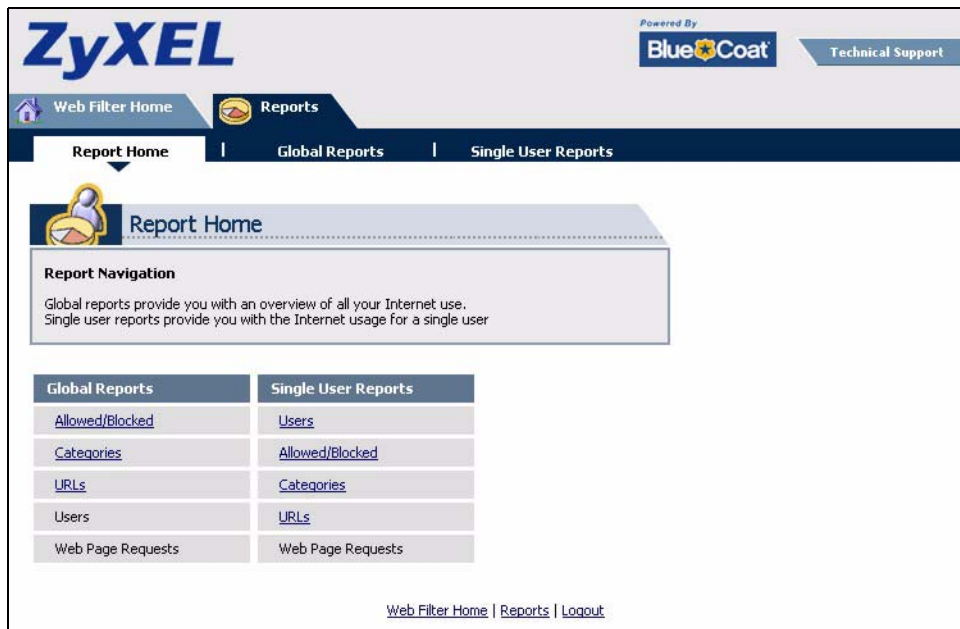
**7** In the **Web Filter Home** screen, click **Reports**.

**Figure 79** Content Filtering Reports Main Screen



**8** Select items under **Global Reports** or **Single User Reports** to view the corresponding reports.

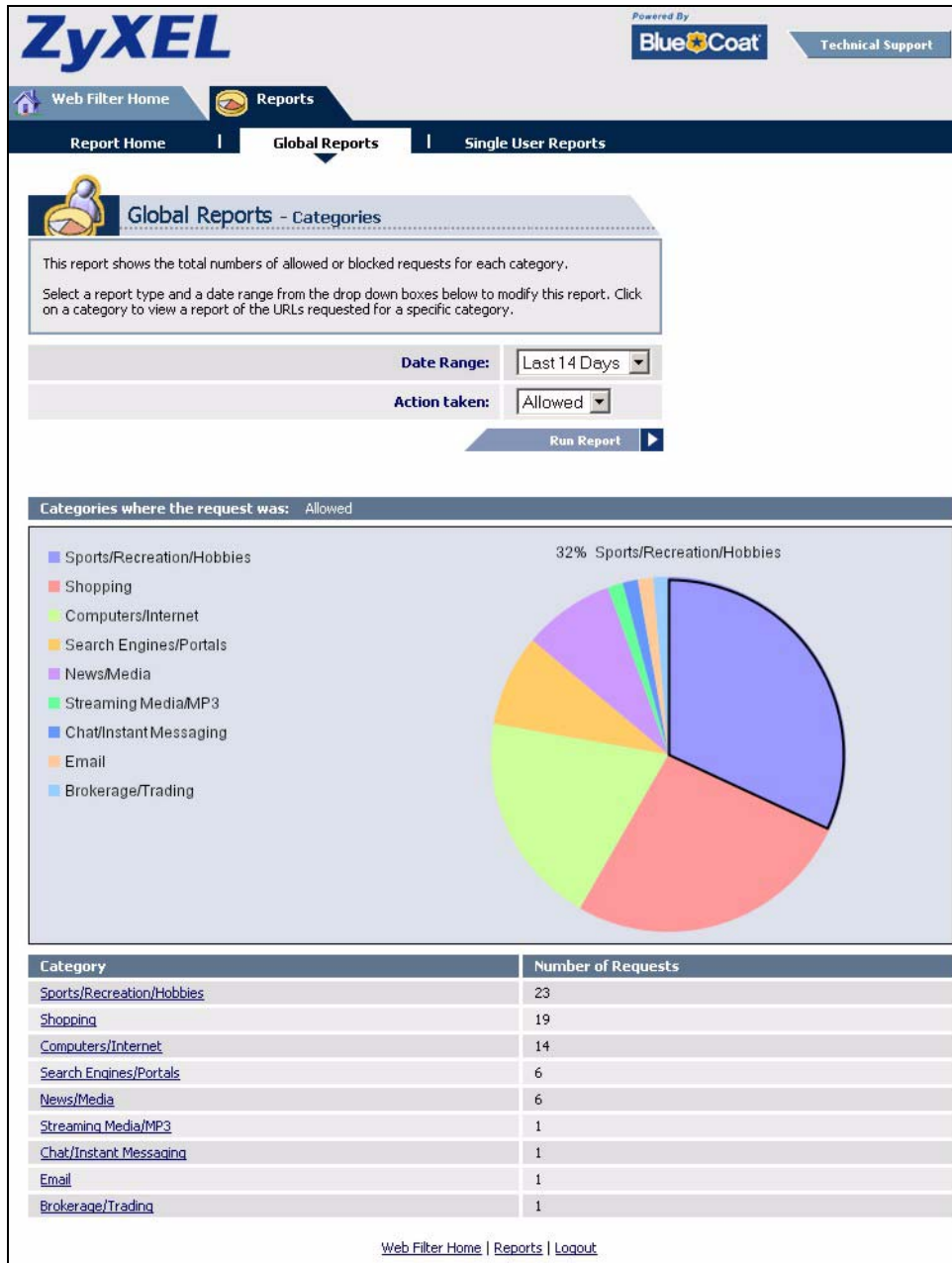
**Figure 80** Blue Coat: Report Home



**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 81 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 82 Requested URLs Example

The screenshot shows the ZyXEL Web Filter Home interface. The top navigation bar includes 'Web Filter Home', 'Reports', 'Report Home', 'Global Reports', and 'Single User Reports'. The main content area is titled 'Global Reports - URLs' and includes a description: 'This report displays allowed or blocked URLs requested within a specific category. Click on a URL to view the users that requested that URL.' Below this are filter options: 'Date Range' (Last 14 Days), 'Action taken' (Allowed), and 'Category' (Sports/Recreation/Hobbies). A 'Run Report' button is located to the right of the filters.

The table below shows the results of the report for the category 'Sports/Recreation/Hobbies'.

Item #	URL	Number of Requests	Open Web Page
1	<a href="http://adsatt.espn.go.com/insertfiles/javascript/flash.js">adsatt.espn.go.com/insertfiles/javascript/flash.js</a>	1	
2	<a href="http://sports.espn.go.com/crossdomain.xml">sports.espn.go.com/crossdomain.xml</a>	1	
3	<a href="http://sports.espn.go.com/sports/tvlistings/fp/headerData">sports.espn.go.com/sports/tvlistings/fp/headerData</a>	1	
4	<a href="http://espn.go.com/Adserver?CallDown&amp;AdTypes=MotionLogo;">espn.go.com/Adserver?CallDown&amp;AdTypes=MotionLogo;</a>	1	
5	<a href="http://espn.go.com/myespn/login3.html">espn.go.com/myespn/login3.html</a>	1	
6	<a href="http://broadband.espn.go.com/EBB2/popup">broadband.espn.go.com/EBB2/popup</a>	1	
7	<a href="http://sports-alt.espn.go.com/espn/format/sponsoredLinkSpot_redesign3">sports-alt.espn.go.com/espn/format/sponsoredLinkSpot_redesign3</a>	1	
8	<a href="http://sports.espn.go.com/espn/fp/pollData">sports.espn.go.com/espn/fp/pollData</a>	1	
9	<a href="http://sports.espn.go.com/espn/util/encodeLess?id=1878300">sports.espn.go.com/espn/util/encodeLess?id=1878300</a>	1	
10	<a href="http://sports.espn.go.com/espn/util/encodeLess?id=1872951">sports.espn.go.com/espn/util/encodeLess?id=1872951</a>	1	
11	<a href="http://sports.espn.go.com/espn/fp/pollDataJS">sports.espn.go.com/espn/fp/pollDataJS</a>	1	
12	<a href="http://static.espn.go.com/swf/fp/superheadline.swf?h=Spur-fect+Ending&amp;tex">static.espn.go.com/swf/fp/superheadline.swf?h=Spur-fect+Ending&amp;tex</a>	1	
13	<a href="http://espn.go.com">espn.go.com</a>	1	
14	<a href="http://wimbledon.org/includes/js/external_sb.js">wimbledon.org/includes/js/external_sb.js</a>	1	
15	<a href="http://espn.go.com/swf/header2005/headers/mlb_hdr.swf">espn.go.com/swf/header2005/headers/mlb_hdr.swf</a>	1	
16	<a href="http://espn.go.com/swf/header2005/search/searchBar.swf">espn.go.com/swf/header2005/search/searchBar.swf</a>	1	
17	<a href="http://sports.espn.go.com/mlb/xml/upcomingTV?sport=mlb">sports.espn.go.com/mlb/xml/upcomingTV?sport=mlb</a>	1	
18	<a href="http://espn.go.com/insertfiles/javascript/horizNav.js">espn.go.com/insertfiles/javascript/horizNav.js</a>	1	
19	<a href="http://sports.espn.go.com/mlb/index">sports.espn.go.com/mlb/index</a>	1	
20	<a href="http://espn.go.com/swf/header2005/tvschedule/tvschedule.swf">espn.go.com/swf/header2005/tvschedule/tvschedule.swf</a>	1	
21	<a href="http://espn-i.starwave.com/media/apphoto/WATW11606230650_thumbnail.jpeg">espn-i.starwave.com/media/apphoto/WATW11606230650_thumbnail.jpeg</a>	1	
22	<a href="http://espn.starwave.com/insertfiles/javascript/motion/motion_index_02.js">espn.starwave.com/insertfiles/javascript/motion/motion_index_02.js</a>	1	
23	<a href="http://sports.espn.go.com/espn/fp/pollDataGen?id=30688">sports.espn.go.com/espn/fp/pollDataGen?id=30688</a>	1	

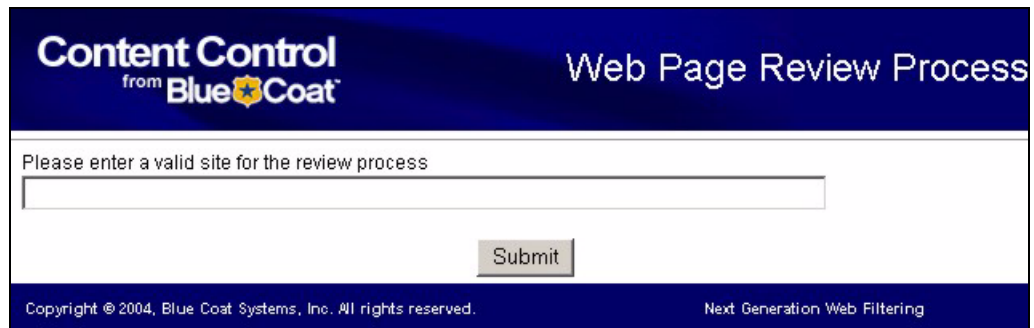
At the bottom of the page, there are links for 'Web Filter Home | Reports | Logout'.

## 10.3 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 10.2 on page 171](#)).
- 2 In the **Web Filter Home** screen (see [Figure 79 on page 174](#)), click **Site Submissions** to open the **Web Page Review Process** screen shown next.



**Figure 83** Web Page Review Process Screen

Content Control  
from Blue Coat

Web Page Review Process

Please enter a valid site for the review process

Submit

Copyright © 2004, Blue Coat Systems, Inc. All rights reserved. Next Generation Web Filtering

- 3 Type the web site's URL in the field and click **Submit** to have the web site reviewed.



# CHAPTER 11

## IPSec VPN

This chapter explains how to set up and maintain IPSec VPNs in the ZyWALL.

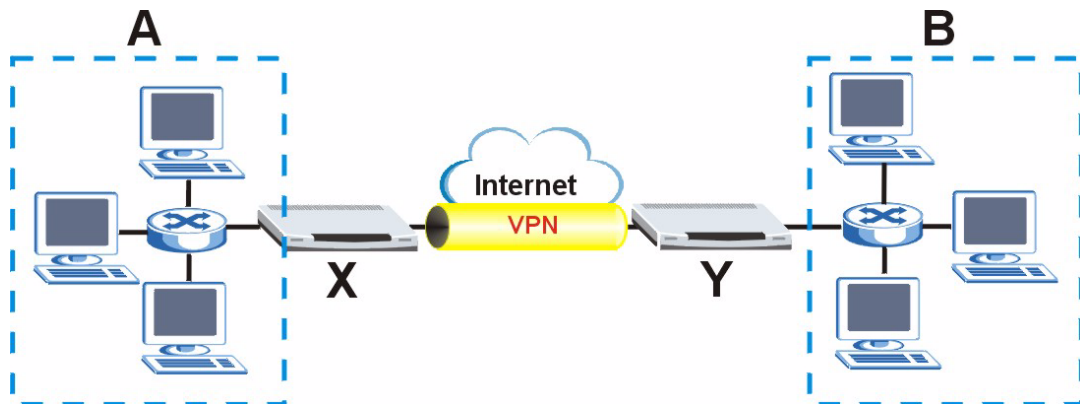
### 11.1 IPSec VPN Overview

A virtual private network (VPN) 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, used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

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.

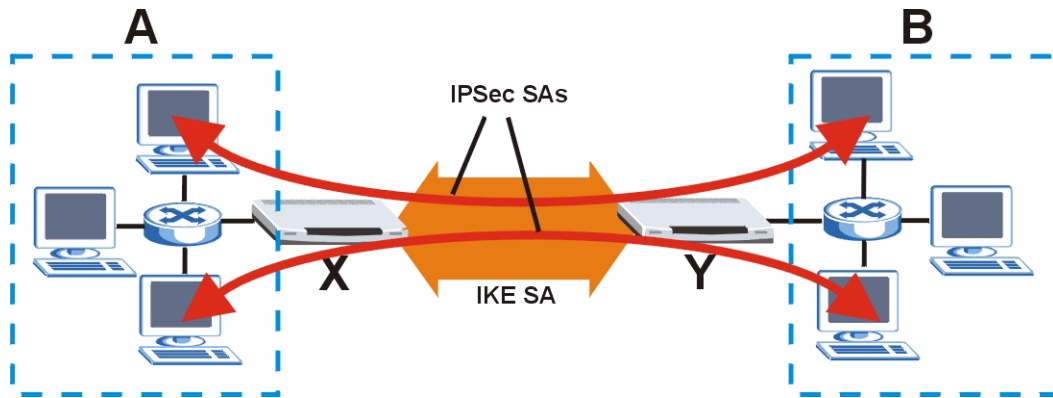
The following figure provides one perspective of a VPN tunnel.

**Figure 84** VPN: High-Level Example



The VPN tunnel (VPN) connects the ZyWALL (X) and the remote IPsec router (Y). These routers then connect the local network (A) and remote network (B).

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyWALL and the remote IPsec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyWALL and remote IPsec router. The second phase uses the IKE SA to establish an IPSec SA between computers on the local network and remote network. The following graphic illustrates this.

**Figure 85** VPN: IKE SA and IPsec SA

In some situations, you might want to set up a VPN tunnel quickly and temporarily. In this case, you can create an IPsec SA using manual keys. In this kind of VPN tunnel, there is no IKE SA, and you specify the encryption and authentication keys manually.

The rest of this section discusses IKE SAs, IPsec SAs, and IPsec SAs using manual keys in more detail. Then, it elaborates on more specific topics, such as encryption and authentication.

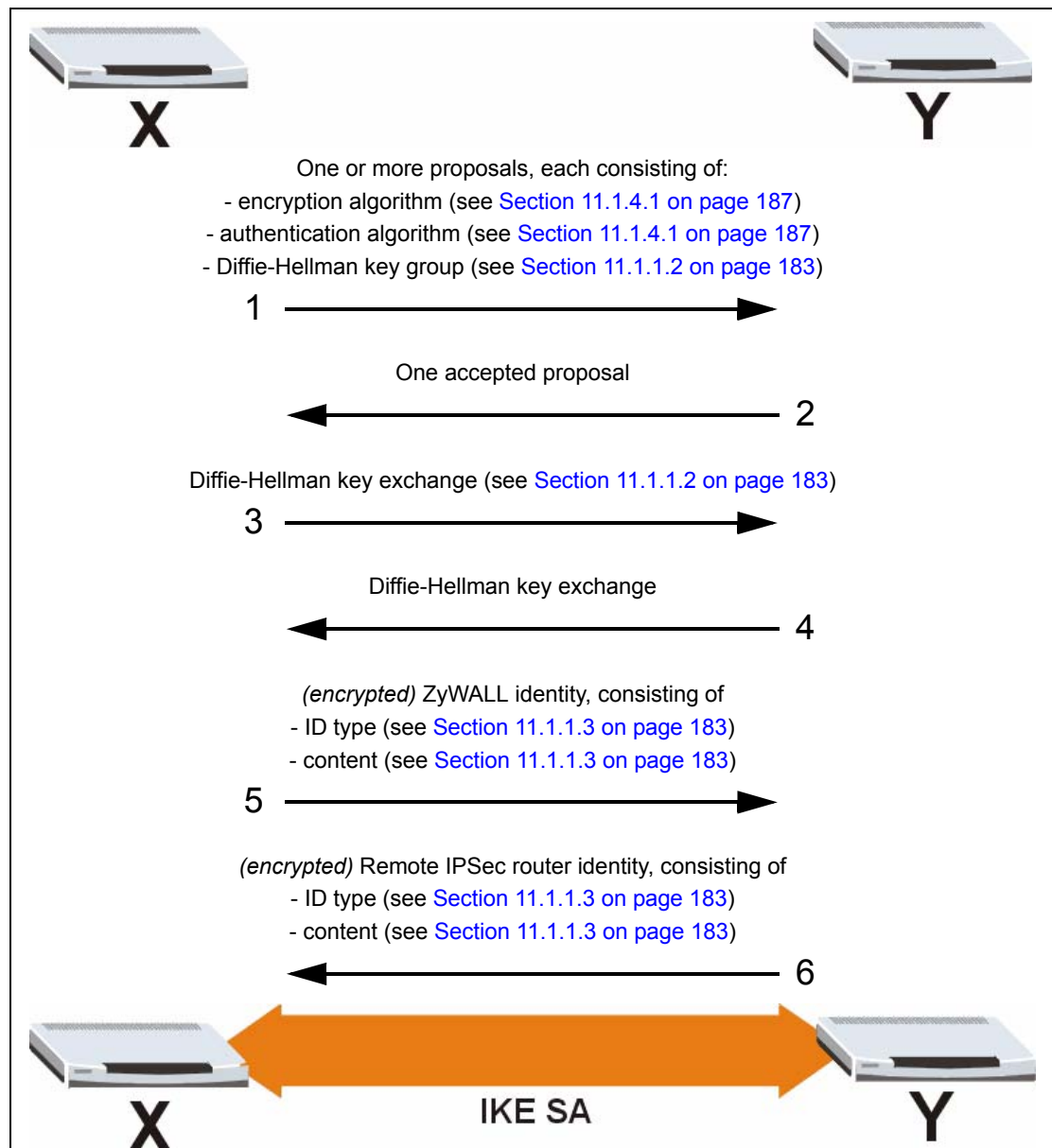
**Note:** If a VPN tunnel should support remote management (such as Telnet, WWW, and so on), you cannot configure it here. You should configure this in the screens for remote management.

### 11.1.1 IKE SA

The negotiation mode determines how an IKE SA is established between the ZyWALL and remote IPsec router. There are two negotiation modes--main mode and aggressive mode. Both routers must use the same negotiation mode.

Main mode is illustrated by the example below, where the ZyWALL (X) is initiating an IKE SA.

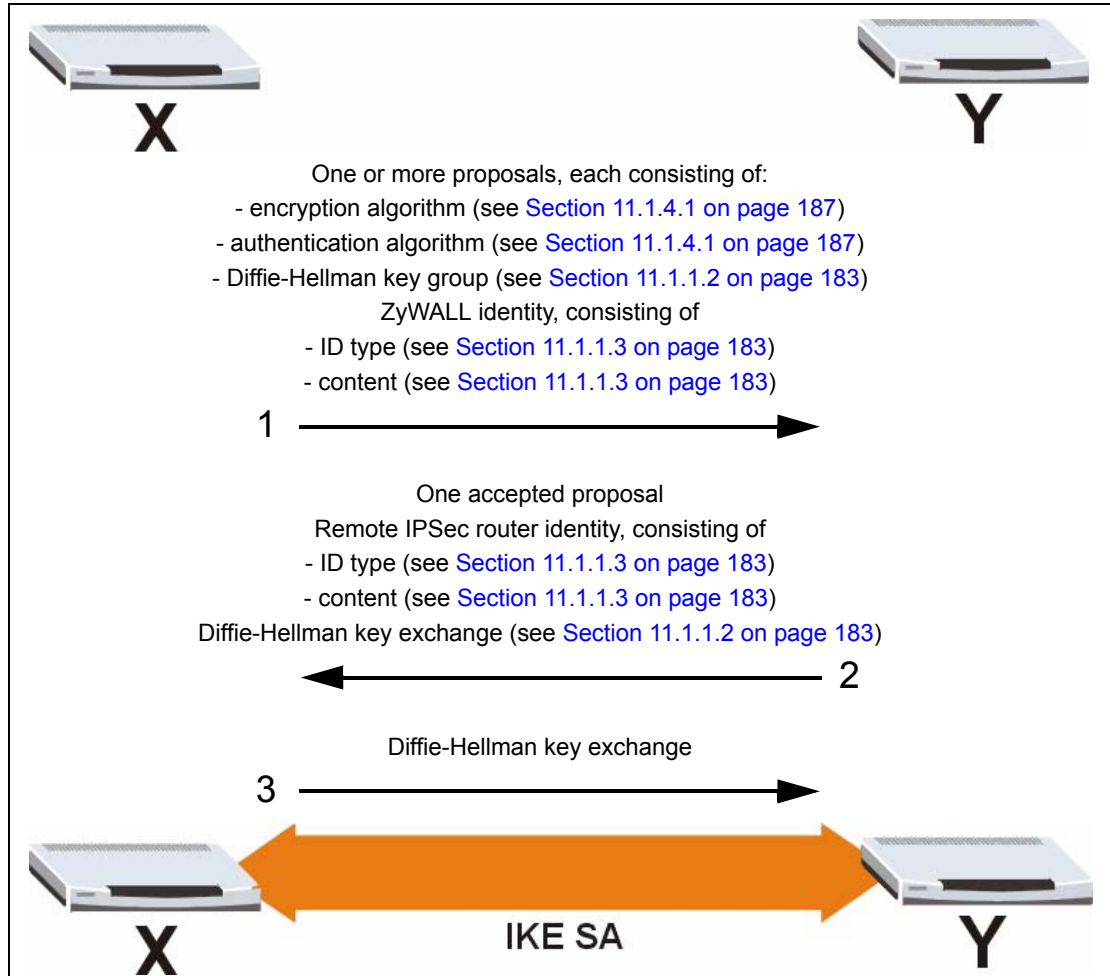
**Figure 86** IKE SA: Main Negotiation Mode



The ZyWALL sends its proposal to the remote IPsec router. The remote IPsec router selects an acceptable proposal and sends the accepted proposal back to the ZyWALL. The ZyWALL and the remote IPsec router then participate in a Diffie-Hellman key exchange, based on the accepted Diffie-Hellman key group, to establish a shared secret. Last, the ZyWALL and the remote IPsec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

Main mode provides better security because your identity is encrypted in steps 5 and 6. The trade-off is the number of steps it takes to establish the IKE SA. In contrast, aggressive mode is faster but does not provide as much security. This mode is illustrated below.

**Figure 87** IKE SA: Aggressive Negotiation Mode



Aggressive mode only takes three steps to establish the IKE SA, but your identity is not encrypted. 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 keys for authentication. For example, the remote IPsec router may be a telecommuter who does not have a static IP address.

The negotiation mode is one characteristic of a IKE SA. The rest of the characteristics include the following:

- the ZyWALL and remote IPsec router - these characteristics explain how the ZyWALL and remote IPsec router are identified in the network.
- IKE SA proposal (and which proposals are acceptable) - a proposal includes encryption algorithms, authentication algorithms, and DHx key groups.

- authentication method (and extended authentication) - these characteristics control how the ZyWALL and remote IPSec router authenticate each other.
- additional properties - these characteristics include the IKE SA life time, NAT traversal, and so on. See [Section 11.1.2.3 on page 186](#) for SA life time, [Section 11.1.4.3 on page 190](#) for NAT traversal and each screen for the other properties.

The first three sets of characteristics are discussed below.

### 11.1.1.1 ZyWALL and Remote IPSec Router

In an IKE SA, the ZyWALL can be identified by a static IP address, a domain name or a dynamic domain name. The remote IPSec router can also be identified by a static IP address, a domain name or a dynamic domain name.

### 11.1.1.2 IKE SA Proposal

An IKE SA consists of an encryption algorithm, authentication algorithm, and Diffie-Hellman (DHx) key group. In the ZyWALL, you can only specify one DHx key group for a VPN gateway, but you can specify multiple pairs of encryption and authentication algorithms. This approach increases the likelihood that the ZyWALL and the remote IPSec router agree on an acceptable IKE SA.

Encryption and authentication algorithms are discussed in more detail in [Section 11.1.4.1 on page 187](#).

Once the IKE SA is established, the ZyWALL and the remote IPSec router use the Diffie-Hellman public-key cryptography protocol to establish a shared secret. The shared secret is then used to generate keys for IKE SA and IPSec SA encryption. The Diffie-Hellman public-key cryptography protocol is based on DHx key groups. Each key group is a fixed number of bits long. The longer the length, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

**Note:** The ZyWALL and the remote IPSec router have to use the same DHx key group.

Perfect Forward Secrecy (PFS), which improves the confidentiality of information encrypted using DHx key groups, is discussed in [Section 11.1.2.1 on page 185](#).

### 11.1.1.3 Authentication Key and Extended Authentication (X-Auth)

If the ZyWALL and the remote IPSec router can authenticate each other with certificates, the certificates provide all the information used for authentication. Otherwise, you have to provide the information manually.

You have to create (and distribute) a pre-shared key for authentication.

**Note:** The ZyWALL and the remote IPSec router must use the same pre-shared key.

The ZyWALL and the remote IPsec router authenticate each other using an ID type and content. The ID type can be domain name, IP address, or e-mail address, and the content is a (properly-formatted) domain name, IP address, or e-mail address. The content is only used for identification. Any such domain name or e-mail address does not have to exist, and any such domain name or IP address does not have to correspond to the ZyWALL's or remote IPsec router's properties.

The ZyWALL and the remote IPsec router have separate ID type and content values, so both of them must store two sets of information, one for themselves and one for the other router. Local ID type and content refers to the ID type and content that applies to the router itself, and peer ID type and content refers to the ID type and content that applies to the other router.

In order to establish an IKE SA, the ZyWALL's local and peer ID type and content must match the corresponding peer and local ID type and content on the remote IPsec router. For example, in [Table 49 on page 184](#), the ZyWALL and the remote IPsec router authenticate each other successfully. In contrast, in [Table 50 on page 184](#), the ZyWALL and the remote IPsec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

**Table 49** VPN Example: Matching ID Type and Content

ZYWALL	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

**Table 50** VPN Example: Mismatching ID Type and Content

ZYWALL	REMOTE IPSEC ROUTER
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

If the ZyWALL and remote IPsec router use certificates, you can also specify a peer ID type of Subject Name. In this case, the ID content comes from the Subject Name of the certificate.

If you want the ZyWALL to ignore the remote IPsec router's ID type and content during authentication, you can select a peer ID type of Any for that VPN gateway.

**Note:** Regardless of the ID type and content configuration, the ZyWALL does not allow you to save multiple active IPsec SAs with overlapping local and remote IP addresses.



Extended authentication is helpful when multiple IPSec routers use one VPN rule to connect to a single IPSec router. In extended authentication, one of the routers (the ZyWALL or the remote IPSec router) verifies a user name and password from the other router using the local user database or an external RADIUS server. As a result, an attacker cannot establish an IPSec SA without a valid user name and password. The ZyWALL can support either role in extended authentication. In server mode, it accepts a user name and password from the remote IPSec router and verifies it using the local user database or a specified server; in client mode, it provides a user name and password to the remote IPSec router for authentication.

## 11.1.2 IPSec SAs Using IKE SAs

In an IPSec SA using an IKE SA, the IPSec SA is established after the ZyWALL and remote IPSec router have established the IKE SA. An IPSec SA is divided into the following sets of characteristics.

- IPSec SA proposal - these characteristics control how the ZyWALL and remote IPSec router negotiate and establish the IPSec SA.
- the local and remote network - these characteristics explain how the local network and the remote network are identified.
- IPSec SA properties - these characteristics control decisions once the IPSec SA is established.

Each set of characteristics is discussed below.

### 11.1.2.1 IPSec SA Proposal

Once the ZyWALL and remote IPSec router have established the IKE SA, they can negotiate an IPSec SA. The active protocol (ESP or AH) provides authentication for the IPSec SA, and you also specify what type of encapsulation (tunnel or transport) the packets should have. Both routers must use the same active protocol and encapsulation. See [Section 11.1.4.1 on page 187](#) and [Section 11.1.4.2 on page 189](#) for more information about the ESP and AH protocols and encapsulation, respectively.

Similar to the IKE SA proposal, the ZyWALL and remote IPSec router negotiate which encryption and authentication algorithms to use. Before the IPSec SA is established, each pair of encryption-authentication algorithms is called a proposal. In this case, if the remote IPSec router does not accept the first proposal, it might accept a different one. See [Section 11.1.4.1 on page 187](#) for more information about encryption and authentication algorithms.

The ZyWALL and remote IPSec router can also enable Perfect Forward Secrecy (PFS). Every time an IPSec SA is established, PFS uses a new Diffie-Hellman exchange to change the root key that is used to generate encryption keys. As a result, if one encryption key is compromised, previous and subsequent keys are secure because they were derived from different root keys. The Diffie-Hellman exchange is time-consuming, however, and it may be unnecessary for data that does not require such security.

### 11.1.2.2 Local and Remote Network

If IPsec SAs have overlapping local networks and overlapping remote networks, only one of these IPsec SAs can be set to active at a time. If a packet has to be routed through an overlapping (inactive) connection, it is dropped.

**Note:** The ZyWALL does not allow you to save multiple active IPsec SAs with overlapping local and remote IP addresses.

### 11.1.2.3 IPsec SA Properties

An IPsec SA can also have the following properties:

- Replay detection - the ZyWALL detects and rejects old or duplicate packets to prevent these kinds of Denial of Service (DoS) attacks.
- NetBIOS traffic - you can set the ZyWALL to allow certain TCP/UDP packets to pass through the IPsec SA so that local computers can find computers on the remote network and vice versa.

### 11.1.3 IPsec SA Using Manual Keys

In IPsec SAs using manual keys, the ZyWALL and remote IPsec router only establish an IPsec SA. They do not establish an IKE SA. In addition, you explicitly provide the encryption key and the authentication key. As a result, this kind of IPsec SA is much simpler to set up than regular IPsec SAs, but it is also less secure. Usually, this kind of IPsec SA is a temporary solution.

IPsec SAs using manual keys have the following characteristics:

- the ZyWALL and remote IPsec router - the ZyWALL and the remote IPsec router can only be identified by their IP addresses. In contrast, IKE SAs are more flexible. (See [Section 11.1.1.1 on page 183](#).)
- manual key - these characteristics specify the manual key, active protocol, and encapsulation. This is discussed in more detail below.
- the local and remote network - this is the same as other IPsec SAs. (See [Section 11.1.2.2 on page 186](#).)
- IPsec SA properties - some features of IPsec SAs using IKE SAs might be available in IPsec SAs using manual keys. (See [Section 11.1.2.3 on page 186](#).)

In IKE SAs and other types of IPsec SAs, you can specify more than one pair of encryption-authentication algorithms for the proposal. In IPsec SAs using manual keys, you can only specify one encryption algorithm and one authentication algorithm, and you have to provide the corresponding encryption key and the authentication key.

Authentication is also simpler. Instead of ID type and content, you specify the Security Parameter Index (SPI). The SPI is used to distinguish different SAs terminating at the same destination and using the same IPsec protocol. This allows you to multiplex IPsec SAs to a single gateway. In IPsec SAs using manual keys, the SPI and the destination IP address

uniquely identify a particular security association. When an IPsec SA using manual keys is established, the SPI is transmitted from the remote IPsec router to the ZyWALL. The ZyWALL then uses the network, encryption and key values that the administrator associated with the SPI to establish the IPsec SA.

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

You also have to specify the encapsulation and active protocol, which are the same characteristics required in other types of IPsec SAs. These characteristics are discussed in detail in [Section 11.1.4.2 on page 189](#) and [Section 11.1.4.1 on page 187](#), respectively.

IPsec SAs using manual keys do not require DHx key groups or PFS. In addition, IPsec SAs using manual keys do not support NAT traversal or many other IPsec SA properties. These IPsec SAs also do not have SA life times.

## 11.1.4 Additional IPsec VPN Topics

This section discusses other IPsec VPN topics that apply to either IKE SAs or IPsec SAs or both. Relationships between the topics are also highlighted.

### 11.1.4.1 Active Protocols, Encryption Algorithms, and Authentication Algorithms

To create an IPsec SA, you must specify an active protocol to describe the packet formats and the default standards for packet structure (including implementation algorithms). The ZyWALL offers AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

The AH protocol was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality. In contrast, the ESP protocol offers encryption and payload padding to conceal the information in the packet, but it has limited authenticating properties because IP header information is not included in authentication.

There is a relationship between the active protocol and the types of encryption and authentication algorithms that are available. This relationship is illustrated in [Table 51 on page 188](#), where more information is also provided about each type of encryption and authentication algorithm.

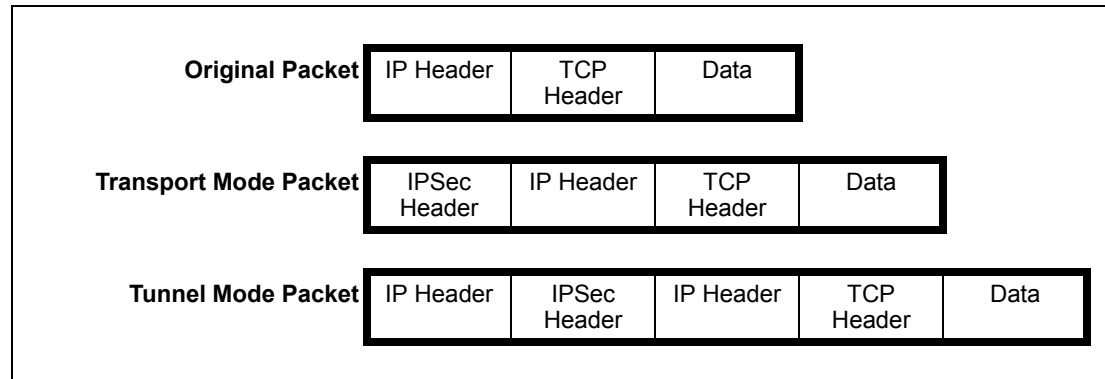
**Table 51** VPN: Types of Encryption and Authentication in ESP and AH

	ESP	AH
<b>Encryption</b>	<b>DES</b> 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 an IPSec SA without encryption.	
<b>Authentication</b>	<b>MD5</b> MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	<b>MD5</b> 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>SHA1</b> for maximum security.	

### 11.1.4.2 Encapsulation

IPSec VPNs use either transport mode or tunnel mode to encapsulate packets. These modes are illustrated below.

**Table 52** VPN: Transport and Tunnel Mode Encapsulation



Tunnel mode is the most common mode of operation. It is required to provide access to internal systems, and it is required for gateway-to-gateway and host-to-gateway communications. Tunnel mode is fundamentally an IPSec SA with authentication and encryption. It encapsulates the entire IP packet to transmit it securely.

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.

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In transport mode, the security protocol (AH or ESP) is located after the original IP header and options and before any upper-layer protocols in the packet (such as TCP or 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.

With AH, 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.

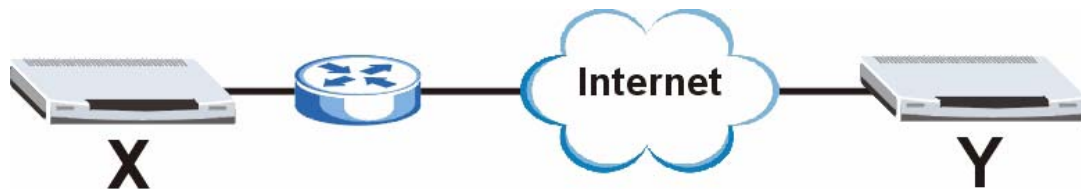
### 11.1.4.3 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec SA using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. NAT is not normally compatible with ESP in transport mode either because the NAT router changes the header of the IPSec packet. However, the ZyWALL's NAT Traversal feature provides a way to handle this.

NAT traversal adds a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. For example, in the figure below, when router X tries to establish an IKE SA, router Y checks the UDP port 500 header, and IPSec routers A and B build the IKE SA.

**Figure 88** VPN Example: NAT Traversal



For NAT traversal to work, you must do the following things:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router A.

The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

**Table 53** VPN: NAT Compatibility with Active Protocol and Encapsulation

ACTIVE PROTOCOL	ENCAPSULATION	NAT COMPATIBLE?
AH	Transport	No
AH	Tunnel	No
ESP	Transport	Yes*
ESP	Tunnel	Yes

\* - This is supported in the ZyWALL if you enable NAT traversal.

#### 11.1.4.4 SA Life Time

One characteristic of SAs is the SA life time. The SA lifetime specifies how long the SA lasts until it times out. When an SA times out, the ZyWALL automatically renegotiates the SA in the following situations:

- there is traffic when the SA life time expires
- the IPsec SA is configured on the ZyWALL as nailed up (see below)

Otherwise, the ZyWALL must re-negotiate the SA the next time someone wants to send traffic.

**Note:** If the IKE SA times out while an IPsec SA is connected, the IPsec SA stays connected.

An IPsec SA can also be set to nailed up. Normally, the ZyWALL drops the IPsec SA when the life time expires or after two minutes of outbound traffic with no inbound traffic. If you set the IPsec SA to nailed up, the ZyWALL automatically renegotiates the IPsec SA when the SA life time expires, and it does not drop the IPsec SA if there is no inbound traffic.

**Note:** The SA life time and nailed up settings only apply if the rule identifies the remote IPsec router by a static IP address or a domain name. If the **Remote Gateway Address** field is set to **0.0.0.0**, the ZyWALL cannot initiate the tunnel (and cannot renegotiate the SA).

#### 11.1.4.5 IPsec High Availability

IPsec high availability (IPsec HA or VPN HA) allows you to use a redundant (backup) VPN connection to another WAN interface on the remote IPsec router if the primary (regular) VPN connection goes down.

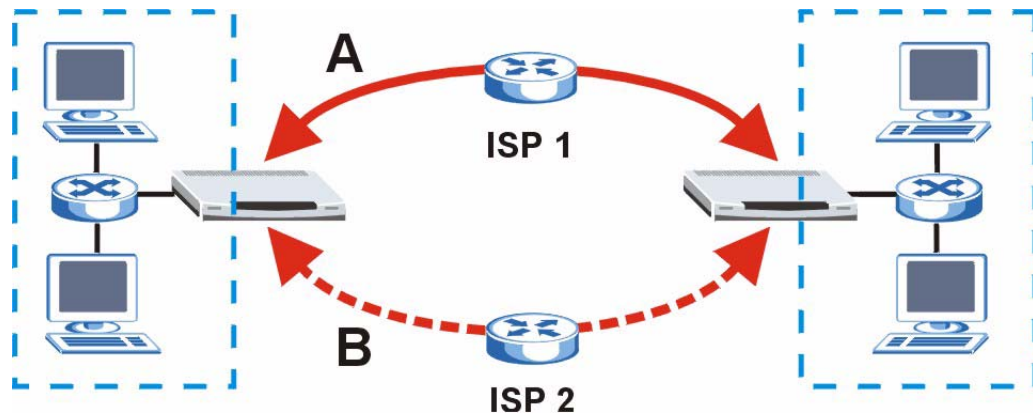
When setting up a IPsec high availability VPN tunnel, the remote IPsec router:

- must have multiple WAN connections
- only needs the configure one corresponding IPsec rule
- should not have IPsec high availability settings in its corresponding IPsec rule
- should ideally identify itself by a domain name (or dynamic domain name).
- must not have the **My IP Address** field set to a specific IP address (use a domain name, dynamic domain name or 0.0.0.0).
- should use a WAN connectivity check to this ZyWALL's WAN IP address

If the remote IPsec router is not a ZyWALL, you may also want to avoid setting the IPsec rule to nailed up.

In the following figure, if primary VPN tunnel A goes down, the ZyWALL uses the redundant VPN tunnel (B).

**Figure 89** IPSec High Availability



## 11.2 VPN Rules (IKE)

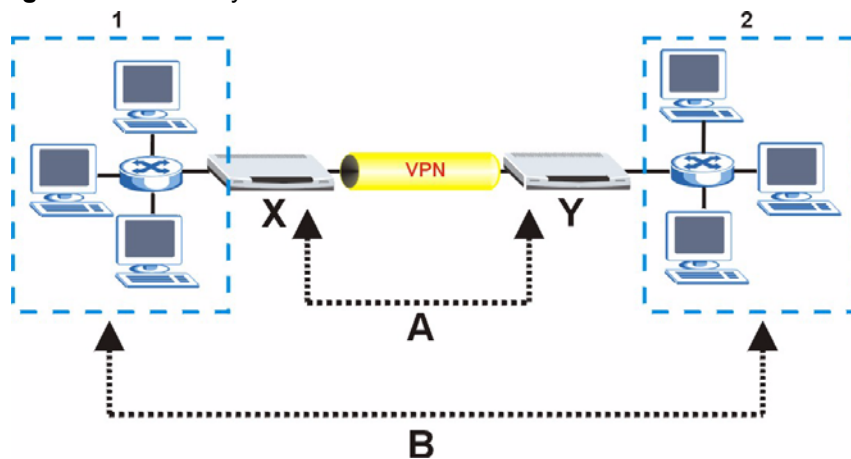
A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.

A gateway policy identifies the IPSec routers at either end of a VPN tunnel. This is used in setting up the IKE (phase 1) security association (SA).

A network policy specifies which devices (behind the IPSec routers) can use the VPN tunnel. This is used in setting up the IPSec (phase 2) SA.

In the following diagram, **X** is your ZyWALL, **Y** is a remote IPSec router, the **A** arrows denote the gateway policy and the **B** arrows denote the network policy. The local network is marked **1**, and the remote network is marked **2**.

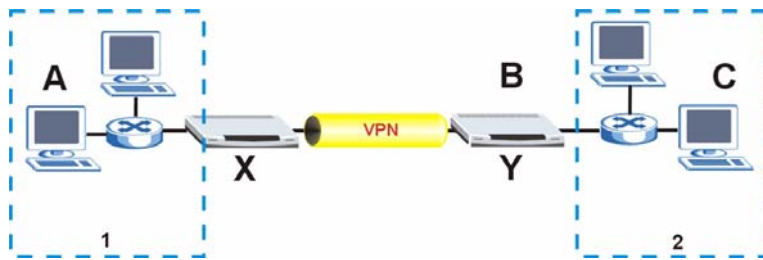
**Figure 90** Gateway and Network Policies



This figure helps explain the main fields in the VPN setup. In this figure, **X** is your ZyWALL, **Y** is a remote IPSec router, **A** denotes a local network IP address, **B** denotes a remote gateway address and **C** denotes a remote network address. The local network is labeled **1** and the remote network is labeled **2**.



**Figure 91** IPSec Fields Summary



Click **VPN** to display the **VPN Rules (IKE)** screen. Use this screen to manage the ZyWALL's list of VPN rules (tunnels) that use IKE SAs.

**Figure 92** VPN Rules (IKE)

The screenshot shows the 'VPN Rules (IKE)' configuration page. At the top, there are tabs for 'VPN Rules (IKE)', 'VPN Rules (Manual)', 'SA Monitor', and 'Global Setting'. Below the tabs is a diagram showing a 'Local Network' connected to 'My ZyWALL', which is connected to the 'Internet' via a 'VPN Tunnel' to a 'Remote Gateway', which is then connected to a 'Remote Network'. Below the diagram is a table of VPN rules.











#	VPN Rules	Gateway Policy	Local Address	Remote Address	Action
1	test2	0.0.0.0	Dynamic		[Edit] [Delete] [Add]
	ex2	0.0.0.0	Any		[Move] [Edit] [Delete] [Add]
	ex3	1.0.0.0 / 255.0.0.0	Any		[Move] [Edit] [Delete] [Add]
2	ToZW2K	172.22.2.155	172.21.1.28		[Edit] [Delete] [Add]
	ex1	192.168.2.33	192.168.1.33 / 255.255.255.0		[Move] [Edit] [Delete] [Add]
3	Recycle Bin				[Delete]
	ex	10.2.1.35	0.0.0.0		[Move] [Edit] [Delete]

The following table describes the labels in this screen.



**Table 54** VPN Rules (IKE)

LABEL	DESCRIPTION
VPN Rules	These VPN rules define the settings for creating VPN tunnels for secure connection to other computers or networks.
	Click this icon to add a VPN gateway policy (or IPSec rule).
Gateway Policies	The first row of each VPN rule represents the gateway policy. The gateway policy identifies the IPSec routers at either end of a VPN tunnel ( <b>My ZyWALL</b> and <b>Remote Gateway</b> ) and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA (click the edit icon to display the other settings).

**Table 54** VPN Rules (IKE) (continued)

LABEL	DESCRIPTION
 My ZyWALL	This represents your ZyWALL. The WAN IP address, domain name or dynamic domain name of your ZyWALL displays in router mode. The ZyWALL's IP address displays in bridge mode.
 Remote Gateway	This represents the remote secure gateway. The IP address, domain name or dynamic domain name of the remote IPSec router displays if you specify it, otherwise <b>Dynamic</b> displays.
	Click this icon to add a VPN network policy.
Network Policies	The subsequent rows in a VPN rule are network policies. 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.
 Local Network	This is the network behind the ZyWALL. A network policy specifies which devices (behind the IPSec routers) can use the VPN tunnel.
 Remote Network	This is the remote network behind the remote IPsec router.
	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. The ZyWALL automatically moves the associated network policy(ies) to the recycle bin.
	Click this icon to establish a VPN connection to a remote network.
	This indicates that a gateway or network policy is not active.
Recycle Bin	The recycle bin holds any network policies without an associated gateway policy.

## 11.3 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.

Use this screen to configure a VPN gateway policy. The gateway policy identifies the IPSec routers at either end of a VPN tunnel (**My ZyWALL** and **Remote Gateway**) and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.

**Figure 93** 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](#))

Primary Remote Gateway  (Domain Name or IP Address)

Enable IPsec High Availability

Redundant Remote Gateway  (Domain Name or IP Address)

Fail back to Primary Remote Gateway when possible

Fail Back Check Interval\*  (180~86400 seconds)

\*Fail Back Check Interval: The time interval for checking availability of Primary Remote Gateway. IPsec SA life time will be superseded by this value when it is larger than this value.

**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
	test	192.168.1.5	10.10.1.1

The following table describes the labels in this screen.

**Table 55** 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 11.1.4.3 on page 190</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. The ZyWALL 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>
Primary Remote Gateway	<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>
Enable IPSec High Availability	<p>Turn on the high availability feature to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down. The remote IPSec router must have a second WAN connection in order for you to use this.</p> <p>To use this, you must identify both the primary and the redundant remote IPSec routers by WAN IP address or domain name (you cannot set either to <b>0.0.0.0</b>).</p>
Redundant Remote Gateway	Type the WAN IP address or the domain name (up to 31 characters) of the backup IPSec router to use when the ZyWALL cannot not connect to the primary remote gateway.

**Table 55** VPN Rules (IKE): Gateway Policy: Edit (continued)

LABEL	DESCRIPTION
Fail back to Primary Remote Gateway when possible	Select this to have the ZyWALL fall back to using the primary remote gateway if the connection becomes available again.
Fail Back Check Interval	<p>Set how often the ZyWALL should check the connection to the primary remote gateway while connected to the redundant remote gateway.</p> <p>Each gateway policy uses one or more network policies. If the fail back check interval is shorter than a network policy's SA life time, the fail back check interval is used as the check interval and network policy SA life time. If the fail back check interval is longer than a network policy's SA life time, the SA lifetime is used as the check interval and network policy SA life time.</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 55** 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 IPSec 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 55** 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' user names and passwords in the authentication server's local user database or a RADIUS server (see <a href="#">Chapter 13 on page 243</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 user name 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 55** 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 92 on page 193</a>). Refer to <a href="#">Section 11.4 on page 200</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.

## 11.4 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. 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.



Figure 94 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 56** 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 56** 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 56** 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 IPSec 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.

## 11.5 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 95** VPN Rules (IKE): Network Policy Move

The following table describes the labels in this screen.

**Table 57** 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.

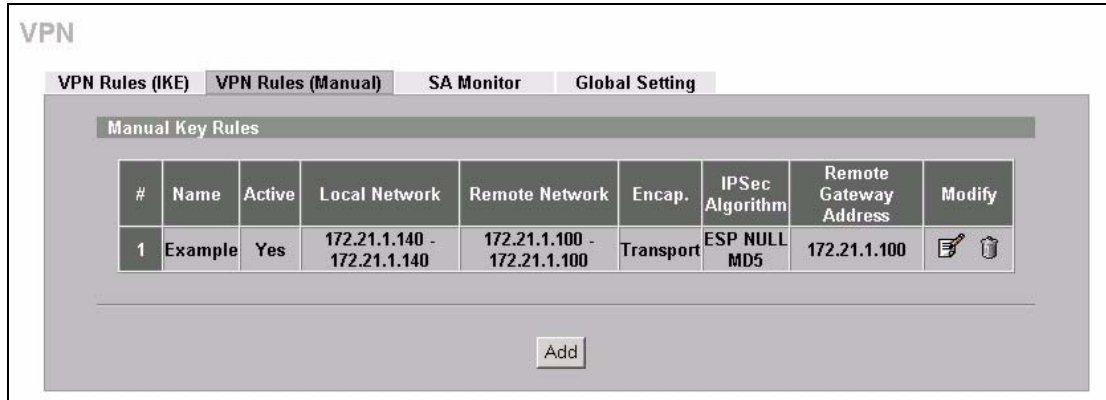
## 11.6 VPN Rules (Manual)

Refer to [Figure 91 on page 193](#) for a graphical representation of the fields in the web configurator.

Click **VPN > VPN Rules (Manual)** to open the **VPN Rules (Manual)** screen.

Use this screen to manage the ZyWALL's list of VPN rules (tunnels) that use manual keys. You may want to configure a VPN rule that uses manual key management if you are having problems with IKE key management.

**Figure 96** VPN Rules (Manual)



The following table describes the labels in this screen.

**Table 58** 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 58** 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.

## 11.7 VPN Rules (Manual): Edit

Click the edit icon on the **VPN Rules (Manual)** screen to open the following screen. Use this screen to configure VPN rules that use manual keys. Manual key management is useful if you have problems with IKE key management.

**Figure 97** VPN Rules (Manual): Edit

The following table describes the labels in this screen.

**Table 59** 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 59** 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	
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>The ZyWALL 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>

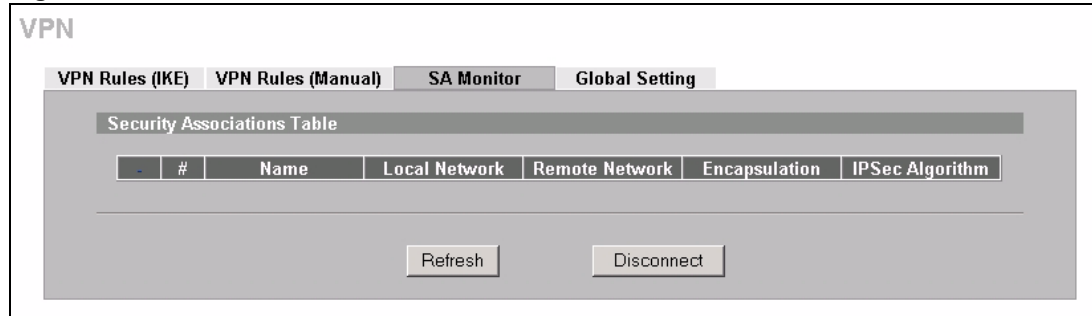
**Table 59** VPN Rules (Manual) Edit (continued)

LABEL	DESCRIPTION
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 (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select <b>AH</b> here, you must select options from the <b>Authentication Algorithm</b> field (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	<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>
Encryption Key	<p>This field is applicable when you select <b>ESP</b> in the <b>Active Protocol</b> field above.</p> <p>With <b>DES</b>, type a unique key 8 characters long. With <b>3DES</b>, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.</p>
Authentication Key	<p>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.</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.

## 11.8 VPN SA Monitor

In the web configurator, click **VPN > SA Monitor**. 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 98** VPN: SA Monitor

The following table describes the labels in this screen.

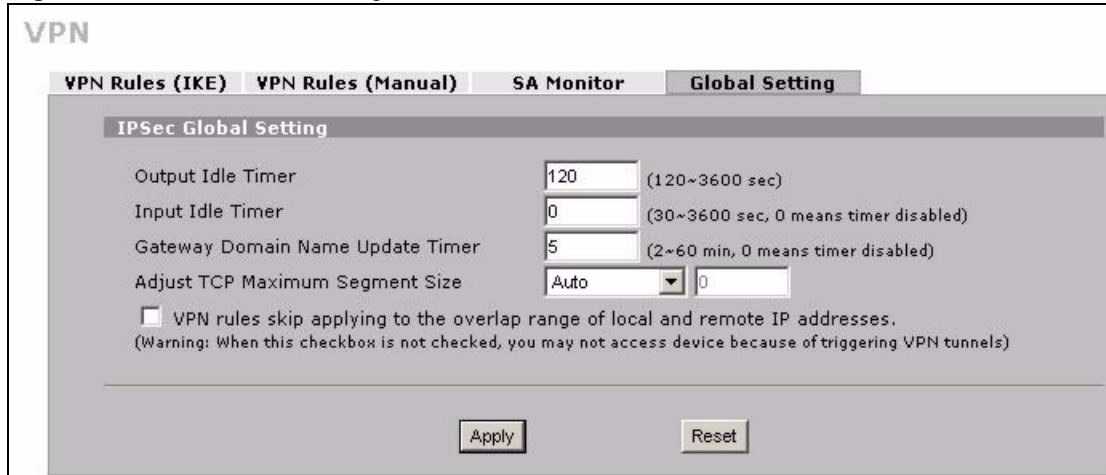
**Table 60** VPN: SA Monitor

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.
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> .

## 11.9 VPN Global Setting

Click **VPN > Global Setting** to open the **VPN Global Setting** screen. Use this screen to change settings that apply to all of your VPN tunnels.

**Figure 99** VPN: Global Setting



The following table describes the labels in this screen.

**Table 61** VPN: Global Setting

LABEL	DESCRIPTION
Output Idle Timer	<p>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.</p> <p>Enter the time period (between 120 and 3600 seconds) to wait before the ZyWALL checks all of the VPN connections to remote IPsec routers.</p> <p>Enter <b>0</b> to disable this feature.</p>
Input Idle Timer	<p>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.</p> <p>Enter the time period (between 30 and 3600 seconds) to wait before the ZyWALL checks all of the VPN connections to remote IPsec routers.</p> <p>Enter <b>0</b> to disable this feature.</p>
Gateway Domain Name Update Timer	<p>This field is applicable when you enter a domain name to identify the ZyWALL and/or the remote secure gateway.</p> <p>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).</p> <p>Enter <b>0</b> to disable this feature.</p>
Adjust TCP Maximum Segment Size	<p>The TCP packets are larger after the ZyWALL encrypts them for VPN. The ZyWALL fragments packets that are larger than a connection's MTU (Maximum Transmit Unit).</p> <p>In most cases you should leave this set to <b>Auto</b>. The ZyWALL automatically sets the Maximum Segment Size (MSS) of the TCP packets that are to be encrypted by VPN based on the encapsulation type.</p> <p>Select <b>Off</b> to not adjust the MSS for the encrypted TCP packets.</p> <p>If your network environment causes fragmentation issues that are affecting your throughput performance, you can manually set a smaller MSS for the TCP packets that are to be encrypted by VPN. Select <b>User-Defined</b> and specify a size from 0~1460 bytes. 0 has the ZyWALL use the auto setting.</p>

**Table 61** VPN: Global Setting (continued)

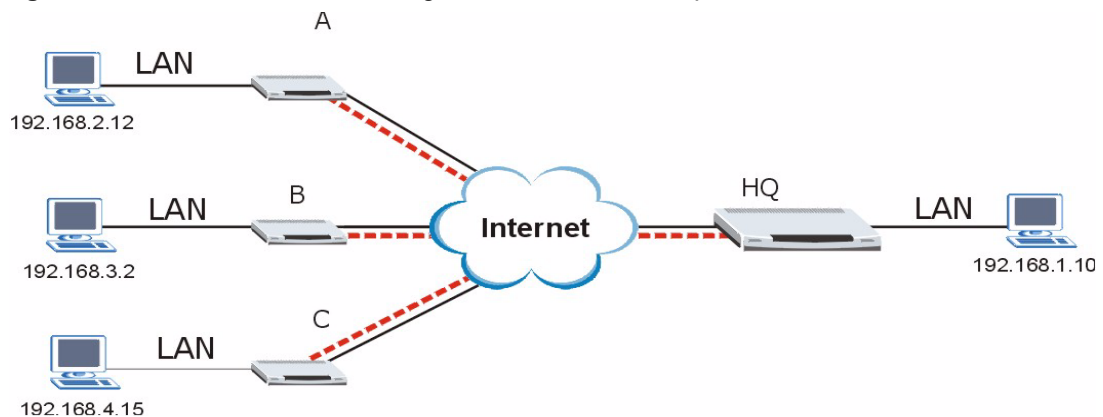
LABEL	DESCRIPTION
VPN rules skip applying to the overlap range of local and remote IP addresses	<p>When you configure a VPN rule, the ZyWALL checks to make sure that the IP addresses in the local and remote networks do not overlap. Select this check box to disable the check if you need to configure a VPN policy with overlapping local and remote IP addresses.</p> <p><b>Note:</b> If a VPN policy's local and remote IP addresses overlap, you may not be able to access the device on your LAN because the ZyWALL automatically triggers a VPN tunnel to the remote device with the same IP address.</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.

## 11.10 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.

### 11.10.1 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 100** Telecommuters Sharing One VPN Rule Example

**Table 62** 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

### 11.10.2 Telecommuters Using Unique VPN Rules Example

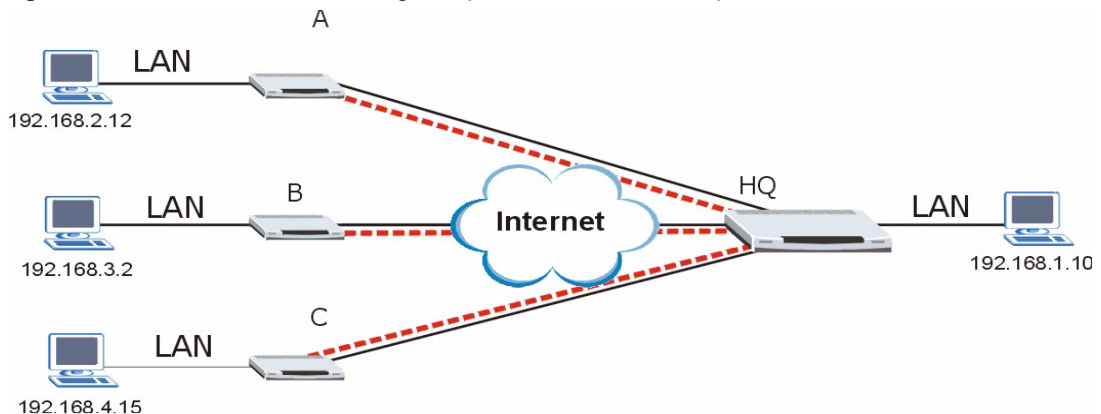
In this example the telecommuters (A, B and C in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see [Section 11.1.1 on page 180](#)), 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 101** Telecommuters Using Unique VPN Rules Example



**Table 63** Telecommuters Using Unique VPN Rules Example

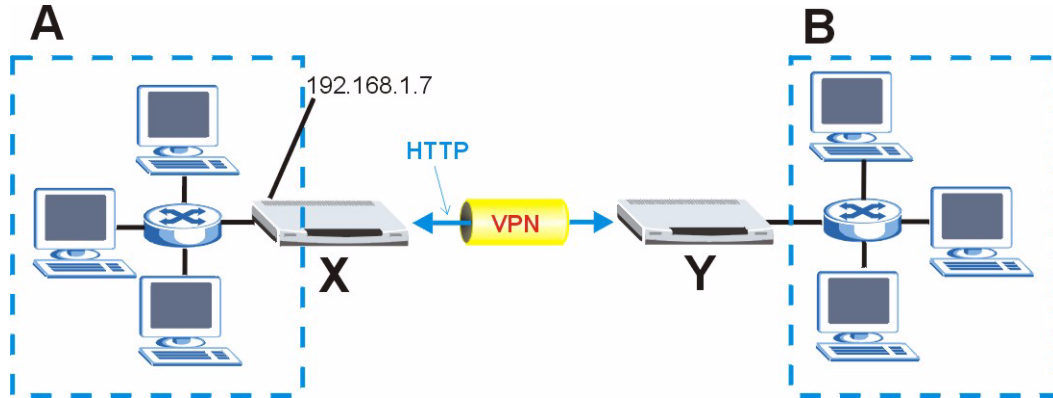
TELECOMMUTERS	HEADQUARTERS
<b>All Telecommuter Rules:</b>	All Headquarters Rules:
My ZyWALL 0.0.0.0	My ZyWALL: bigcompanyhq.com
Remote Gateway Address: bigcompanyhq.com	Local Network - Single IP Address: 192.168.1.10
Remote Network - Single IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: 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
Local IP Address: 192.168.4.15	Remote Gateway Address: telecommuterc.dydns.org
	Remote Address 192.168.4.15

## 11.11 VPN and Remote Management

You can allow someone to use a service (like Telnet or HTTP for example) through a VPN tunnel to manage the ZyWALL. One of the ZyWALL's ports must be part of the VPN rule's local network. This can be the ZyWALL's LAN port if you do not want to allow remote management on the WAN port. You also have to configure remote management (**REMOTE MGMT**) to allow management access for the service through the specific port.

In the following example, the VPN rule's local network (**A**) includes the ZyWALL's LAN IP address of 192.168.1.7. Someone in the remote network (**B**) can use a service (like HTTP for example) through the VPN tunnel to access the ZyWALL's LAN interface. Remote management must also be configured to allow HTTP access on the ZyWALL's LAN interface.

**Figure 102** VPN for Remote Management Example





# CHAPTER 12

## Certificates

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

### 12.1 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).

### 12.1.1 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.

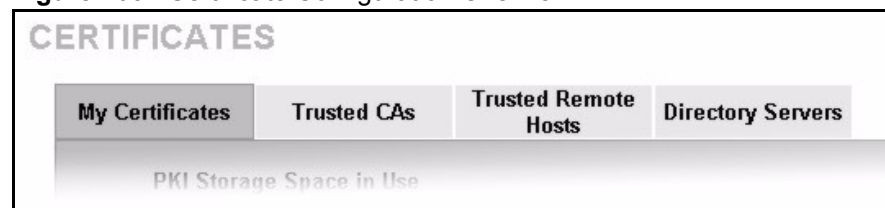
## 12.2 Self-signed Certificates

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.

## 12.3 Configuration Summary

This section summarizes how to manage certificates on the ZyWALL.

**Figure 103** 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).

## 12.4 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 104** My Certificates

**CERTIFICATES**

My Certificates Trusted CAs Trusted Remote Hosts Directory Servers

PKI Storage Space in Use

0%  41% 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 2 Plus Factory Default Certificate	CN=ZyWALL 2 Plus Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT	
2	Jim	REQ	CN=Jim.something, OU=Sales, O=SomeCompany, C=USA	N/A	N/A	N/A	
3	SomeCompany	SELF	CN=SomeCompany.com, OU=Sales, O=SomeCompany, C=USA	CN=SomeCompany.com, OU=Sales, O=SomeCompany, C=USA	2006 Mar 27th, 06:51:07 GMT	2009 Mar 27th, 06:51:07 GMT	

Import Create Refresh

The following table describes the labels in this screen.

**Table 64** 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 64** 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>

## 12.5 My Certificate Import

Click **SECURITY > CERTIFICATES > My Certificates > 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.

### 12.5.1 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 105** My Certificate Import

**CERTIFICATES - MY CERTIFICATE - IMPORT**

**Import**

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

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.

File Path:

The following table describes the labels in this screen.

**Table 65** 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.

## 12.6 My Certificate Create

Click **SECURITY > CERTIFICATES > My Certificates > 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 106** 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 66** 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.
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 12.7 on page 224</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.

**Table 66** My Certificate Create (continued)

LABEL	DESCRIPTION
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.

## 12.7 My Certificate Details

Click **SECURITY > CERTIFICATES > My Certificates** to open the **My Certificates** screen (see [Figure 104 on page 219](#)). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyWALL uses to sign the trusted remote host certificates that you import to the ZyWALL.



**Figure 107** My Certificate Details

**CERTIFICATES - MY CERTIFICATE - DETAILS**

---

Name

Property  Default self-signed certificate which signs the imported remote host certificates.

**Certification Path**

**Certificate Information**

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	946684930
Subject	CN=ZyWALL 2 Plus Factory Default Certificate
Issuer	CN=ZyWALL 2 Plus Factory Default Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2000 Jan 1st, 00:00:00 GMT
Valid To	2030 Jan 1st, 00:00:00 GMT
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	EMAIL=factory@auto.gen.cert
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	27:6d:5a:28:73:34:58:70:06:a3:e7:03:e8:ad:f9:67
SHA1 Fingerprint	4e:f9:9d:cb:05:53:e0:05:92:6c:a4:3d:e1:41:52:d9:09:98:71:7d

**Certificate in PEM (Base-64) Encoded Format**

```

-----BEGIN CERTIFICATE-----
MIIBpDCCAU6gAwIBAgIEOG1EAjANBgkqhkiG9w0BAQUFADAOMTIwMAVDVQQDEyIa
eVdBTEwgMiBQbHVzIEZhY3RvcnkgRGVmYXZvdCBDZXJ0aWZpY2FOZTAeFw0wMDAx
MDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBaMDQxMjAwBgNVBAMTKVp5V0FMTCAyIFBz
dXN0eSdG9yeSBEZWZhdWx0IENlcjZm1jYXR1MFwwDQYJKoZIhvcNAQEBBQAD
SwAwSABjBAP51yIiHWKOWeiR4c9gGVN2gHbncIB3HiyBN367YJXBB9fUFL7eaVjg
613EJlk/NBLAKTyact464EDASU3dqOsCAwEAANIMEYwDgYDVROPAQEABAQDAgKk
MCAGA1UdEQQZMBEaBFWZhy3Rvcn1AYXV0by5nZW4uY2VydDASBgNVHRMBAQAECDAG
AQH/AgEBMAOGCSqGSIb3DQEBBQUAAOEAAANKtrzt18DJysHfUfJbKQ3Bg9X39vWky
aahQdWVLxjzHvw/zmfTUUE2pM1skwipzOZJnlmKjtO1HXWdypG9PJQ==
    
```

The following table describes the labels in this screen.

**Table 67** 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 67** 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.

## 12.8 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 108** Trusted CAs



The following table describes the labels in this screen.

**Table 68** 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.
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".

**Table 68** Trusted CAs (continued)

LABEL	DESCRIPTION
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.

## 12.9 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 109** Trusted CA Import

The following table describes the labels in this screen.

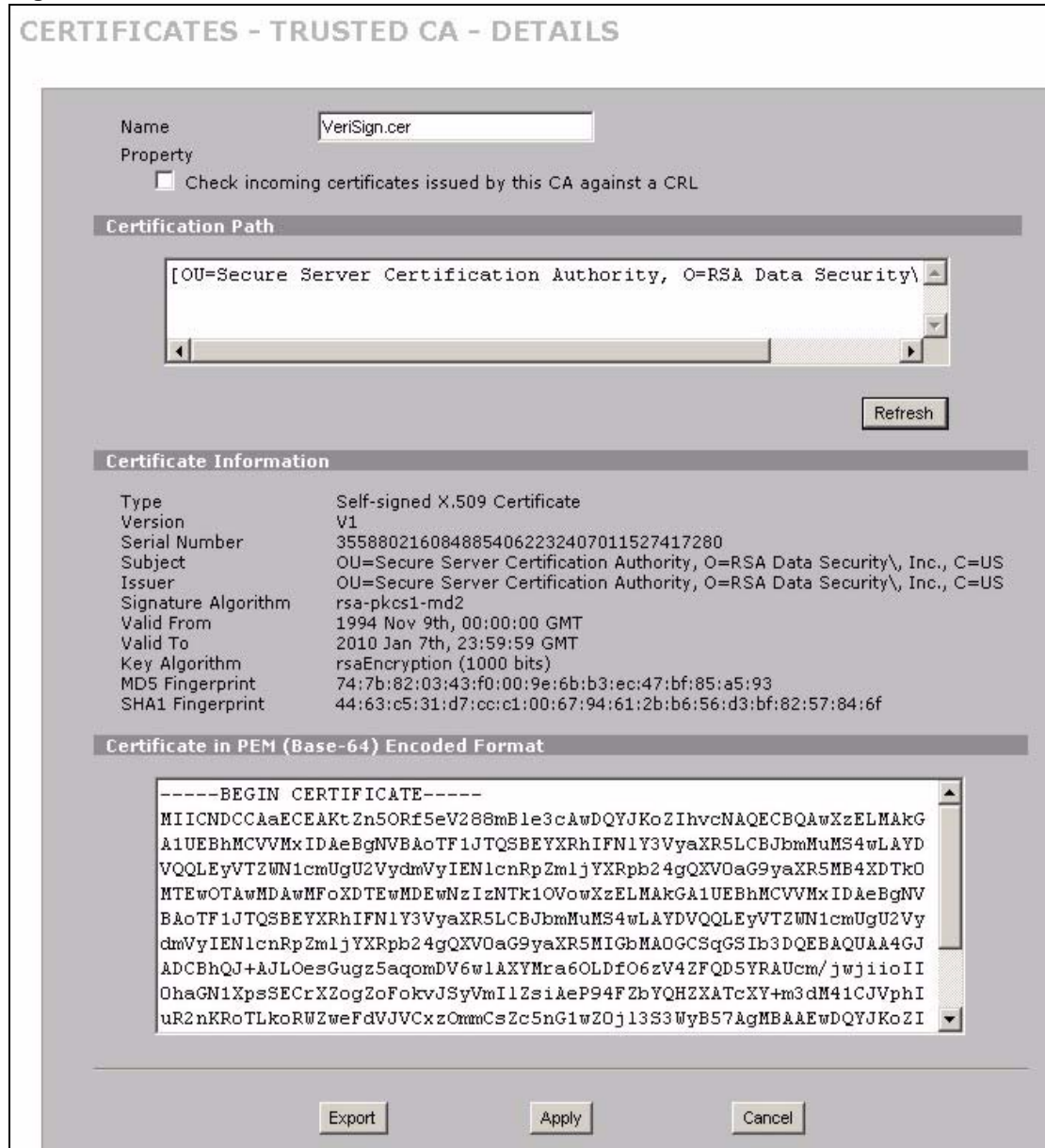
**Table 69** Trusted CA Import

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 CAs</b> screen.

## 12.10 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 110** Trusted CA Details



The following table describes the labels in this screen.

**Table 70** 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).
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).

**Table 70** Trusted CA Details (continued)

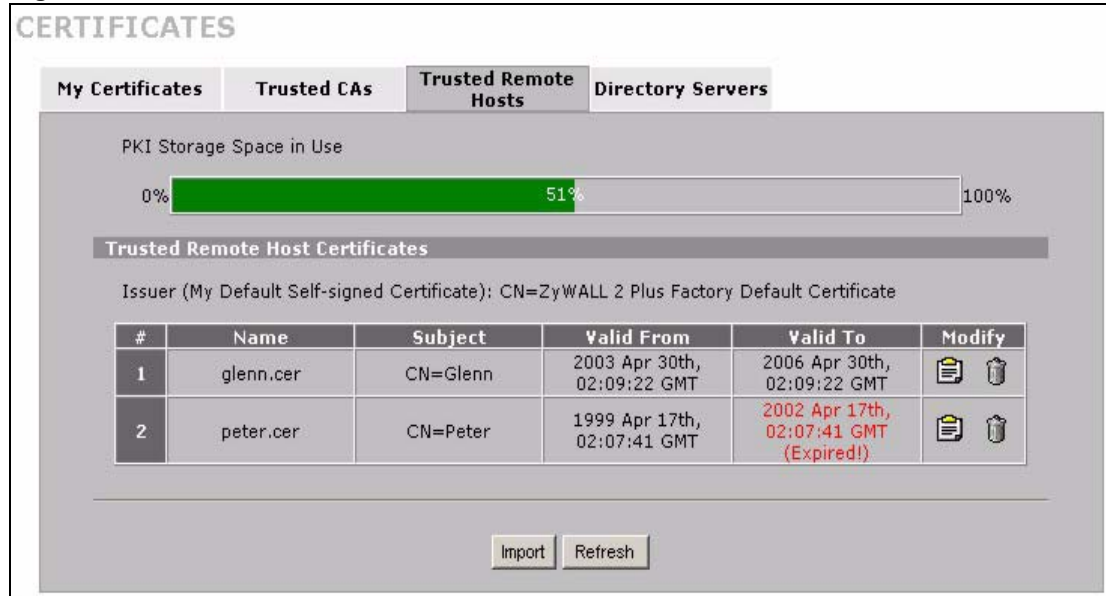
LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to 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.
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.

## 12.11 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 111** Trusted Remote Hosts

The following table describes the labels in this screen.

**Table 71** 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 71** 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.

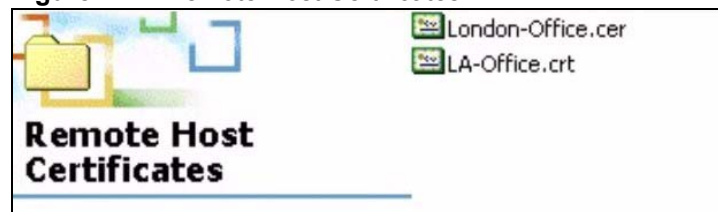
## 12.12 Verifying a Trusted Remote Host's Certificate

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.

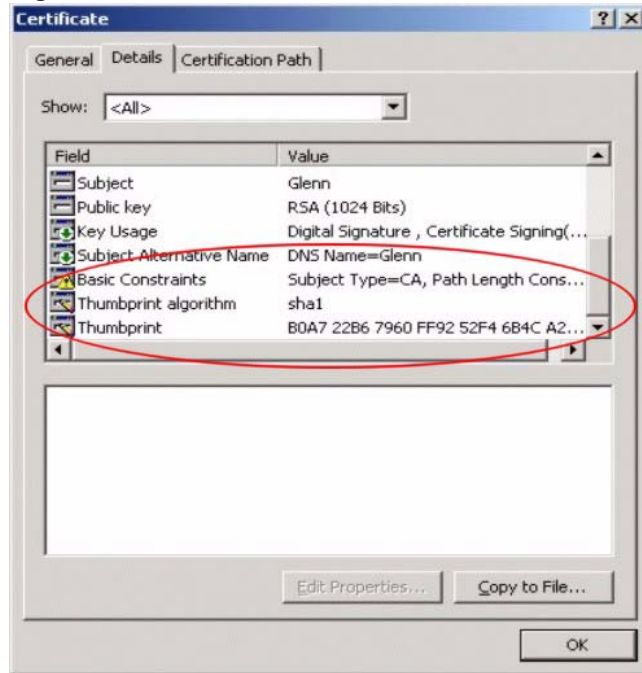
### 12.12.1 Trusted Remote Host Certificate Fingerprints

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 112** Remote Host Certificates

- 3 Double-click the certificate's icon to open the **Certificate** window. Click **Details** and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

**Figure 113** Certificate Details

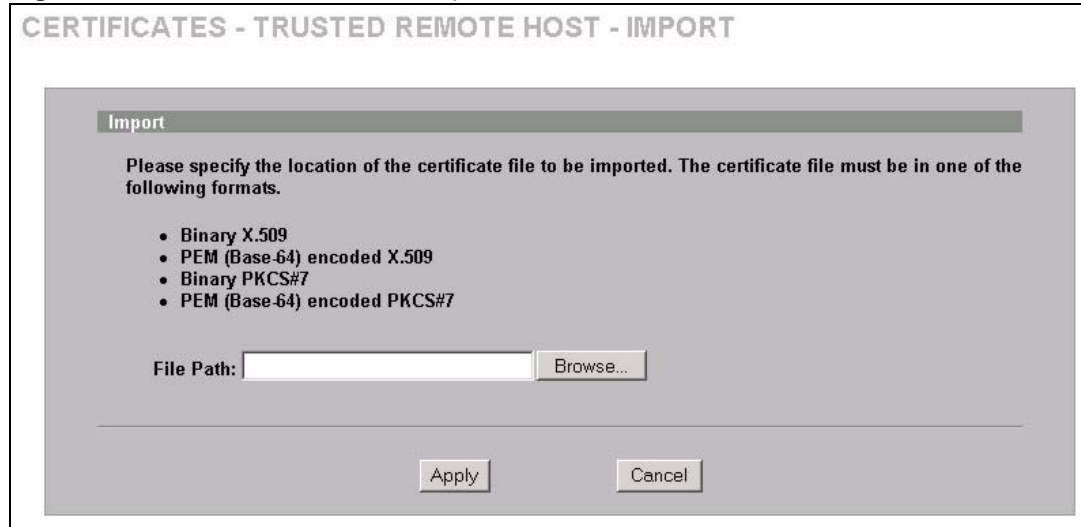
Verify (over the phone for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.

## 12.13 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 114** Trusted Remote Host Import



The following table describes the labels in this screen.

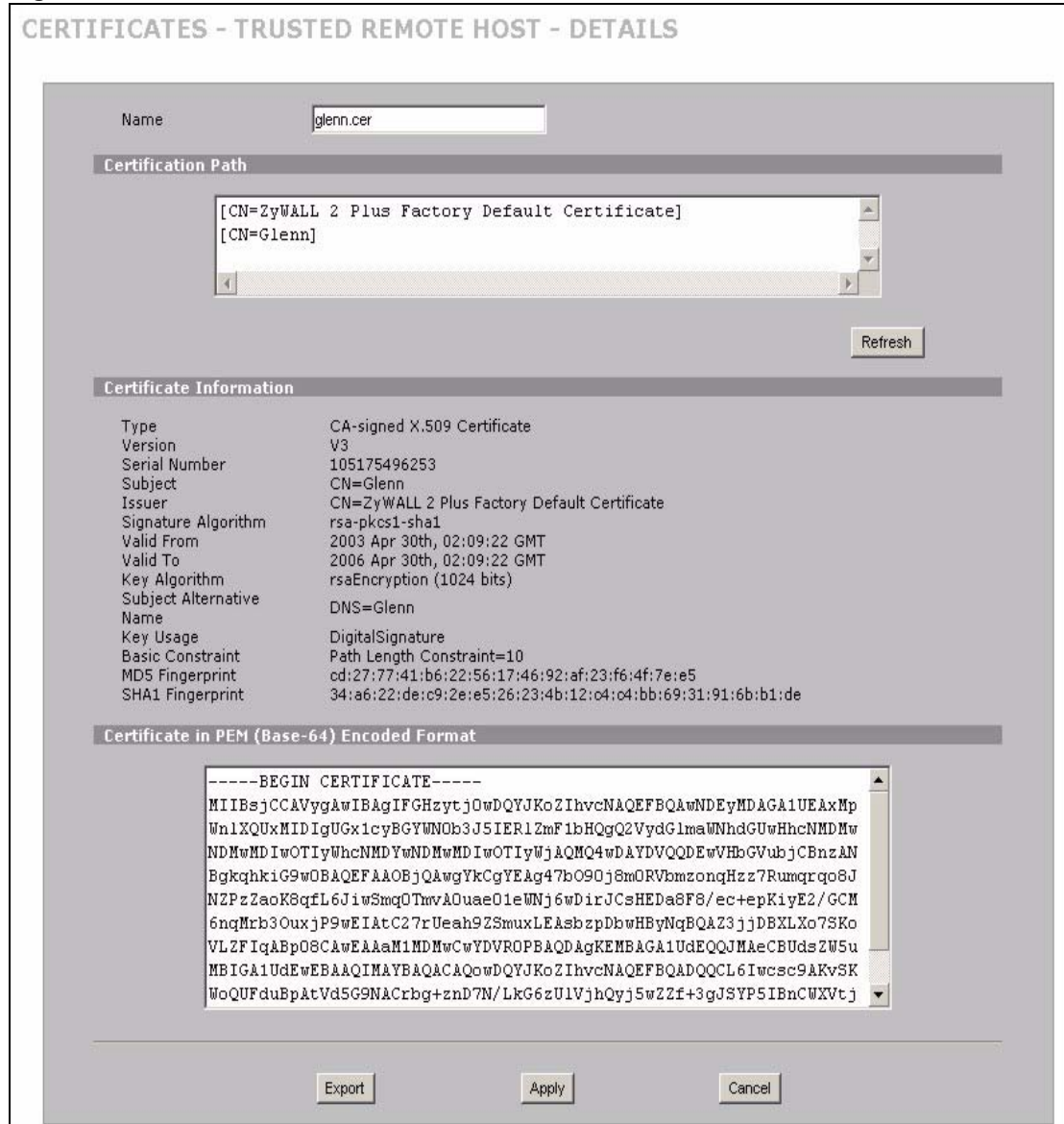
**Table 72** Trusted Remote Host Import

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.

## 12.14 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 115** Trusted Remote Host Details



The following table describes the labels in this screen.

**Table 73** 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 73** Trusted Remote Host Details (continued)

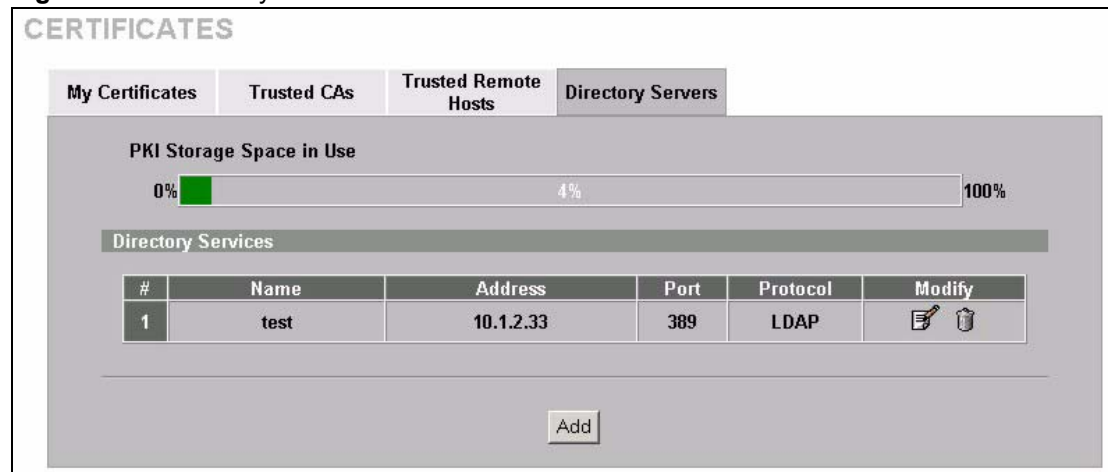
LABEL	DESCRIPTION
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The ZyWALL is the Certification Authority 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 12.12 on page 234</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 12.12 on page 234</a> for how to verify a remote host's certificate.

**Table 73** 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.

## 12.15 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 116** Directory Servers

The following table describes the labels in this screen.

**Table 74** 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.

## 12.16 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 117** 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 75** 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 13

## Authentication Server

This chapter discusses how to configure the ZyWALL's authentication server feature.

### 13.1 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 a RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) server for an unlimited number of users. The ZyWALL uses the local user database for VPN extended authentication.

### 13.2 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.

### 13.3 RADIUS

The ZyWALL can use a RADIUS server to authenticate an unlimited number of users. 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 the ZyWALL acts as a message relay between the client and the network RADIUS server.

### 13.3.1 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the ZyWALL 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 ZyWALL 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 ZyWALL 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.

## 13.4 Local User Database

Click **SECURITY > AUTH SERVER** to open the **Local User Database** screen. Use this screen to change your ZyWALL's local user list.

Figure 118 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 76** 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.

## 13.5 RADIUS

Use RADIUS to authenticate users using an external server.

Click **SECURITY > AUTH SERVER > RADIUS** to open the **RADIUS** screen. Use this screen to set up your ZyWALL's RADIUS server settings.

**Figure 119** RADIUS

The following table describes the labels in this screen.

**Table 77** RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select the check box to enable user authentication through an external authentication server. Clear the check box to enable user authentication using the local user profile on the ZyWALL.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	The default port of the RADIUS server for authentication is <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 14

## Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

### 14.1 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.

#### 14.1.1 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 78** 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.

## 14.1.2 What NAT Does

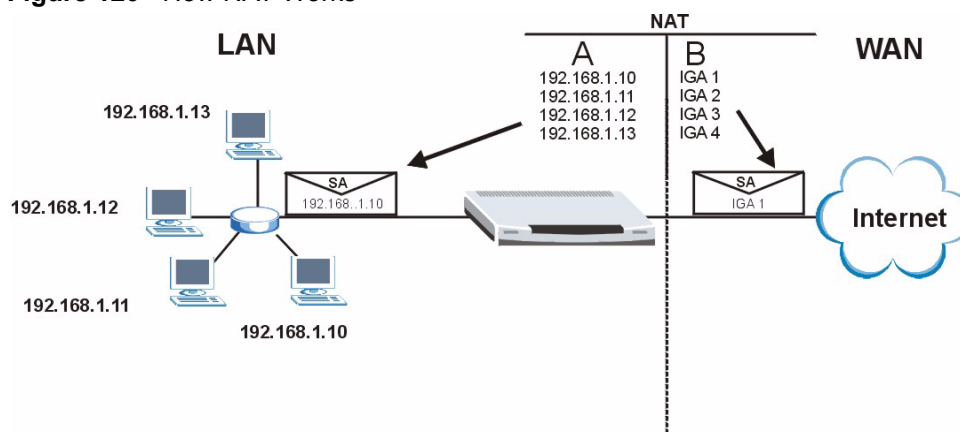
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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. 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)*.

## 14.1.3 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, in which NAT table column **A** shows ILAs and column **B** shows IGAs.

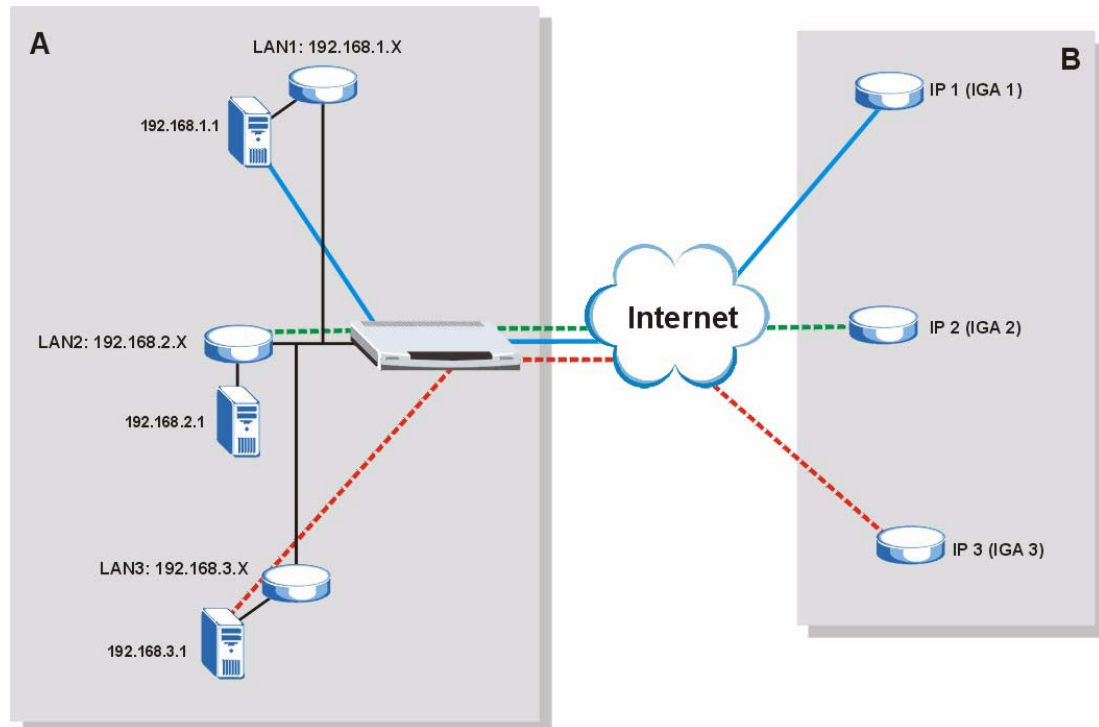
**Figure 120** How NAT Works



### 14.1.4 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. In this example, corporation A's networks are labeled A, and Corporation B's networks are labeled B.

**Figure 121** NAT Application With IP Alias



The following table describes the routes in this example.

**Table 79** NAT Application With IP Alias

WAN ADDRESS	LAN ADDRESS (DEFAULT IPS)
IGA1 	192.168.1.1
IGA2 	192.168.2.1
IGA3 	192.168.3.1

### 14.1.5 Port Restricted Cone NAT

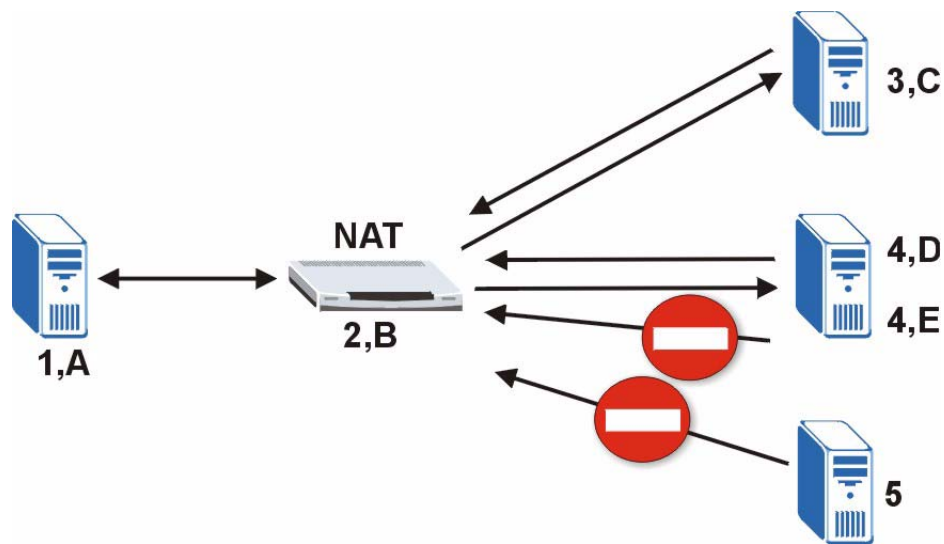
At the time of writing ZyWALL ZyNOS version 4.00 uses port restricted cone NAT. Port restricted cone NAT maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the ZyWALL maps the source address of all packets 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 122** Port Restricted Cone NAT Example



### 14.1.6 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.

**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 80** 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

## 14.2 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.

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

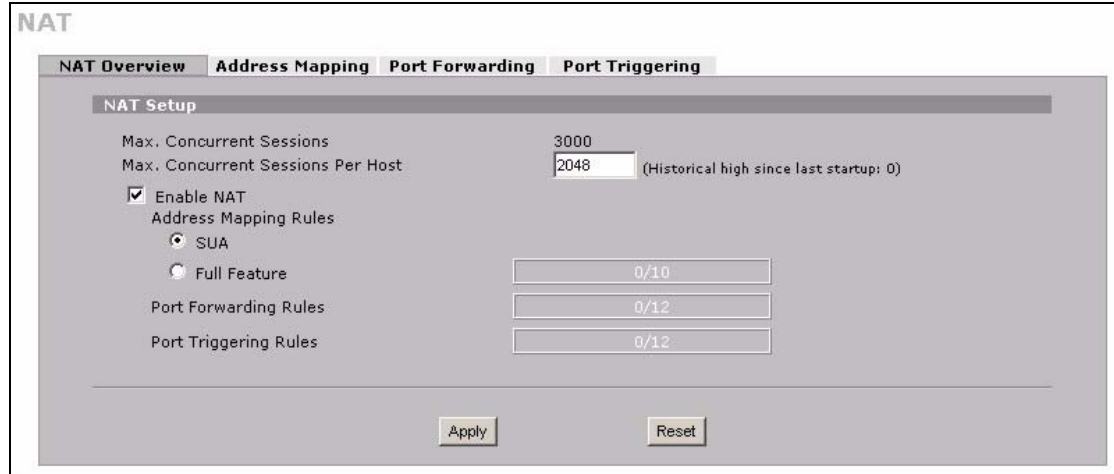
SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.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

Selecting **SUA** means (latent) multiple WAN-to-LAN address translation. That means that computers on your LAN 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 LAN.

## 14.3 NAT Overview

Click **ADVANCED > NAT** to open the **NAT Overview** screen.

**Figure 123** NAT Overview



The following table describes the labels in this screen.

**Table 81** 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.
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	Select <b>SUA</b> to have the ZyWALL use its permanent, pre-defined NAT address mapping rules. 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. The bar displays how many of the ZyWALL's possible address mapping rules are configured. The first number shows how many address mapping rules are configured on the ZyWALL. The second number shows the maximum number of address mapping rules that can be configured on the ZyWALL.
Port Forwarding Rules	The bar displays how many of the ZyWALL's possible port forwarding rules are configured. The first number shows how many port forwarding rules are configured on the ZyWALL. The second number shows the maximum number of port forwarding rules that can be configured on the ZyWALL.
Port Triggering Rules	The bar displays how many of the ZyWALL's possible trigger port rules are configured. The first number shows how many trigger port rules are configured on the ZyWALL. The second number shows the maximum number of trigger port rules that can be configured on the ZyWALL.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 14.4 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.

Click **ADVANCED > NAT > Address Mapping** to open the following screen. The screen appears as shown (some of the screen's blank rows are not shown). Use this screen to change your ZyWALL's address mapping settings.

**Figure 124** 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

#	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	...	...	...	...	-	 

Insert new rule before rule  (rule number).

The following table describes the labels in this screen.

**Table 82** NAT Address Mapping

LABEL	DESCRIPTION
SUA Address Mapping Rules	This read-only table displays the default address mapping rules.
Full Feature 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.
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.

### 14.4.1 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 125** NAT Address Mapping Edit

**NAT - ADDRESS MAPPING**

**Address Mapping Rule**

Type: One-to-One

Local Start IP: 0 . 0 . 0 . 0

Local End IP: N/A

Global Start IP: 0 . 0 . 0 . 0

Global End IP: N/A

Apply Cancel

The following table describes the labels in this screen.

**Table 83** NAT Address Mapping Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. <ol style="list-style-type: none"> <li><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><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><b>Many-to-Many Overload:</b> Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</li> <li><b>Many One-to-One:</b> Many One-to-One mode maps each local IP address to unique global IP addresses.</li> <li><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.

## 14.5 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.

### 14.5.1 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.

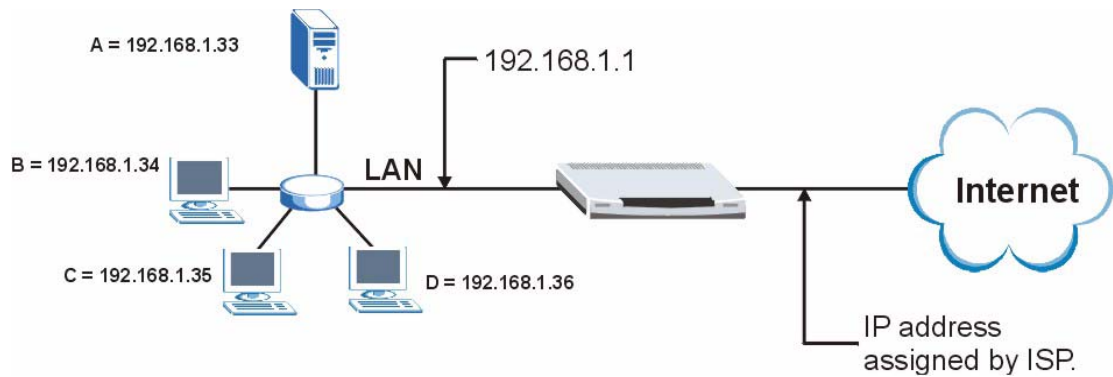
**Note:** If you do not assign a **Default Server IP** address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

### 14.5.2 Port Forwarding: Services and Port Numbers

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network. See [Appendix E on page 541](#) for a list of commonly used services and port numbers.

### 14.5.3 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.

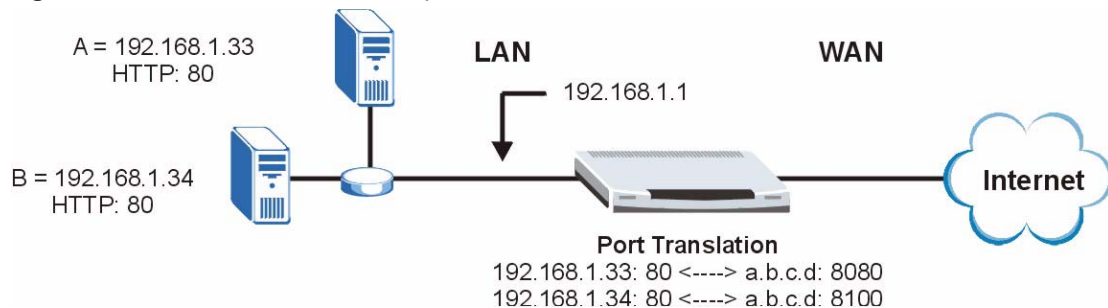
**Figure 126** Multiple Servers Behind NAT Example

## 14.5.4 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. When you use port forwarding without port translation, a single server on the LAN 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 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 127** Port Translation Example

## 14.6 Port Forwarding 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.

Click **ADVANCED > NAT > Port Forwarding** to open the **Port Forwarding** screen.

Refer to [Appendix E on page 541](#) 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 128** Port Forwarding

**NAT**

**NAT Overview** | **Address Mapping** | **Port Forwarding** | **Port Triggering**

**Port Forwarding Rules**

Default Server: 192 . 168 . 1 . 5

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	WebServer	80 - 80	0 - 0	192 . 168 . 1 . 12
2	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
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
11	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
*	<input type="checkbox"/>	RR-Reserved	1026 - 1026	0 - 0	192 . 168 . 1 . 1

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 84** Port Forwarding

LABEL	DESCRIPTION
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a <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.
#	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.
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.

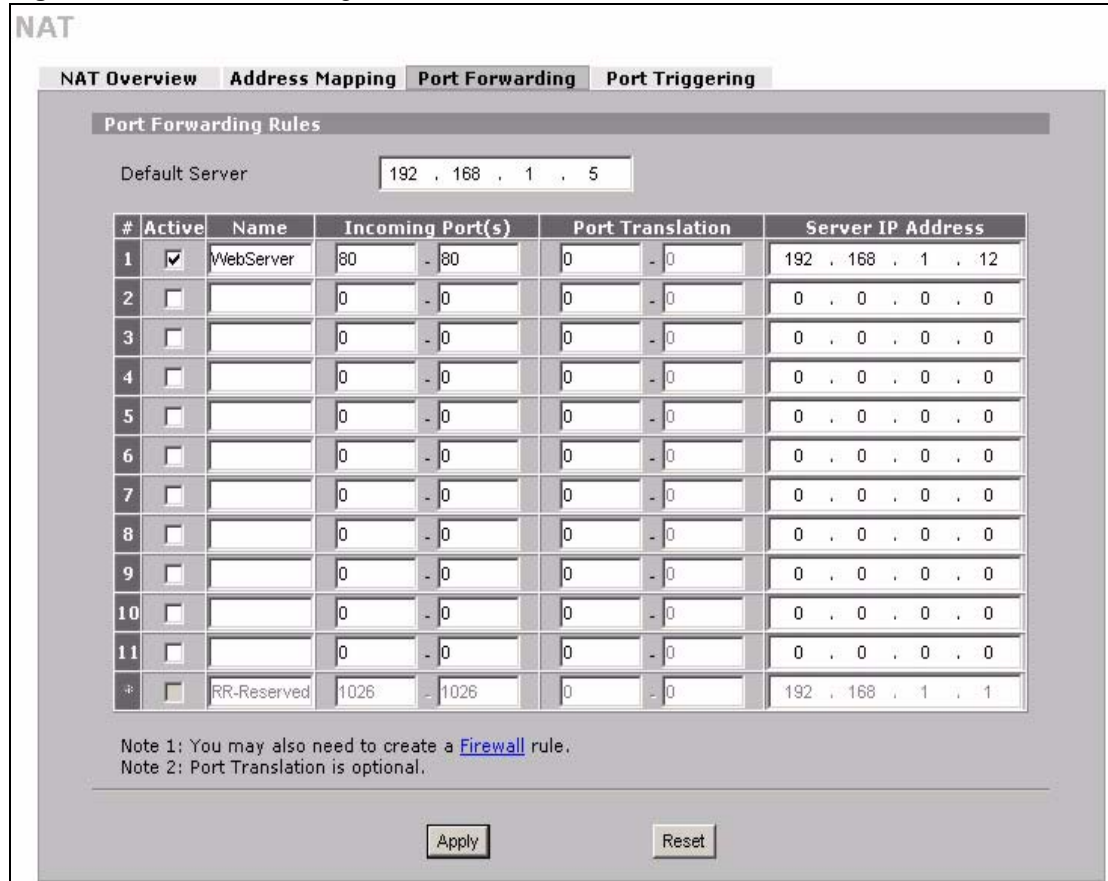
## 14.7 Port Forwarding WAN to LAN HTTP Rule Example

The following example shows how to configure a port forwarding rule to allow access from the WAN to a public HTTP (web) server at LAN IP address 192.168.1.12.

**Note:** You would also need to configure a corresponding firewall rule in order to allow access from the WAN to the server.

- 1 Select the **Active** check box to turn on the rule.
- 2 Specify a name for the rule.
- 3 List port 80 as the incoming port (list it twice).
- 4 Specify the IP address of the HTTP server on the LAN (192.168.1.12 in this example).

**Figure 129** Port Forwarding



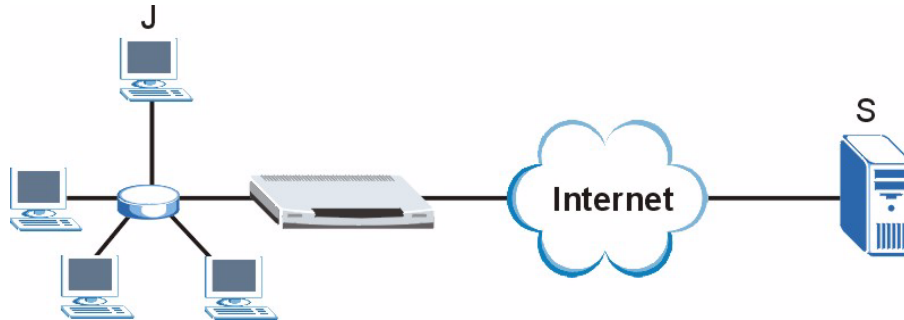
## 14.8 Port Triggering

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 130** Trigger Port Forwarding Process: Example



- 1** Jane's computer, labeled **J** in the figure, requests a file from the Real Audio server (port 7070) labeled **S** in the figure.
- 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 > Port Triggering**. The screen appears as shown.

**Figure 131** Port Triggering

**NAT**

NAT Overview | Address Mapping | Port Forwarding | **Port Triggering**

Port Triggering Rules

#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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

Apply      Reset

The following table describes the labels in this screen.

**Table 85** Port Triggering

LABEL	DESCRIPTION
#	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.
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 15

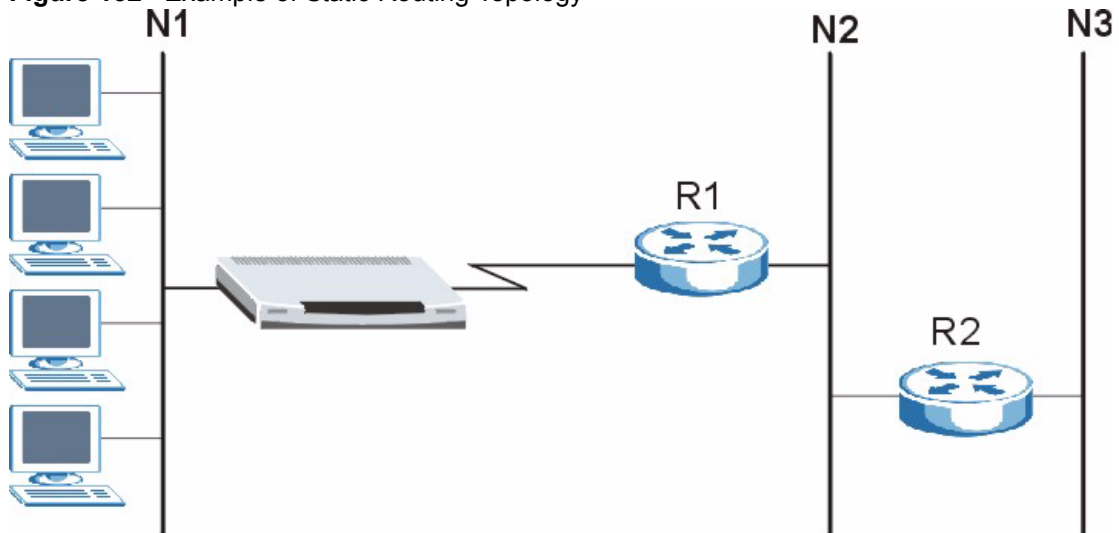
## Static Route

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

### 15.1 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 132** Example of Static Routing Topology



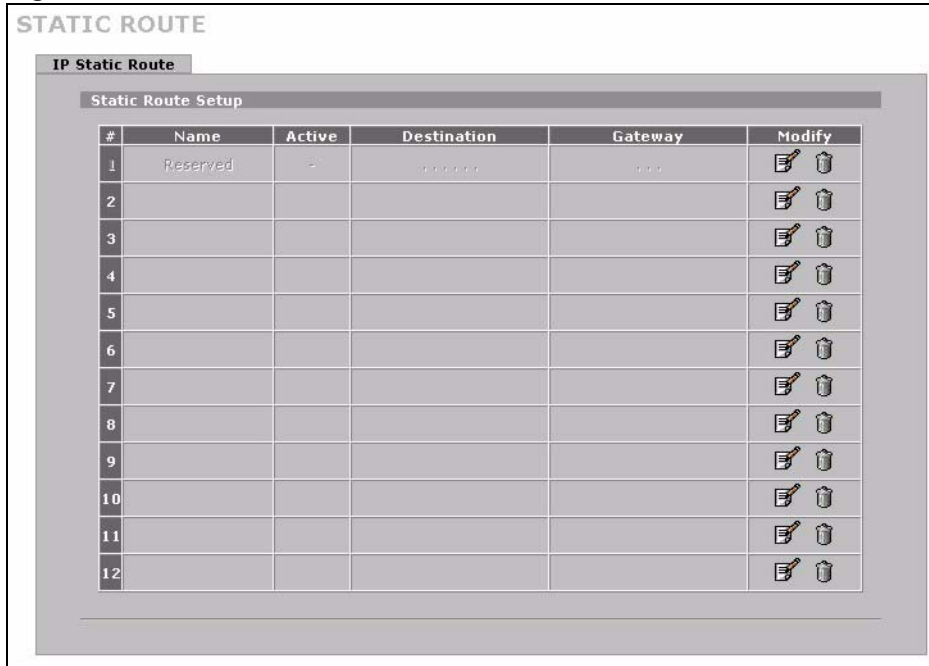
### 15.2 IP Static Route Screen

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

**Note:** The first static route entry is for the default WAN route. You cannot modify or delete it. The name 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 133** IP Static Route



The following table describes the labels in this screen.

**Table 86** IP Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Name	This is the name that describes or identifies this route.
Active	This field shows whether this static route is active ( <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.

### 15.2.1 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 134** IP Static Route Edit

The following table describes the labels in this screen.

**Table 87** 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.
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 16

## Bandwidth Management

This chapter describes the functions and configuration of bandwidth management with multiple levels of sub-classes.

### 16.1 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.

### 16.2 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 16.11.1 on page 278](#)) 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 16.11 on page 277](#) for details).

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

## 16.3 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.

## 16.4 Application-based Bandwidth Management

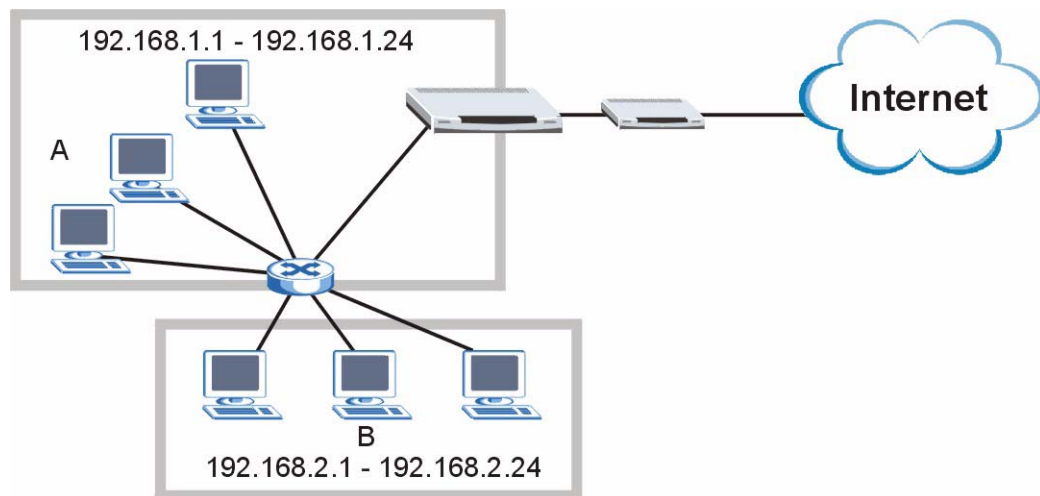
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

## 16.5 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 135** Subnet-based Bandwidth Management Example



## 16.6 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 88** 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

## 16.7 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.

### 16.7.1 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.

### 16.7.2 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.

### 16.7.3 Maximize Bandwidth Usage

The maximize bandwidth usage option (see [Figure 136 on page 276](#)) 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.

### 16.7.4 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 16.8 on page 274](#)).

### 16.7.5 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 89** 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.



### 16.7.5.1 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 90** 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.

### 16.7.5.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the amount of bandwidth that each class gets.

**Table 91** 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.

## 16.8 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 16.8.1 on page 274](#)).

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.

### 16.8.1 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 92** 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.

## 16.9 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.

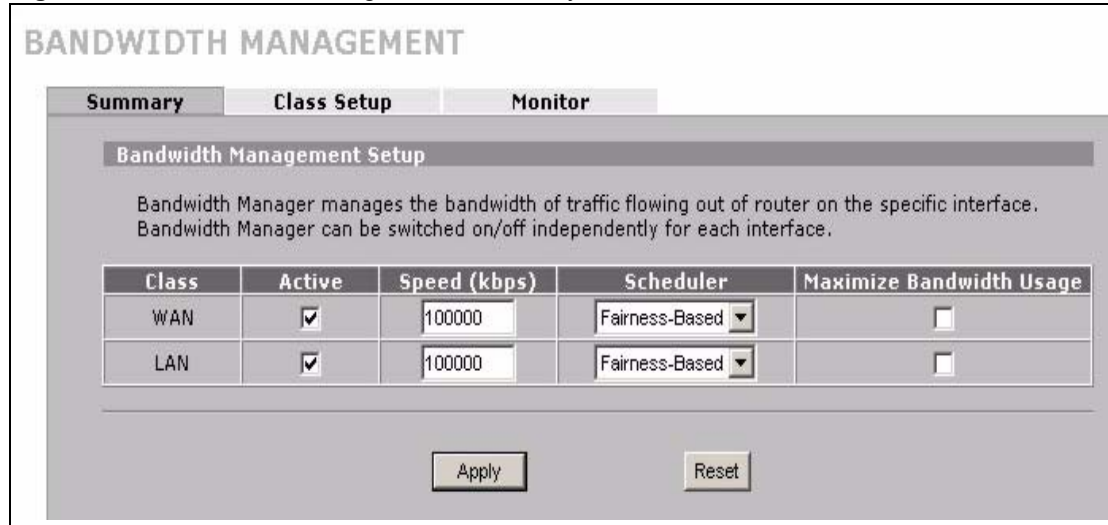
- 1 The ZyWALL sends traffic according to each bandwidth class's bandwidth budget.
- 2 The ZyWALL assigns a parent class's unused bandwidth to its sub-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The ZyWALL gives priority to sub-classes of higher priority and 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.

## 16.10 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 136** Bandwidth Management: Summary



The following table describes the labels in this screen.

**Table 93** 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 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 16.11 on page 277</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 16.7 on page 271</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 16.7.4 on page 272</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.

## 16.11 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 16.10 on page 275](#) 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 > Class Setup**. The screen appears as shown (with example classes).

**Figure 137** 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 94** 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 94** 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.

### 16.11.1 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 > Class Setup**. Click the **Add Sub-Class** button to open the following screen.

**Figure 138** Bandwidth Management: Edit Class

**BANDWIDTH MANAGEMENT - EDIT CLASS**

---

**Class Configuration**

Class Name:

Bandwidth Budget:  (Kbps)

Priority:  (0-7)

Borrow bandwidth from parent class

---

**Filter Configuration**

Enable Bandwidth Filter

Service:

Destination IP Address:

Destination Subnet Mask:

Destination Port:

Source IP Address:

Source Subnet Mask:

Source Port:

Protocol ID:

The following table describes the labels in this screen.

**Table 95** 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	<p>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.</p> <p>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.</p> <p>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 16.7.4 on page 272</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 93 on page 276</a>).</p>
Filter Configuration	

**Table 95** 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 D on page 533</a> for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See <a href="#">Appendix E on page 541</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 D on page 533</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 95** Bandwidth Management: Edit Class (continued)

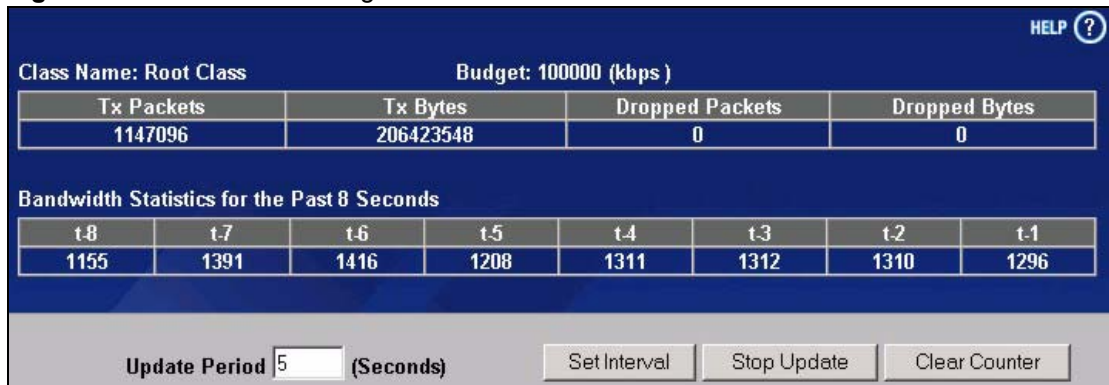
LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

**Table 96** Services and Port Numbers

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

## 16.11.2 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 139** Bandwidth Management: Statistics

The following table describes the labels in this screen.

**Table 97** 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.

## 16.12 Configuring Monitor

Click **ADVANCED > BW MGMT > Monitor** to open the following screen. Use this screen to view the device's bandwidth usage and allotments.

**Figure 140** Bandwidth Management: Monitor

Class	Budget (kbps)	Current Usage (kbps)
Root Class	100000	25
Admin	15000	0
COE	5000	0
CPE	5000	0
Default Class	85000	25

The following table describes the labels in this screen.

**Table 98** 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 17

## DNS

This chapter shows you how to configure the DNS screens.

### 17.1 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.

### 17.2 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 17.5.1 on page 286](#)).

### 17.3 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.
- 3 Use the **REMOTE MGMT DNS** screen to configure the ZyWALL (in router mode) to accept or discard DNS queries.

## 17.4 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.

### 17.4.1 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.

## 17.5 Name Server Record

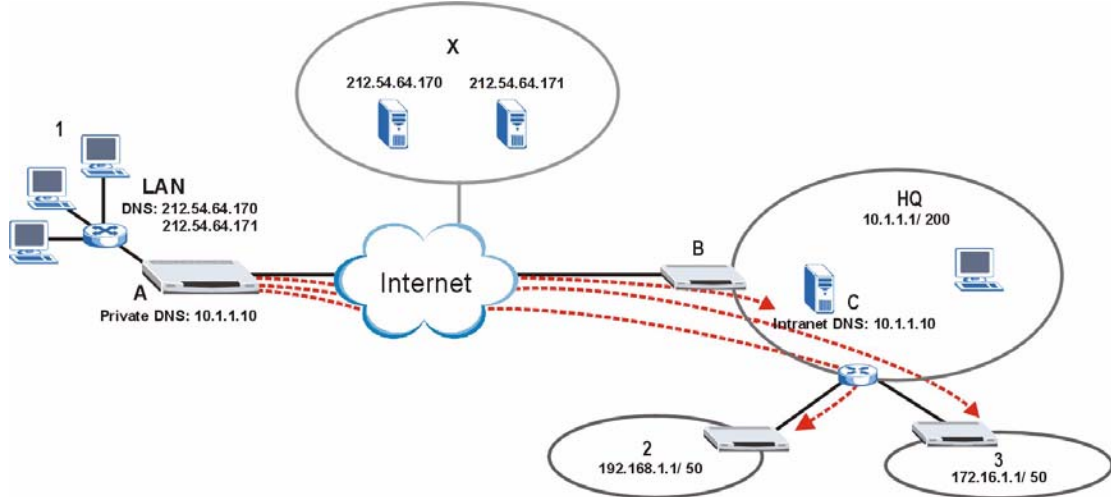
A name server record contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. A domain zone may also be included. A domain zone is a fully qualified domain name without the host. For example, `zyxel.com.tw` is the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

### 17.5.1 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 (shown by dashed lines) are created from ZyWALL A; one to branch office **2**, one to branch office **3** and another to headquarters (**HQ**) through a remote IPsec router (**B**). 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 (**C**) in headquarters. ISP DNS servers are labeled **X**.

**Figure 141** 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.

## 17.6 System Screen

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

**Figure 142** System DNS

**DNS**

System    Cache    DHCP    DDNS

---

**Address Record**

#	FQDN	Wildcard	IP Address	Modify
1	www.zyxel.com.tw	No	172.23.23.41 (WAN)	

Add

---

**Name Server Record**

#	Domain Zone	From	DNS Server	Modify
1	*	WAN (172.23.23.41)	172.23.5.1 172.23.5.2	
-	*	Default	172.23.5.1 172.23.5.2	N/A

Insert new record before record  (record number)

The following table describes the labels in this screen.

**Table 99** 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 100 on page 289</a> for information on the fields.
Name Server Record	A name server record contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. When the ZyWALL needs to resolve a domain name, it checks it against the name server record entries in the order that they appear in this list. A "*" indicates a name server record without a domain zone. The default record is grayed out. The ZyWALL uses this default record if the domain name that needs to be resolved does not match any of the other name server records.
#	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 101 on page 290</a> for information on the fields.

## 17.6.1 Adding an Address Record

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



**Figure 143** System DNS: Add Address Record

The following table describes the labels in this screen.

**Table 100** 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 the 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.

## 17.6.2 Inserting a Name Server record

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

**Figure 144** System DNS: Insert Name Server Record

The following table describes the labels in this screen.

**Table 101** 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 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.

## 17.7 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.

## 17.8 Configure DNS Cache

To configure your ZyWALL's DNS caching, click **ADVANCED > DNS > Cache**. The screen appears as shown.

**Figure 145** DNS Cache

**DNS**

System Cache DHCP DDNS

**DNS Cache Setup**

Cache Positive DNS Resolutions  
Maximum TTL  (60~3600 sec)

Cache Negative DNS Resolutions  
Negative Cache Period  (60~3600 sec)

**DNS Cache Entry**

#	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 102** 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.
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.

## 17.9 Configuring DNS DHCP

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

**Figure 146** DNS DHCP

The screenshot shows the 'DNS DHCP' configuration page. At the top, there are tabs for 'System', 'Cache', 'DHCP', and 'DDNS'. The 'DHCP' tab is selected. Below the tabs is a header 'DNS Servers Assigned by DHCP Server'. Underneath, there is a 'Selected Interface' dropdown menu currently set to 'LAN'. Below that is a table with three rows, each representing a DNS server. The columns are '#', 'DNS', and 'IP'. The first row is '1 First DNS Server', the second is '2 Second DNS Server', and the third is '3 Third DNS Server'. Each row has a 'DNS' dropdown menu set to 'From ISP' and an 'IP' dropdown menu showing the WAN IP and DNS server address. At the bottom of the form are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 103** 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 IP address displays in the field to the right (read-only). The ZyWALL tells the DHCP clients that the ZyWALL itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyWALL, the ZyWALL forwards the query to the ZyWALL's system DNS server (configured in the <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.

## 17.10 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.

### 17.10.1 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.

### 17.10.2 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.

## 17.11 Configuring Dynamic DNS

To change your ZyWALL's DDNS, click **ADVANCED > DNS > DDNS**. The screen appears as shown.

Figure 147 DDNS

**DNS**

System Cache DHCP **DDNS**

**Account Setup**

Active

Service Provider [www.DynDNS.ORG](http://www.DynDNS.ORG)

Username

Password

**My Domain Names**

#	Domain Name	DDNS Type	Offline	Wildcard	IP Address Update Policy
1	ZyWALL	Dynamic	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Use WAN IP Address
2	<input type="text"/>	Dynamic	<input type="checkbox"/>	<input type="checkbox"/>	Use WAN IP Address
3	<input type="text"/>	Dynamic	<input type="checkbox"/>	<input type="checkbox"/>	Use WAN IP Address
4	<input type="text"/>	Dynamic	<input type="checkbox"/>	<input type="checkbox"/>	Use WAN IP Address
5	<input type="text"/>	Dynamic	<input type="checkbox"/>	<input type="checkbox"/>	Use WAN IP Address

Apply Reset

The following table describes the labels in this screen.

Table 104 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	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 104** DDNS

LABEL	DESCRIPTION
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>
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 18

## Remote Management

This chapter provides information on the Remote Management screens.

### 18.1 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 8 on page 131](#) for details on configuring firewall rules.

You may manage your ZyWALL from a remote location via:

- Internet (WAN only)
- LAN only,
- ALL (LAN&WAN)
- Neither (Disable).

**Note:** When you choose **WAN** only or **ALL** (LAN & WAN), 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

#### 18.1.1 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.

### 18.1.2 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.

## 18.2 Introduction to HTTPS

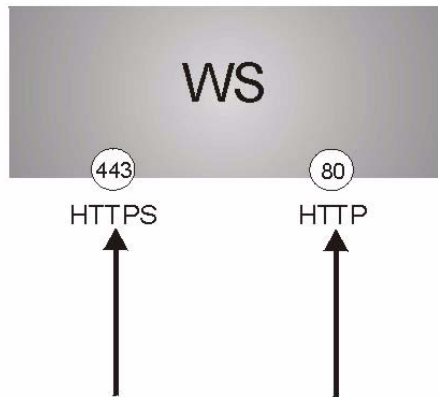
HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the 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 12 on page 217](#) 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 148** HTTPS Implementation

**Note:** If you disable **HTTP Server Access (Disable)** in the **REMOTE MGMT WWW** screen, then the ZyWALL blocks all HTTP connection attempts.

## 18.3 WWW

Click **ADVANCED > REMOTE MGMT** to open the **WWW** screen. Use this screen to change your ZyWALL's web settings.

**Figure 149** WWW

The screenshot shows the **REMOTE MANAGEMENT** interface with the **WWW** tab selected. The interface is divided into sections for **HTTPS** and **HTTP** configurations.

**HTTPS Configuration:**

- Server Certificate: auto\_generated\_self\_signed\_cert (See [My Certificates](#))
- Authenticate Client Certificates (See [Trusted CAs](#))
- Server Port: 443
- Server Access: All
- Secure Client IP Address:  All  Selected (0 . 0 . 0 . 0)

**HTTP Configuration:**

- Server Port: 80
- Server Access: All
- Secure Client IP Address:  All  Selected (0 . 0 . 0 . 0)

**Notes:**

- Note 1: For [UPnP](#) to function normally, the HTTP service must be available for LAN computers using UPnP.
- Note 2: You may also need to create a [Firewall](#) rule.

Buttons for **Apply** and **Reset** are located at the bottom of the configuration area.

The following table describes the labels in this screen.

**Table 105** 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 G on page 557</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	
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.

## 18.4 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.

## 18.4.1 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 150** Security Alert Dialog Box (Internet Explorer)



## 18.4.2 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 151** Security Certificate 1 (Netscape)**Figure 152** Security Certificate 2 (Netscape)

### 18.4.3 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 G on page 557](#) 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 156 on page 305](#) 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**.

## 18.4.4 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 153** Login Screen (Internet Explorer)



**Figure 154** Login Screen (Netscape)

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

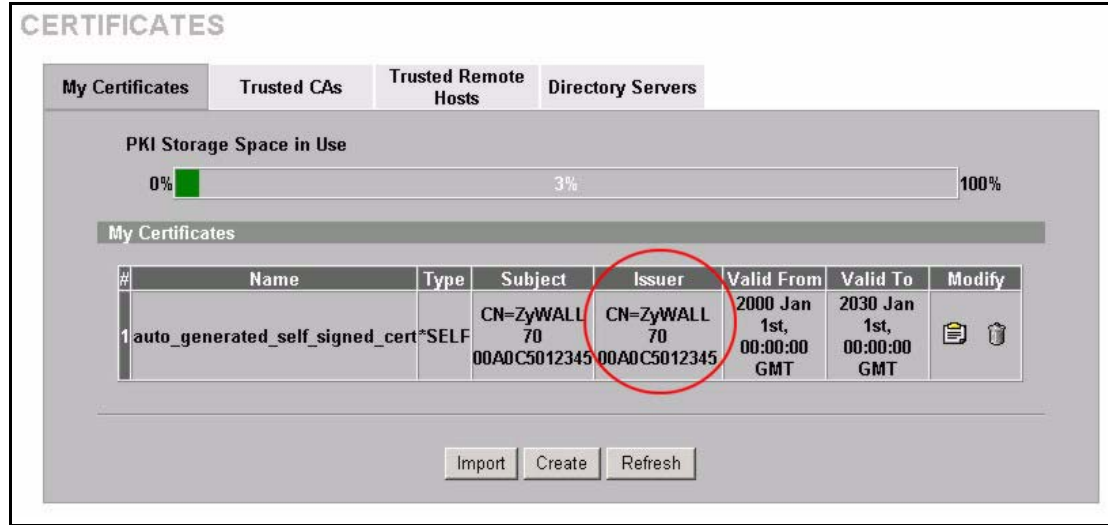
The factory default certificate is a common default certificate for all ZyWALL models.

**Figure 155** 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.

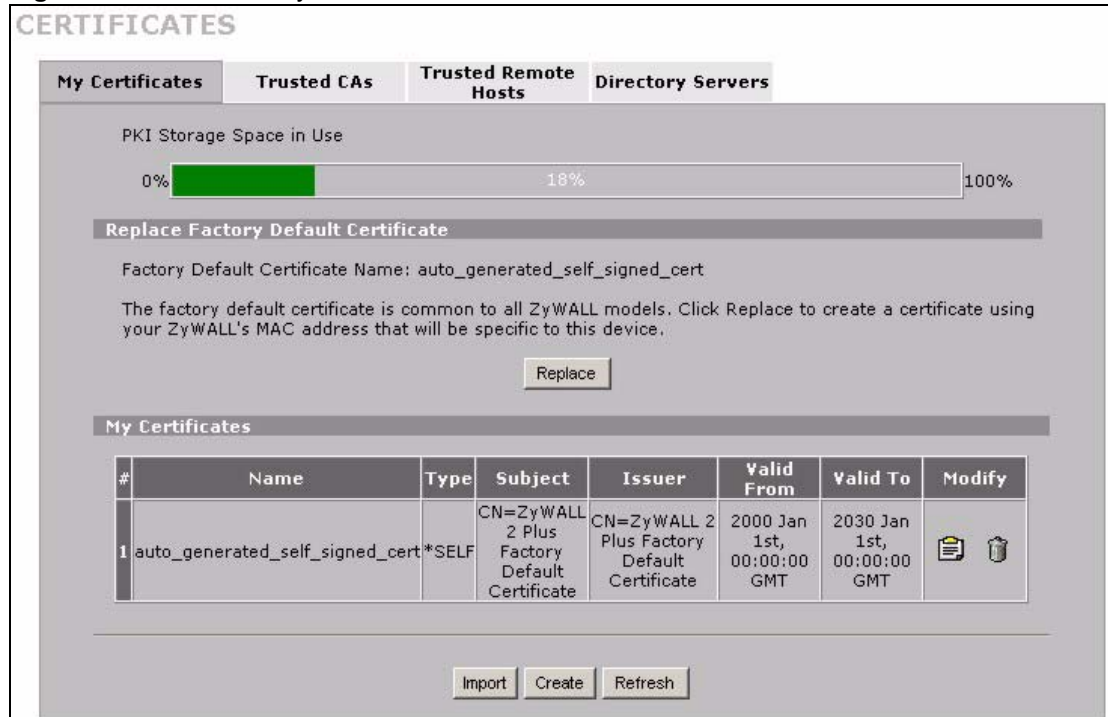


**Figure 156** Device-specific Certificate



Click **Ignore** in the **Replace Certificate** screen to use the common ZyWALL certificate. You will then see this information in the **My Certificates** screen.

**Figure 157** Common ZyWALL Certificate



## 18.5 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. The SSH server is labeled **A**, and the SSH client is labeled **B**.

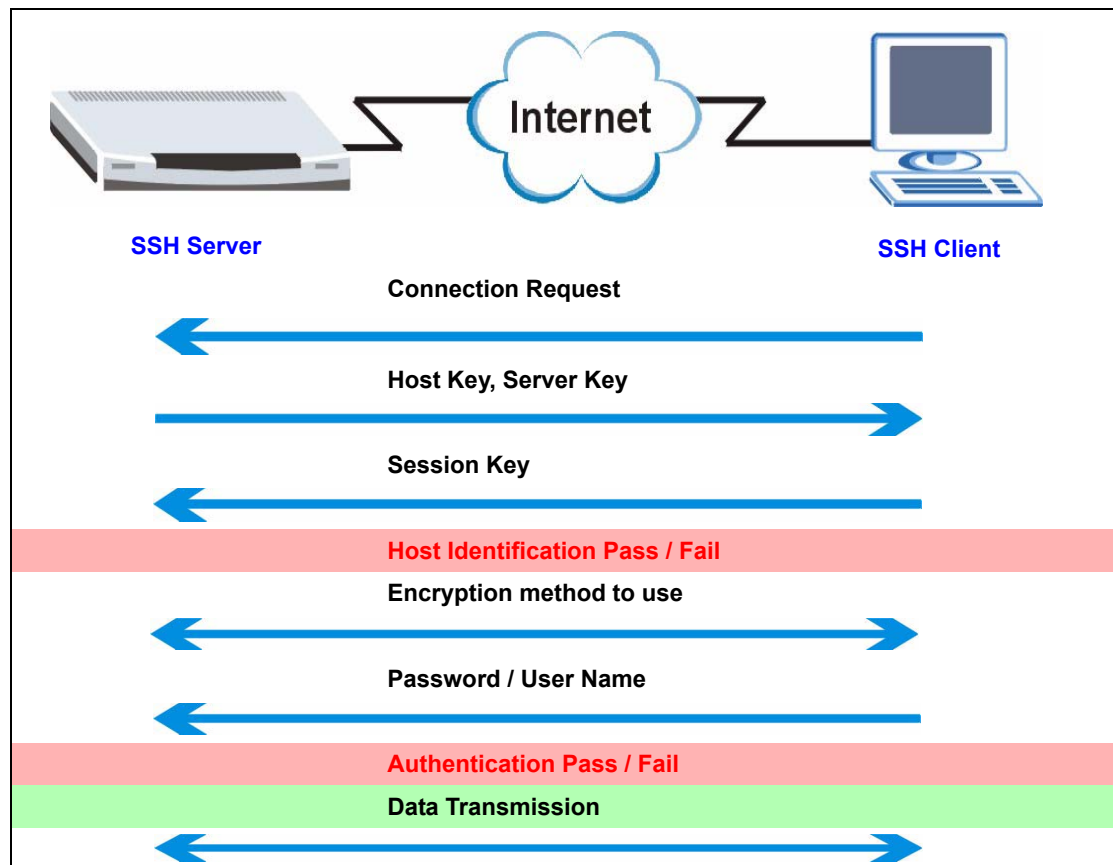
**Figure 158** SSH Communication Example



## 18.6 How SSH Works

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

**Table 106** 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.

# **18.7 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.

## **18.7.1 Requirements for Using SSH**

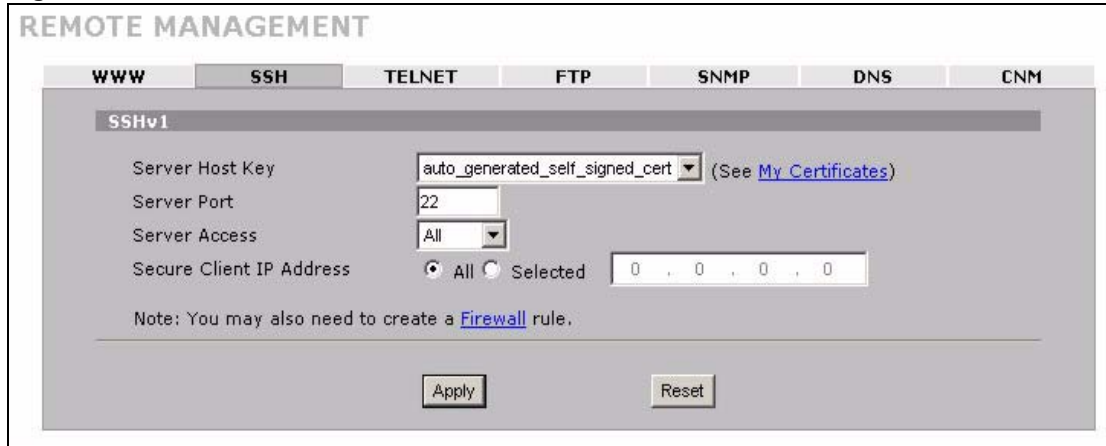
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL over SSH.

# **18.8 Configuring SSH**

Click **ADVANCED > REMOTE MGMT > SSH** 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 159** SSH



The following table describes the labels in this screen.

**Table 107** 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 12 on page 217</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.

## 18.9 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.

### 18.9.1 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 160** SSH Example 1: Store Host Key



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

## 18.9.2 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 161** 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 162** 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.

## 18.10 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.

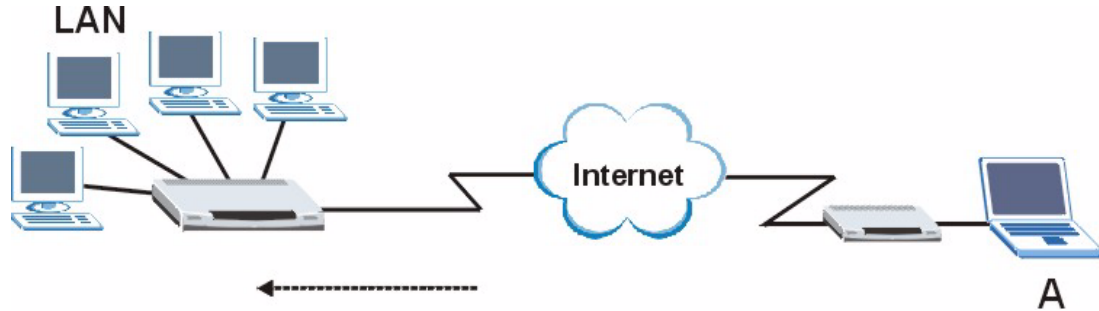
**Figure 163** Secure FTP: Firmware Upload Example

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

## 18.11 Telnet

You can configure your ZyWALL for remote Telnet access as shown next. The computer using telnet to access the LAN is labeled **A**, and the arrow shows the direction of incoming traffic.

**Figure 164** Telnet Configuration on a TCP/IP Network



## 18.12 Configuring TELNET

Click **ADVANCED > REMOTE MGMT > TELNET** to open the Telnet screen. Use this screen 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 165** Telnet

The screenshot shows the 'REMOTE MANAGEMENT' configuration page with the 'TELNET' tab selected. The configuration options are as follows:

- Server Port:** 23
- Server Access:** All
- Secure Client IP Address:** All (selected), Selected (0 . 0 . 0 . 0)

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 of the configuration area.

The following table describes the labels in this screen.

**Table 108** 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.

**Table 108** Telnet (continued)

LABEL	DESCRIPTION
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.

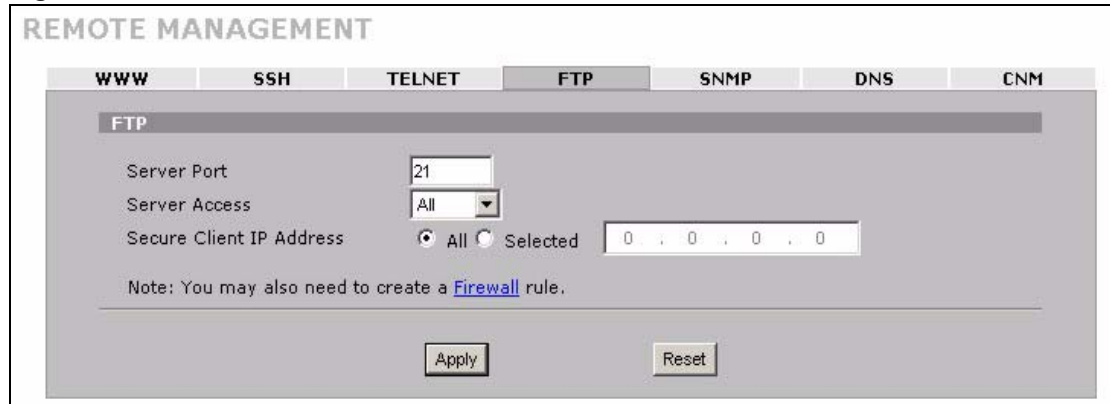
## 18.13 FTP

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 > FTP**. The screen appears as shown.

**Note:** It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

**Figure 166** FTP



The following table describes the labels in this screen.

**Table 109** 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.



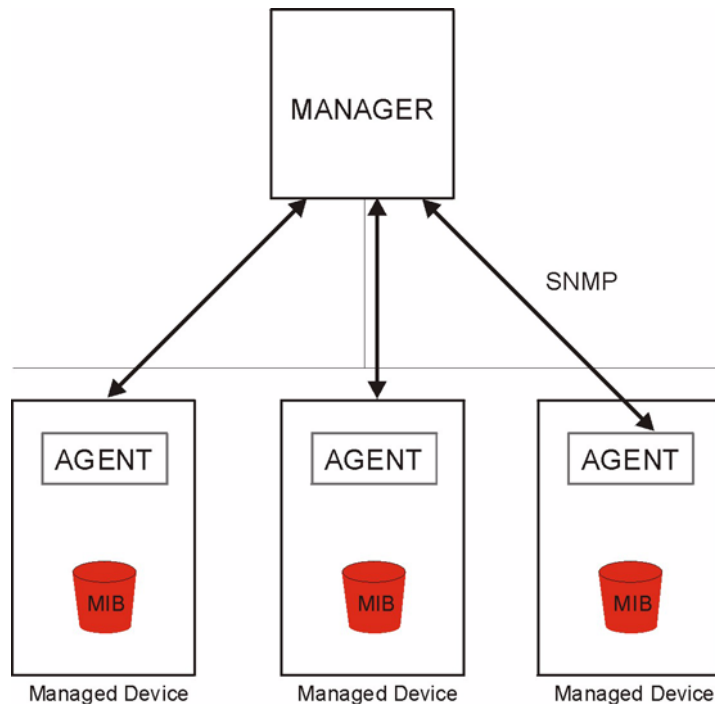
**Table 109** FTP

LABEL	DESCRIPTION
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.

## 18.14 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.

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

**Figure 167** 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.

### 18.14.1 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.

### 18.14.2 SNMP Traps

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

**Table 110** 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, CI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

### 18.14.3 REMOTE MANAGEMENT: SNMP

To change your ZyWALL's SNMP settings, click **ADVANCED > REMOTE MGMT > SNMP**. The screen appears as shown.

**Figure 168** SNMP

The following table describes the labels in this screen.

**Table 111** 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.

**Table 111** SNMP (continued)

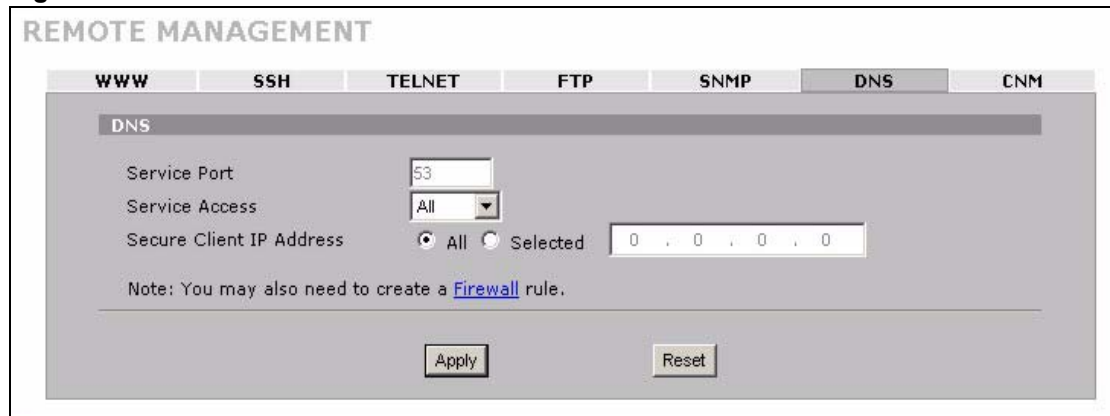
LABEL	DESCRIPTION
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select <b>All</b> to allow any computer to access the ZyWALL using this service. Choose <b>Selected</b> to just allow the computer with the IP address 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.

## 18.15 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 109](#) for more information.

Click **ADVANCED > REMOTE MGMT > DNS** 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 169** DNS



The following table describes the labels in this screen.

**Table 112** DNS

LABEL	DESCRIPTION
Service 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.

**Table 112** DNS

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your customized settings.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 18.16 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.

## 18.17 Configuring CNM

Vantage CNM is disabled on the device by default. Click **ADVANCED > REMOTE MGMT > CNM** to configure your device's Vantage CNM settings.

**Figure 170** CNM

**REMOTE MANAGEMENT**

WWW | SSH | TELNET | FTP | SNMP | DNS | **CNM**

**Registration Information**

Registration Status: Not Registered

Last Registration Time: 0000 - 00 - 00, 00 : 00 : 00

Refresh

**Vantage CNM Setup**

Enable

Vantage CNM Server Address: 0 . 0 . 0 . 0

Encryption Algorithm: 3DES

Encryption Key:

Apply | Reset

The following table describes the labels in this screen.

**Table 113** 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>
Last Registration Time	<p>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.</p>
Refresh	<p>Click <b>Refresh</b> to update the registration status and last registration time.</p>
Vantage CNM Setup	
Enable	<p>Select this check box to allow Vantage CNM to manage your ZyWALL.</p>
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	<p>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.</p>
Encryption Key	<p>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.</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>







# CHAPTER 19

## UPnP

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

### 19.1 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.

#### 19.1.1 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.

#### 19.1.2 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 14 on page 249](#) for further information about NAT.

#### 19.1.3 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.

### 19.1.4 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.

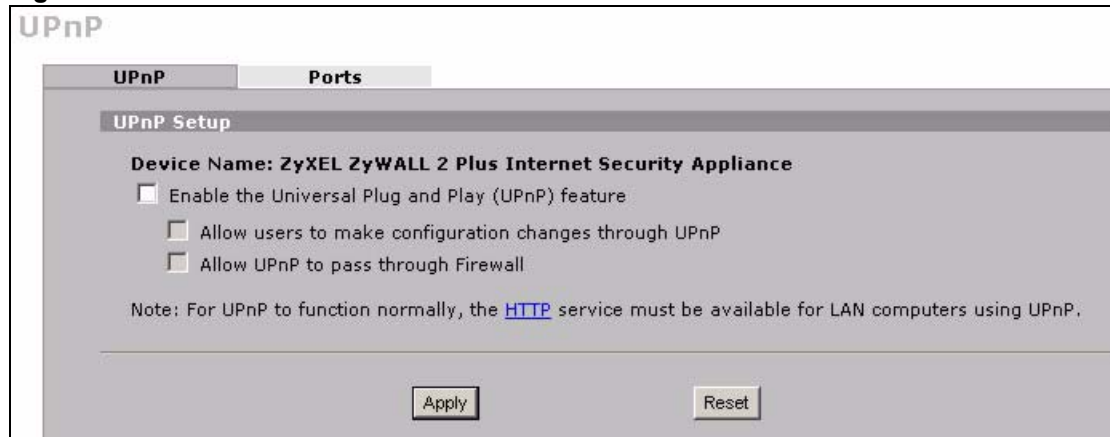
The ZyWALL only sends UPnP multicasts to the LAN.

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.

## 19.2 Configuring UPnP

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

**Figure 171** UPnP



The following table describes the fields in this screen.

**Table 114** UPnP

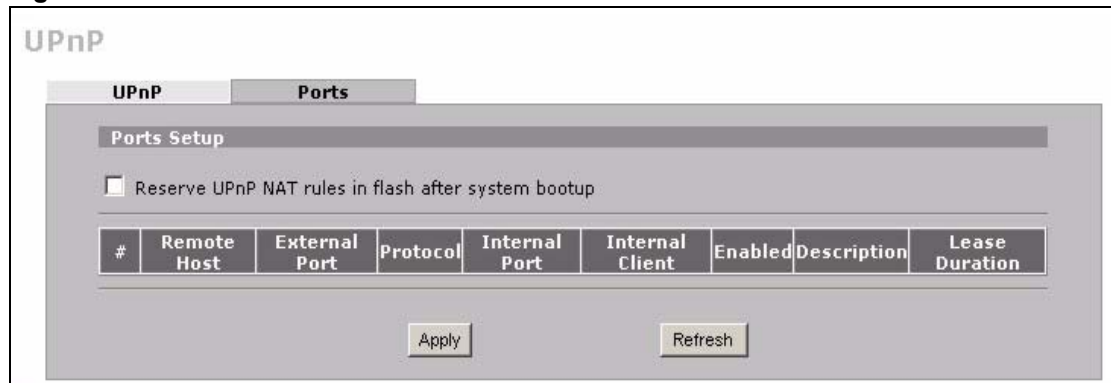
LABEL	DESCRIPTION
UPnP Setup	
Device Name	This identifies the ZyXEL device in UPnP applications.
Enable the Universal Plug and Play (UPnP) feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyWALL's IP address (although you must still enter the password to access the web configurator).

**Table 114** 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).
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 19.3 Displaying UPnP Port Mapping

Click **UPnP > Ports** to display the UPnP Ports screen. Use this screen to view the NAT port mapping rules that UPnP creates on the ZyWALL.

**Figure 172** UPnP Ports

The following table describes the labels in this screen.

**Table 115** 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.
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.

**Table 115** UPnP Ports (continued)

LABEL	DESCRIPTION
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.

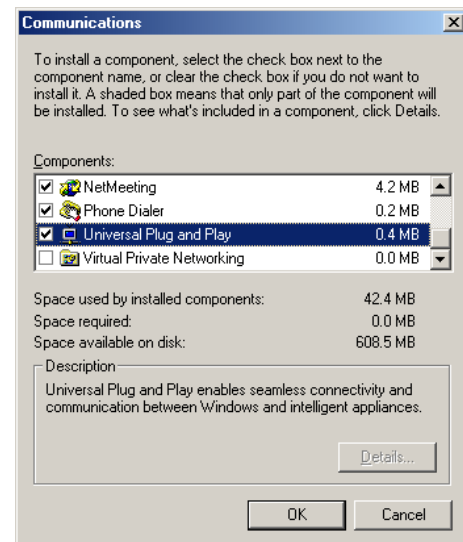
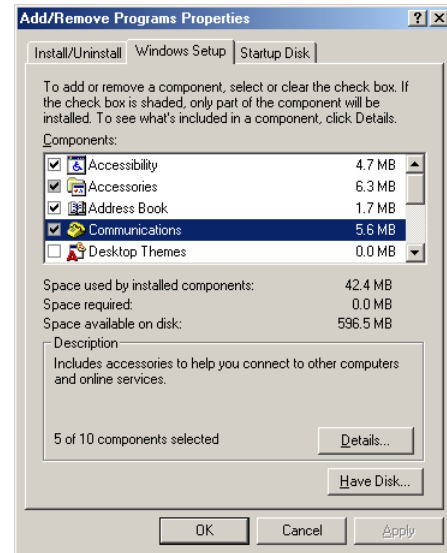
## 19.4 Installing UPnP in Windows Example

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

## 19.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

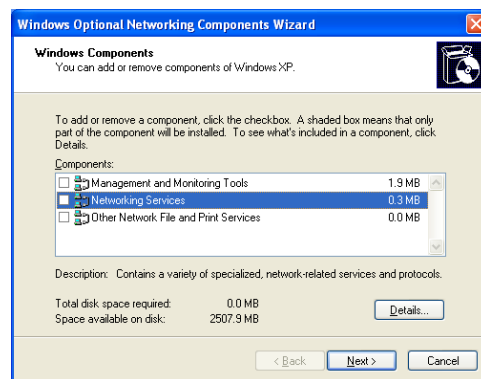
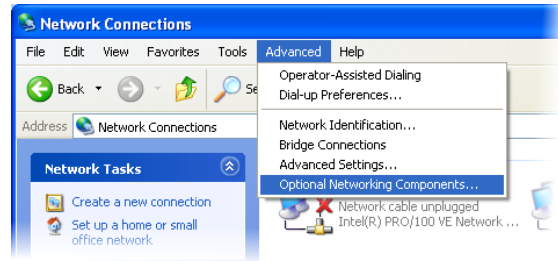
- 1 Click **Start > Settings > Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click **Windows Setup** and select **Communication** in the **Components** selection box. Click **Details**.
- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.
- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.



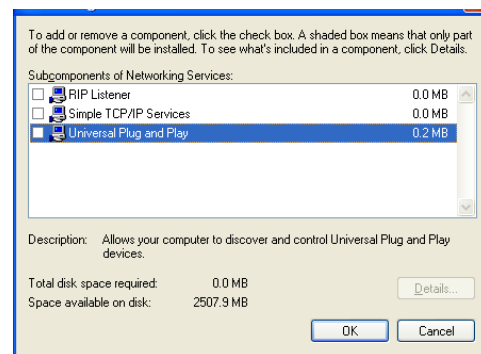
## 19.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

- 1 Click **Start > Settings > 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**.



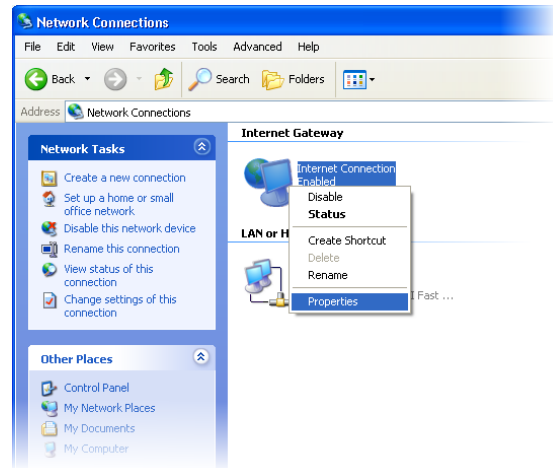
## 19.5 Using UPnP in Windows XP Example

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.

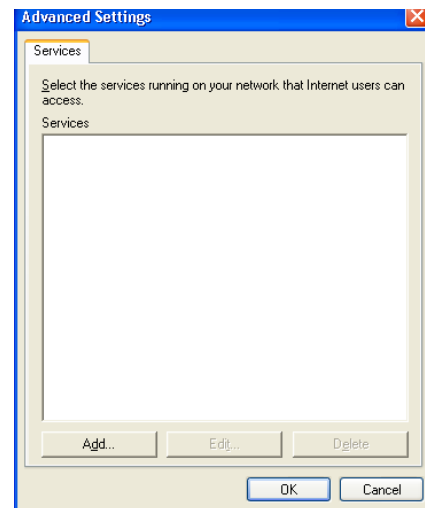
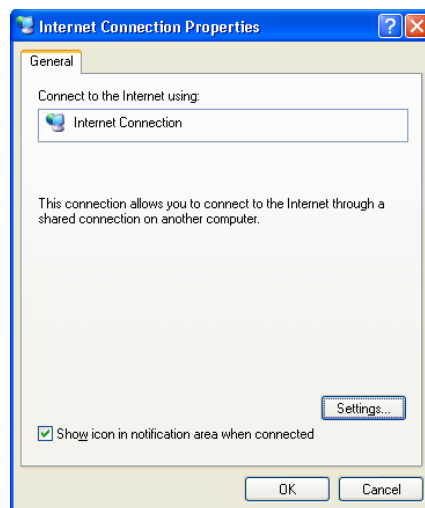
## 19.5.1 Auto-discover Your UPnP-enabled Network Device

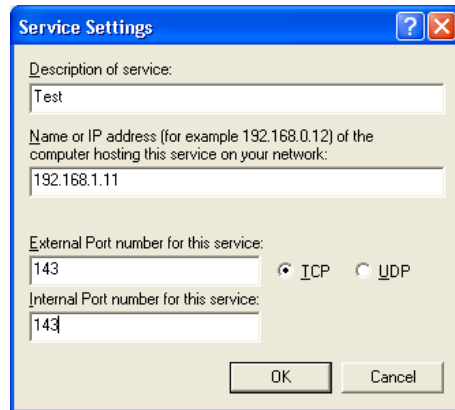
- 1 Click **Start > Control Panel**. Double-click **Network Connections**. An icon displays under **Internet Gateway**.
- 2 Right-click the icon and select **Properties**.



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

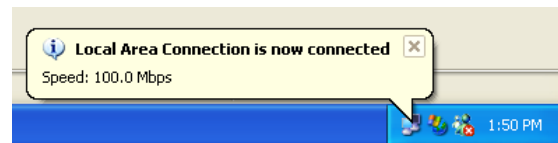
You may edit or delete the port mappings or click **Add** to manually add port mappings.



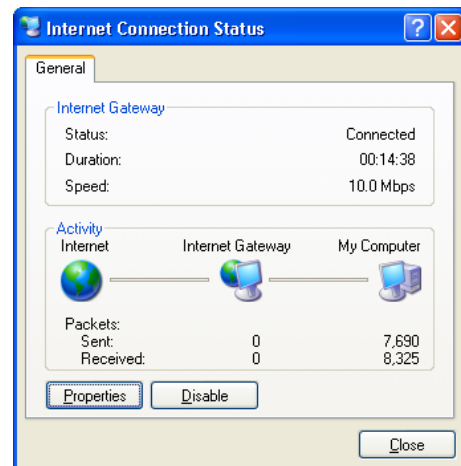


**Note:** When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 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.



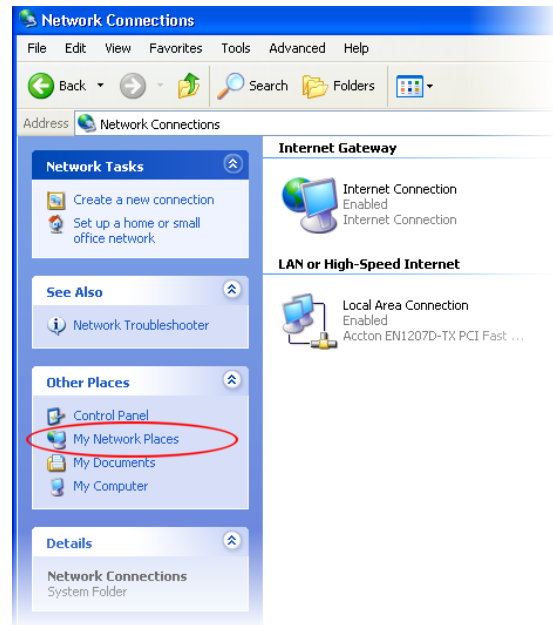
## 19.5.2 Web Configurator Easy Access

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.

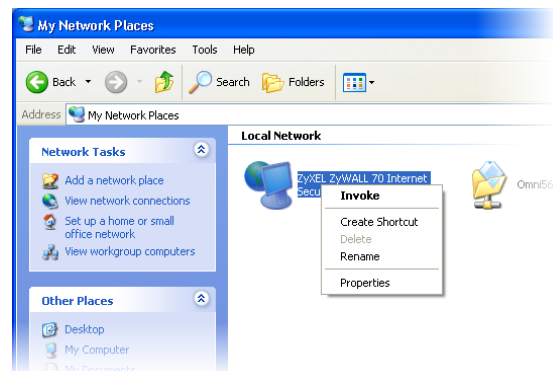


Follow the steps below to access the web configurator.

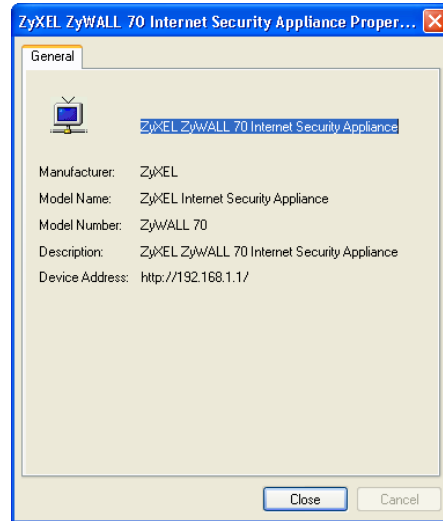
- 1 Click **Start > Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.



- 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 20

## ALG Screen

This chapter covers how to use the ZyWALL's ALG feature to allow certain applications to pass through the ZyWALL.

### 20.1 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.

#### 20.1.1 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**.

#### 20.1.2 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.

## 20.2 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.

## 20.3 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.

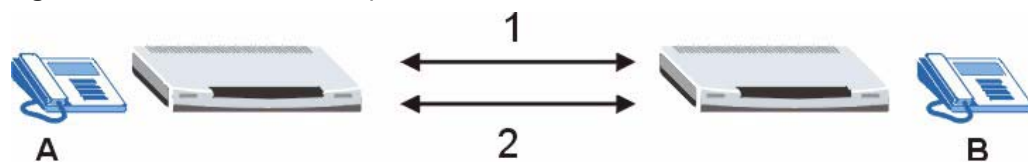
## 20.4 RTP

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.

### 20.4.1 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. The following example shows H.323 signaling and audio sessions between H.323 devices A and B. In this figure, the arrow marked **1** shows a signaling session over TCP port 1720 and the arrow marked **2** shows an audio session using RTP.

**Figure 173** H.323 ALG Example



- 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.

## 20.5 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.

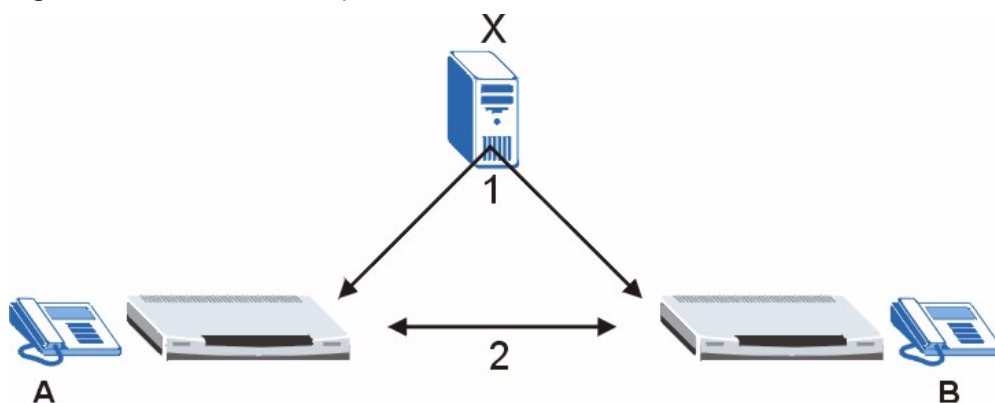
### 20.5.1 STUN

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.

### 20.5.2 SIP ALG Details

- SIP clients can be connected to the LAN. A SIP server must be on the WAN.
- You can make and receive calls between the LAN and the WAN. You cannot make a call between the LAN and the LAN.
- 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 (**X**). The signaling session over UDP port 5060 is shown by the arrow marked **1** and the audio session using RTP is shown by the arrow marked **2**.



### 20.5.3 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.

### 20.5.4 SIP Audio Session Timeout

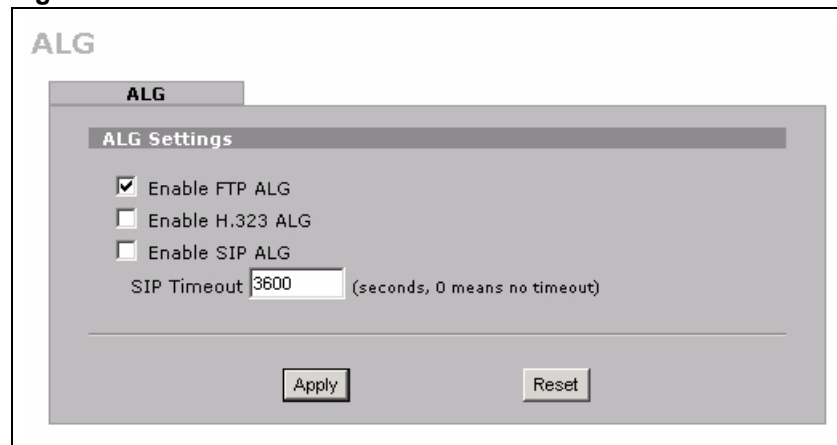
If no voice packets go through the SIP ALG before the timeout period (default 5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

## 20.6 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 175** ALG





The following table describes the labels in this screen.

**Table 116** ALG

<b>LABEL</b>	<b>DESCRIPTION</b>
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 21

## Logs Screens

This chapter contains information about configuring general log settings and viewing the ZyWALL's logs. Refer to [Appendix N on page 587](#) for example log message explanations.

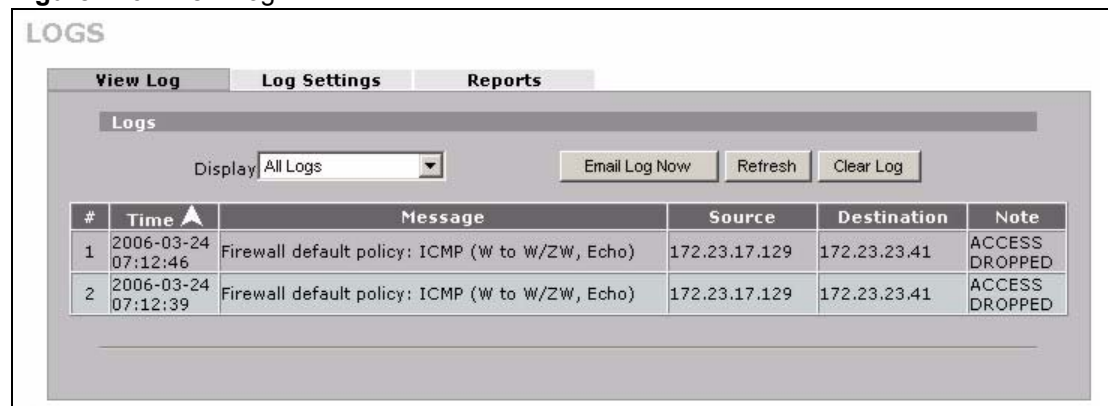
### 21.1 Configuring View Log

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 21.3 on page 342](#)). 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 176** View Log



The following table describes the labels in this screen.

**Table 117** View Log

LABEL	DESCRIPTION
Display	The categories that you select in the <b>Log Settings</b> page (see <a href="#">Section 21.3 on page 342</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.

**Table 117** View Log (continued)

LABEL	DESCRIPTION
Time	This field displays the time the log was recorded. See <a href="#">Section 22.4 on page 353</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 21.3 on page 342</a> ).
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to delete all the logs.

## 21.2 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 118** Example Log Description

LABEL	DESCRIPTION
#	This is log number five.
time	The log was generated on June 8, 2004 at 5:58 and 20 seconds AM.
source	The log was generated due to a NetBIOS packet sent from IP address 172.21.4.187 port 137.
destination	The NetBIOS packet was sent to the 172.21.255.255 subnet port 137. This was a NetBIOS UDP broadcast packet meant to discover devices on the network.
notes	The ZyWALL blocked the packet.
message	The ZyWALL blocked the packet in accordance with the firewall's default policy of blocking sessions that are initiated from the WAN. "UDP" means that this was a User Datagram Protocol packet. "W to W/ZW" indicates that the packet was traveling from the WAN to the WAN or the ZyWALL.

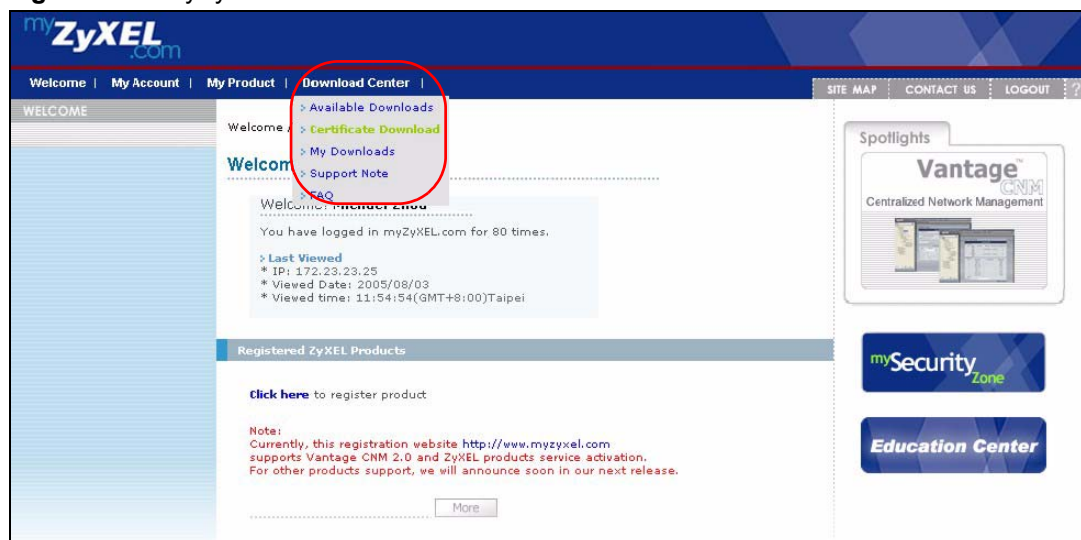
## 21.2.1 Certificate Not Trusted Log Note

myZyXEL.com and the update server use certificate signed by VeriSign to identify themselves. The default configuration file includes a trusted CA certificate signed by VeriSign. 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. If you deleted the trusted CA certificate signed by VeriSign, 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.

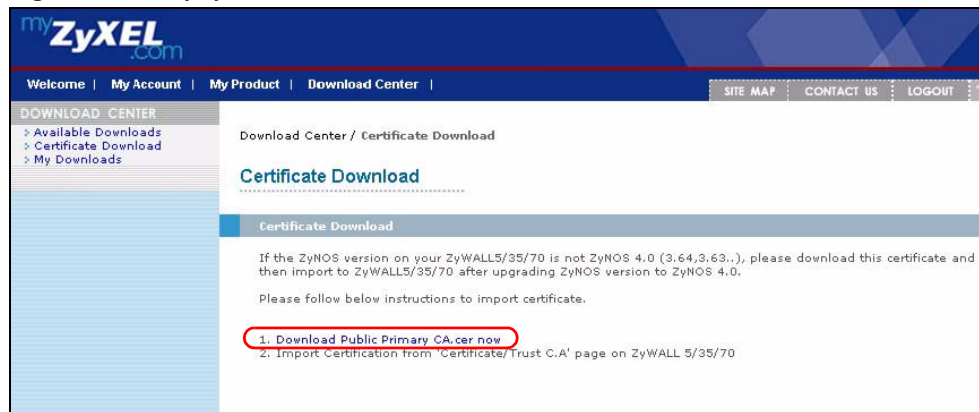
- 1 Go to <http://www.myZyXEL.com> and log in with your account.
- 2 Click **Download Center > Certificate Download**.

**Figure 177** myZyXEL.com: Download Center



- 3 Click the link in the **Certificate Download** screen.

Figure 178 myZyXEL.com: Certificate Download



## 21.3 Configuring Log Settings

To change your ZyWALL's log settings, click **LOGS > Log Settings**. 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 179 Log Settings

## LOGS

View Log
**Log Settings**
Reports

### E-mail Log Settings

Mail Server	<input type="text"/>	(Outgoing SMTP Server Name or IP Address)
Mail Subject	<input type="text"/>	
Mail Sender	<input type="text"/>	(E-Mail Address)
Send Log to	<input type="text"/>	(E-Mail Address)
Send Alerts to	<input type="text"/>	(E-Mail Address)
Log Schedule	None <input type="button" value="v"/>	
Day for Sending Log	Sunday <input type="button" value="v"/>	
Time for Sending Log	0 (Hour) 0 (Minute)	
<input type="checkbox"/> SMTP Authentication		
User Name	<input type="text"/>	
Password	<input type="text"/>	

---

### Syslog Logging

Active

Syslog Server  (Server Name or IP Address)

Log Facility  Local 1

---

#### Log

- System Maintenance
- System Errors
- Access Control
  - Asymmetrical Routes
  - Multicasts / Broadcasts
- TCP Reset
- Packet Filter
- ICMP
- Remote Management
- Call Record
- PPP
- UPnP
- Forward Web Sites
- Blocked Web Sites
- Blocked Java etc.
- Attacks
- IPSec
- IKE
- PKI
- SSL/TLS

#### Send Immediate Alert

- System Errors
- Access Control
- Blocked Web Sites
- Blocked Java etc.
- Attacks
- IPSec
- IKE
- PKI

---

### Log Consolidation

Active

Log Consolidation Period  1 ~ 600 (Seconds)

The following table describes the labels in this screen.

**Table 119** 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 119** 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.

## 21.4 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:

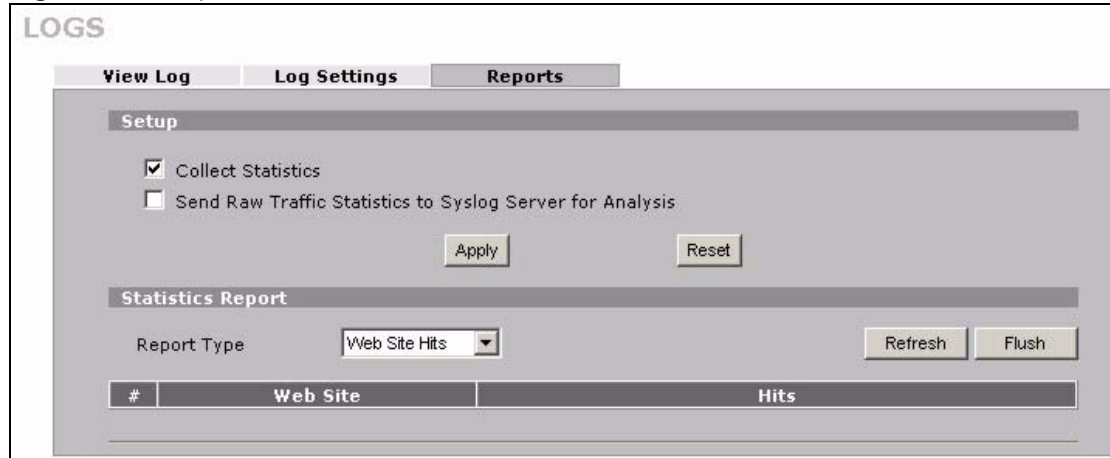
- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN IP addresses to and/or from which the most traffic has been sent
- How much traffic has 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 view your ZyWALL's log reports or change your ZyWALL's log reports settings, click **LOGS > Reports**. The screen appears as shown.

**Figure 180** 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 120** Reports

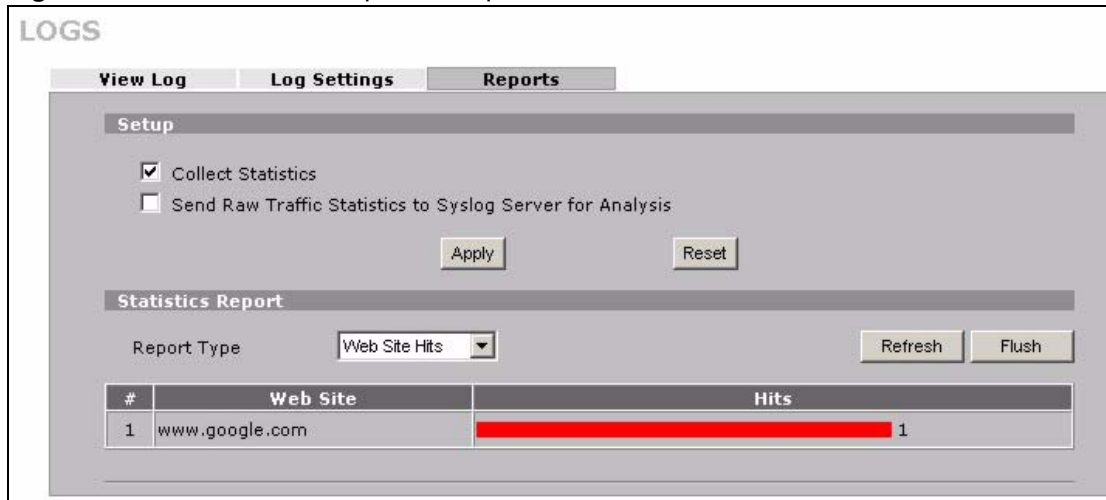
LABEL	DESCRIPTION
Collect Statistics	Select the check box and click <b>Apply</b> to have the ZyWALL record report data.
Send Raw Traffic Statistics to Syslog Server for Analysis	Select the check box and click <b>Apply</b> to have the ZyWALL send unprocessed traffic statistics to a syslog server for analysis. 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.
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 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.

## 21.4.1 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 181** Web Site Hits Report Example



The following table describes the label in this screen.

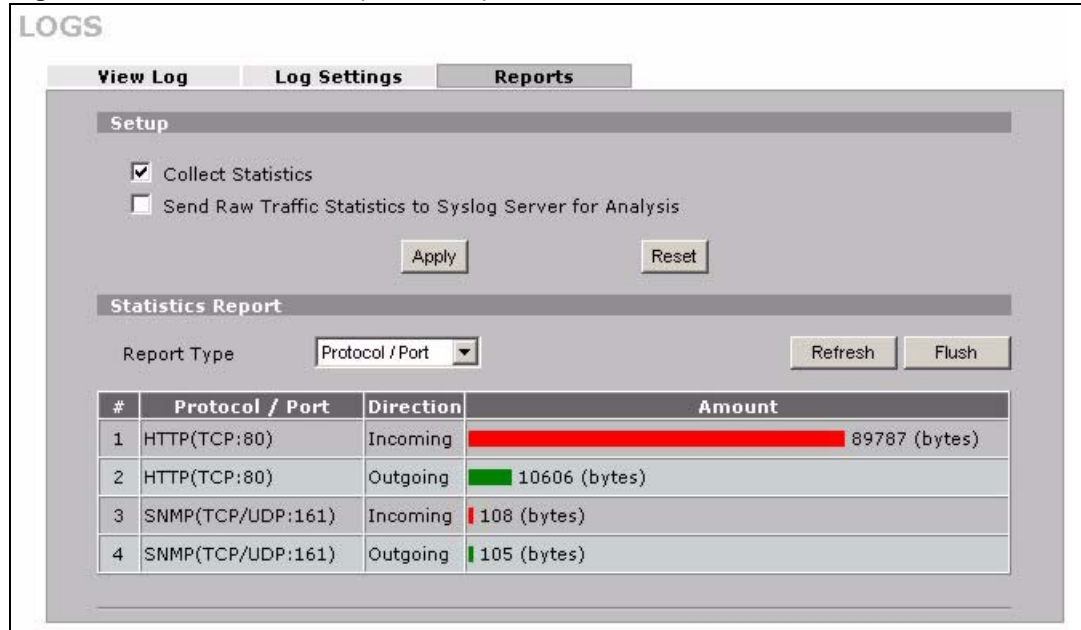
**Table 121** Web Site Hits Report

LABEL	DESCRIPTION
Web Site	This column lists the domain names of the web sites visited most often from computers on the LAN. The names are ranked by the number of visits to each web site and listed in descending order with the most visited web site listed first. The ZyWALL counts each page viewed in a web site as another hit on the web site.
Hits	This column lists how many times each web site has been visited. The count starts over at 0 if a web site passes the hit count limit (see <a href="#">Table 124 on page 349</a> ).

## 21.4.2 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 182** Protocol/Port Report Example



The following table describes the labels in this screen.

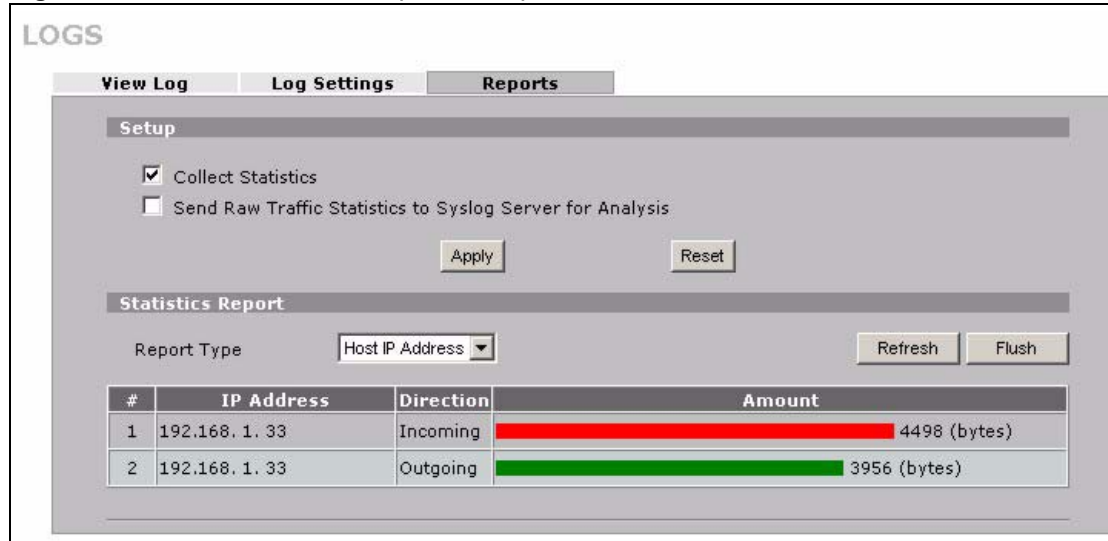
**Table 122** Protocol/ Port Report

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. This field displays <b>Outgoing</b> to denote traffic that is going out from the LAN 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 124 on page 349</a> ).

### 21.4.3 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 IP addresses that the most traffic has been sent to and/or from and how much traffic has been sent to and/or from those IP addresses.

**Note:** Computers take turns using dynamically assigned LAN IP addresses. The ZyWALL continues recording the bytes sent to or from a LAN IP address when it is assigned to a different computer.

**Figure 183** Host IP Address Report Example

The following table describes the labels in this screen.

**Table 123** Host IP Address Report

LABEL	DESCRIPTION
IP Address	This column lists the LAN IP addresses to and/or from which the most traffic has been sent. The LAN IP addresses are listed in descending order with the LAN IP address to and/or from which the most traffic was sent listed first.
Direction	This field displays <b>Incoming</b> to denote traffic that is coming in from the WAN to the LAN. This field displays <b>Outgoing</b> to denote traffic that is going out from the LAN to the WAN.
Amount	This column displays how much traffic has gone to and from the listed LAN IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN IP passes the bytes count limit (see <a href="#">Table 124 on page 349</a> ).

## 21.4.4 Reports Specifications

The following table lists detailed specifications on the reports feature.

**Table 124** 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 22

## Maintenance

This chapter displays information on the maintenance screens.

### 22.1 Maintenance Overview

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

### 22.2 General Setup

#### 22.2.1 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".

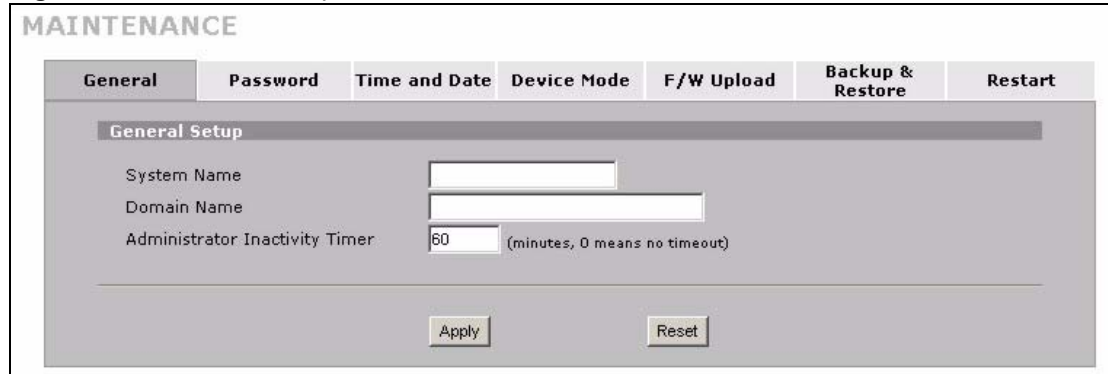
- In Windows 95/98 click **Start > Settings > Control Panel > Network > Identification**, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start > Settings > Control Panel** and then double-click **System**. Click **Network Identification**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

#### 22.2.2 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 184** General Setup



The following table describes the labels in this screen.

**Table 125** 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.

## 22.3 Configuring Password

To change your ZyWALL's password (recommended), click **MAINTENANCE > Password**. The screen appears as shown.



**Figure 185** Password Setup

The screenshot shows the 'MAINTENANCE' menu with the 'Password' tab selected. The 'Password Setup' 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 126** 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.

## 22.4 Time and Date

There is a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL.

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

**Figure 186** Time and Date

The following table describes the labels in this screen.

**Table 127** 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 127** 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.

## 22.5 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 128** 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.

### 22.5.1 Resetting the Time

The ZyWALL resets the time in the following instances:

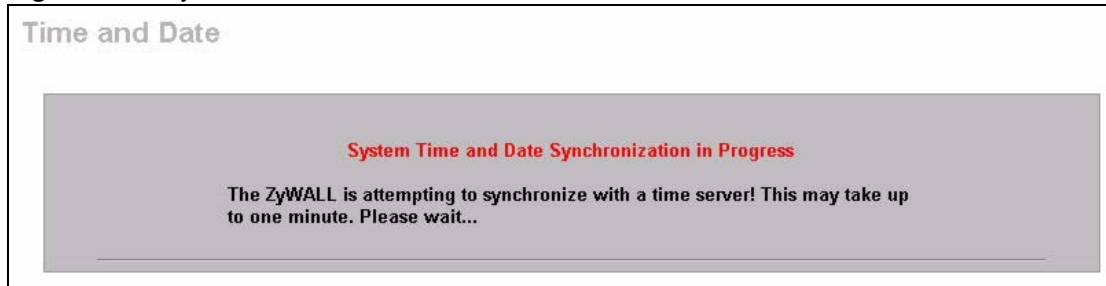
- When you click **Synchronize Now**.
- On saving your changes.
- When the ZyWALL starts up.
- 24-hour intervals after starting.

### 22.5.2 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.

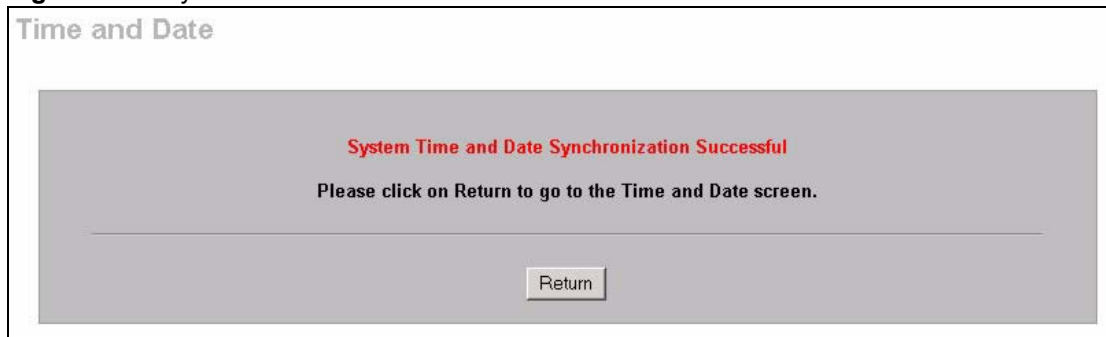
When the **System Time and Date Synchronization in Process** screen appears, wait up to one minute.

**Figure 187** Synchronization in Process



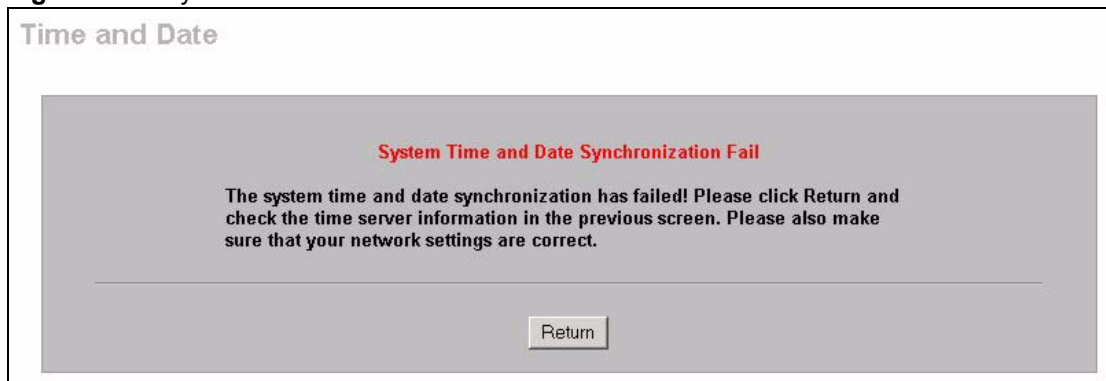
Click the **Return** button to go back to the **Time and Date** screen after the time and date is updated successfully.

**Figure 188** 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 189** Synchronization Fail



## 22.6 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 129** 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).

## 22.7 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.

## 22.8 Configuring Device Mode (Router)

To configure and have your ZyWALL work as a router or a bridge, click **MAINTENANCE > Device Mode**. The following applies when the ZyWALL is in router mode.

**Figure 190** Device Mode (Router Mode)

The screenshot shows the 'MAINTENANCE' page with the 'Device Mode' tab selected. The 'Current Device Mode' section shows 'Router'. The 'Device Mode Setup' section includes a note that the ZyWALL restarts automatically after a change. There are two radio buttons: 'Router' (selected) and 'Bridge'. Below the 'Bridge' option are input fields for IP Address (192.168.1.1), IP Subnet Mask (255.255.255.0), and Gateway IP Address (0.0.0.0). 'Apply' and 'Reset' buttons are at the bottom.

The following table describes the labels in this screen.

**Table 130** 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> or <b>WAN</b> to go to the <b>LAN</b> or <b>WAN</b> screen where you can view and/or change the corresponding settings.

**Table 130** 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.

## 22.9 Configuring Device Mode (Bridge)

To configure and have your ZyWALL work as a router or a bridge, click **MAINTENANCE > Device Mode**. The following applies when the ZyWALL is in bridge mode.

**Figure 191** Device Mode (Bridge Mode)



The following table describes the labels in this screen.

**Table 131** 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 131** Device Mode (Bridge Mode) (continued)

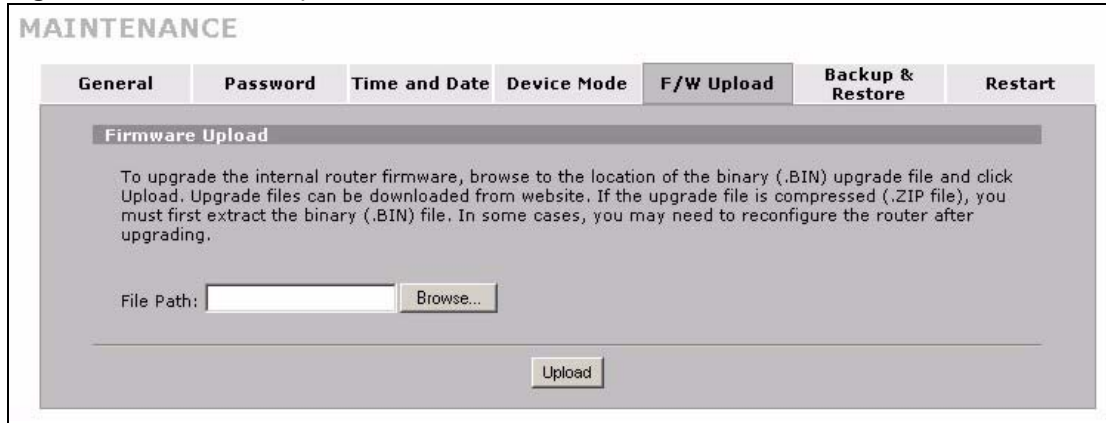
LABEL	DESCRIPTION
Device Mode Setup	
Router	Select this radio button and click <b>Apply</b> to set the ZyWALL to router mode.
LAN Interface IP Address	Enter the IP address of your ZyWALL's LAN port in dotted decimal notation. 192.168.1.1 is the factory default.
LAN Interface Subnet Mask	Enter the IP 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.

## 22.10 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 35.5 on page 476](#) for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE > F/W UPLOAD**. Follow the instructions in this screen to upload firmware to your ZyWALL.

**Figure 192** Firmware Upload



The following table describes the labels in this screen.

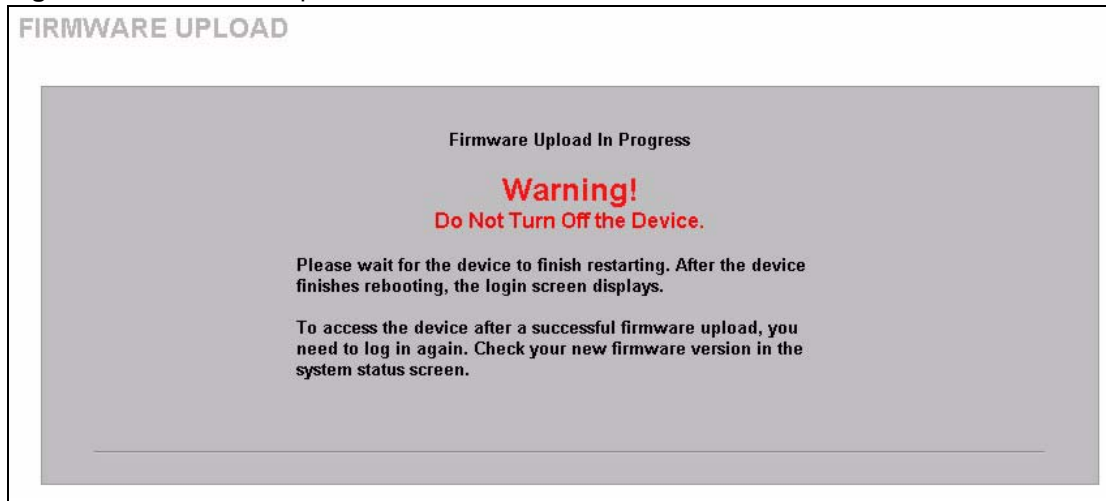
**Table 132** Firmware Upload

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.

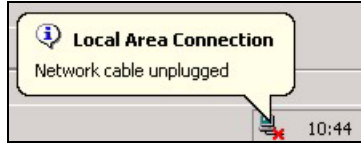
**Note:** Do not turn off the ZyWALL while firmware upload is in progress!

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

**Figure 193** 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 194** 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.

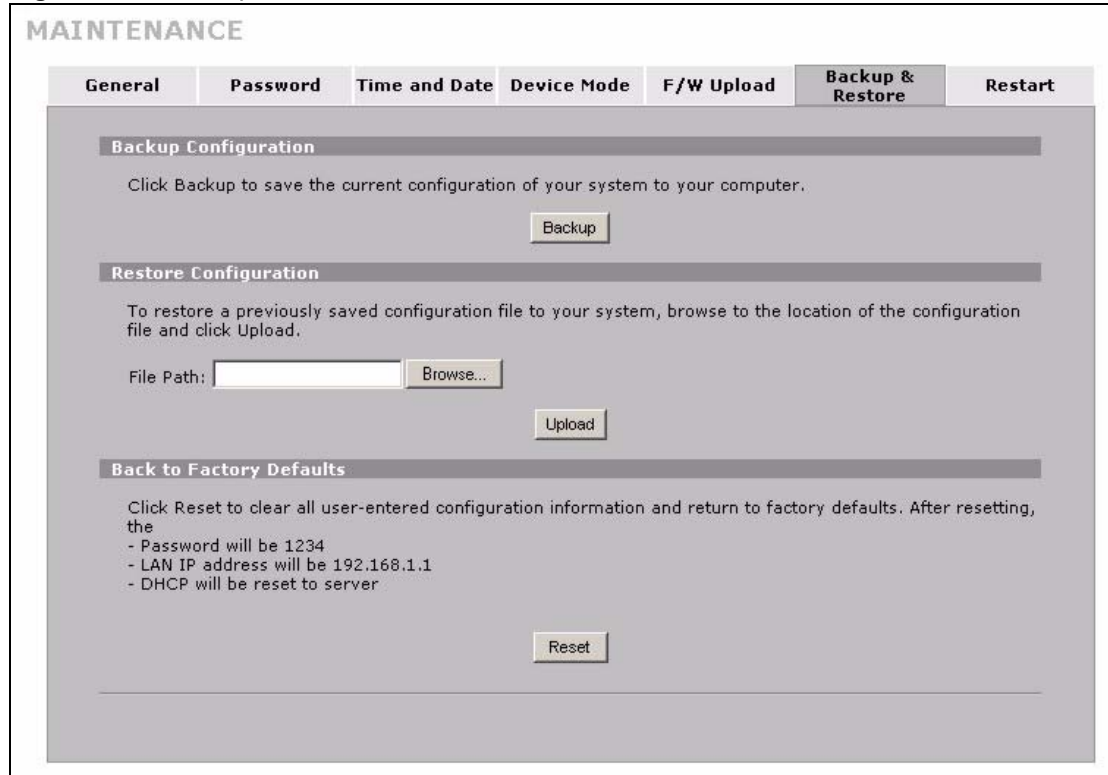
**Figure 195** Firmware Upload Error

## 22.11 Backup and Restore

See [Section 35.5 on page 476](#) for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE > Backup & Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

**Figure 196** Backup and Restore



### 22.11.1 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.

### 22.11.2 Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your ZyWALL.

**Table 133** 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.

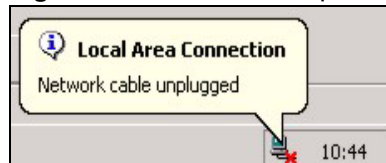
After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyWALL again.

**Figure 197** 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 198** 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.

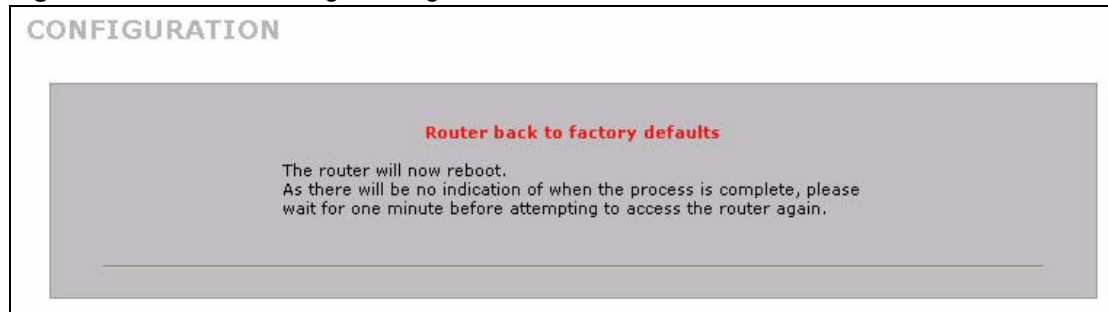
**Figure 199** Configuration Upload Error



### 22.11.3 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 200** Reset Warning Message



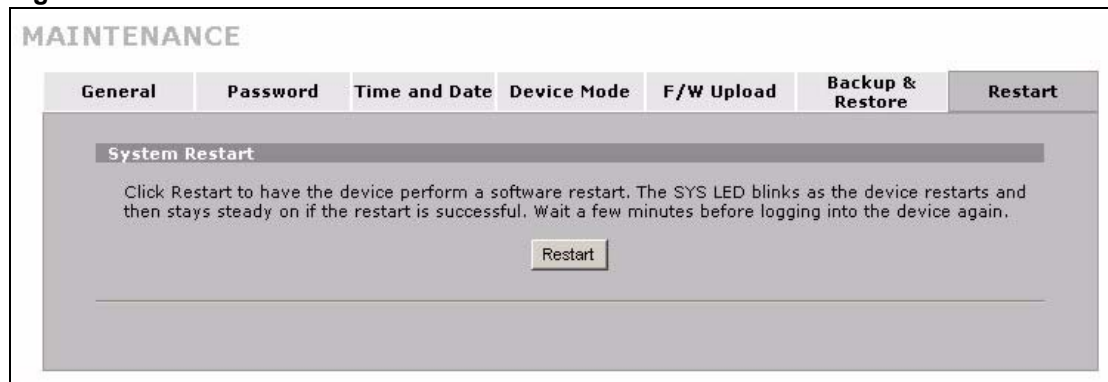
You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyWALL. Refer to [Section 2.3 on page 54](#) for more information on the **RESET** button.

### 22.12 Restart Screen

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

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

**Figure 201** Restart Screen



# CHAPTER 23

## Introducing the SMT

This chapter explains how to access the System Management Terminal and gives an overview of its menus.

### 23.1 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.

### 23.2 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.

#### 23.2.1 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 202** Initial Screen

```

Copyright (c) 1994 - 2006 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
AUX port init . done
Modem init . inactive

Press ENTER to continue...
    
```

### 23.2.2 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 203** Password Screen

```

Enter Password : XXXX
    
```

### 23.3 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 134** Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press the [ESC] key to move back to the previous menu.
Move to a “hidden” menu	Press [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.



**Table 134** Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
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 to 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.

### 23.3.1 Main Menu

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

**Figure 204** Main Menu (Router Mode)

```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.

ZyWALL 2 Plus Main Menu

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

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

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

99. Exit

Enter Menu Selection Number:
```

**Figure 205** Main Menu (Bridge Mode)

```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.

ZyWALL 2 Plus Main Menu

Getting Started
  1. General 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 135** 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.
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.
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.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this menu to exit (necessary for remote configuration).

### 23.3.2 SMT Menus Overview

The following table gives you an overview of your ZyWALL's various SMT menus.

**Table 136** 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			

**Table 136** SMT Menus Overview (continued)

<b>MENUS</b>	<b>SUB MENUS</b>		
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	
	11.2 Remote Node Profile (Backup ISP)	11.2.1 Remote Node PPP Options	
		11.2.2 Remote Node Network Layer Options	
		11.2.3 Remote Node Script	
		11.2.4 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 136** 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			
26 Schedule Setup	26.1 Schedule Set Setup		

## 23.4 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 206** 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.

## **23.5 Resetting the ZyWALL**

See [Section 2.3 on page 54](#) for directions on resetting the ZyWALL.

# CHAPTER 24

## SMT Menu 1 - General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

### 24.1 Introduction to General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

### 24.2 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 207** 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 137** 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 137** 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 208** 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 137 on page 375](#)).

**Table 138** 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).



## 24.2.1 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 209** 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 139** Menu 1.1: Configure Dynamic DNS

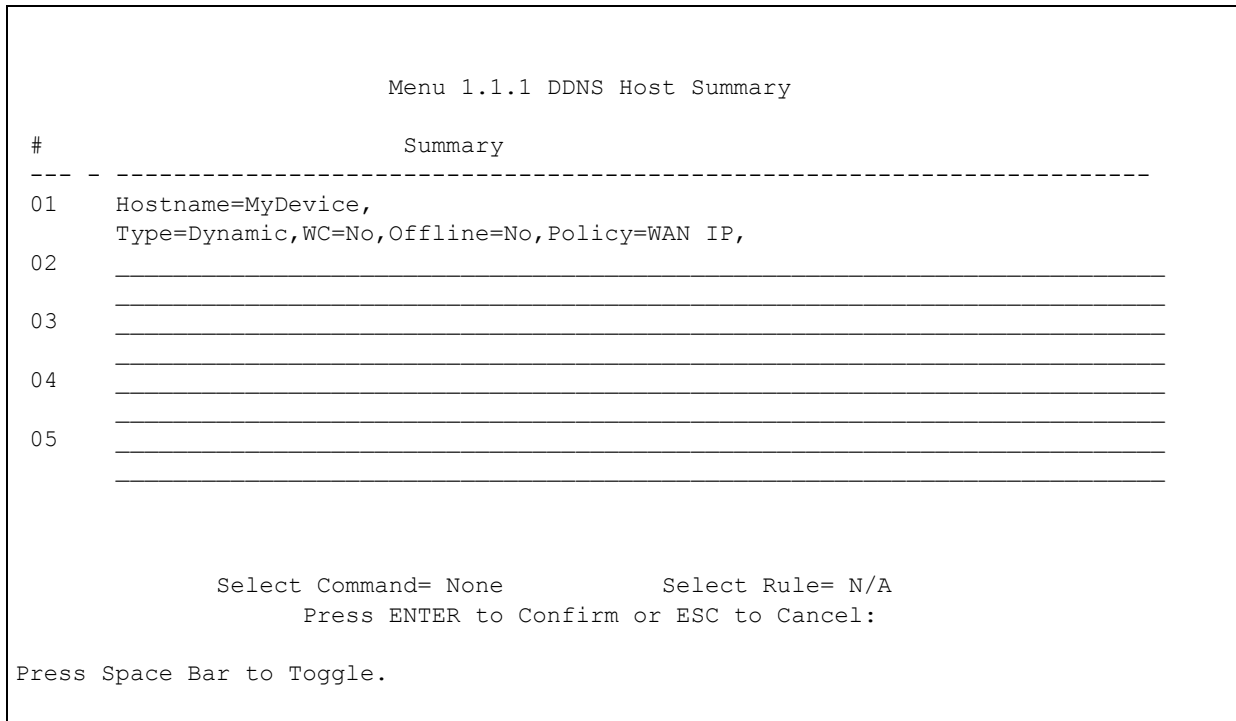
FIELD	DESCRIPTION
Service Provider	This is the name of your Dynamic DNS service provider.
Active	Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to make dynamic DNS active.
Username	Enter your user name.
Password	Enter the password assigned to you.
Edit Host	Press [SPACE BAR] and then [ENTER] 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.	

### 24.2.1.1 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 210** Menu 1.1.1: DDNS Host Summary



The following table describes the fields in this screen.

**Table 140** 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 211** Menu 1.1.1: DDNS Edit Host

```

Menu 1.1.1 - DDNS Edit Host

Hostname= MyDevice
DDNS Type= DynamicDNS
Enable Wildcard Option= No
Enable Off Line Option= N/A
IP Address Update Policy:
    Let DDNS Server Auto Detect= No
    Use User-Defined= No
    Use WAN IP Address= N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 141** 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).
IP Address Update Policy:	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. 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. 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.

**Table 141** Menu 1.1.1: DDNS Edit Host (continued)

FIELD	DESCRIPTION
Let DDNS Server Auto Detect	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.  <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.
Use User-Defined	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. Only select <b>Yes</b> if the ZyWALL uses or is behind a static public IP address.
Use WAN IP Address	Enter the static public IP address if you select <b>Yes</b> in the <b>Use User-Defined</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.	

The IP address updates when you reconfigure menu 1 or perform DHCP client renewal.

# CHAPTER 25

## 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.

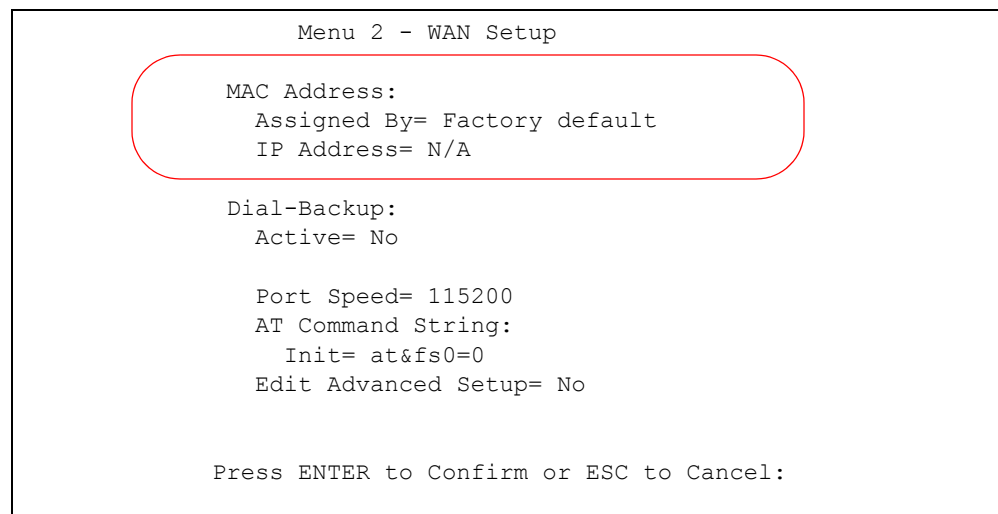
### 25.1 Introduction to WAN and Dial Backup Setup

This chapter explains how to configure settings for your WAN port and how to configure the ZyWALL for a dial backup connection.

### 25.2 WAN Setup

From the main menu, enter 2 to open menu 2.

**Figure 212** MAC Address Cloning in WAN Setup



The following table describes the fields in this screen.

**Table 142** MAC Address Cloning in WAN Setup

FIELD	DESCRIPTION
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.	

## 25.3 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.

## 25.4 Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

**Figure 213** Menu 2: Dial Backup Setup

```

Menu 2 - WAN Setup

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 143** 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.	

## 25.5 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 214** 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 144** 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 145** 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.

## 25.6 Remote Node Profile (Backup ISP)

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 215** Menu 11.2: Remote Node Profile (Backup ISP)

```

Menu 11.2 - Remote Node Profile (Backup ISP)

Rem Node Name=                               Edit PPP Options= No
Active= No                                     Edit IP= No
                                                Edit Script Options= No

Outgoing:
  My Login= ChangeMe
  My Password= *****
  Retype to Confirm= *****
  Authen= CHAP/PAP
  Pri Phone #= 0
  Sec Phone #=

Telco Option:
  Allocated Budget (min)= 0
  Period(hr)= 0
  Schedules=
  Always On= No

Session Options:
  Edit Filter Sets= No
  Idle Timeout(sec)= 100

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

The following table describes the fields in this menu.

**Table 146** Menu 11.2: 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 11.2.1 - Remote Node PPP Options</b> (see <a href="#">Section 25.7 on page 387</a> ).

**Table 146** Menu 11.2: 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 11.2.2 - Remote Node Network Layer Options</b> . See <a href="#">Section 25.8 on page 388</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 11.2.3 - Remote Node Script</b> ). See <a href="#">Section 25.9 on page 390</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 38 on page 495</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 11.2.4 to edit the filter sets. See <a href="#">Section 25.10 on page 391</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.	

## 25.7 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 11.2 - Remote Node Profile (Backup ISP)**, and use the space bar to select **Yes**. Press [Enter] to open **Menu 11.2.1 - Remote Node PPP Options** as shown next.

**Figure 216** Menu 11.2.1: Remote Node PPP Options

```
Menu 11.2.1 - 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 147** Menu 11.2.1: 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.	

## 25.8 Editing TCP/IP Options

Move the cursor to the **Edit IP** field in menu 11.2, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.2.2 - Remote Node Network Layer Options**.

**Figure 217** Menu 11.2.2: Remote Node Network Layer Options

```

Menu 11.2.2 - 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
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 148** Menu 11.2.2: 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> . See <a href="#">Chapter 14 on page 249</a> for a full discussion on this feature.
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> .

**Table 148** Menu 11.2.2: Remote Node Network Layer Options

FIELD	DESCRIPTION
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 93</a> for more information on this feature.
Once you have completed filling in <b>Menu 11.2.2 Remote Node Network Layer Options</b> , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11.2, or press [ESC] at any time to cancel.	

## 25.9 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 218** Menu 11.2.3: Remote Node Script

```

Menu 11.2.3 - 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 149** Menu 11.2.3: 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.

## 25.10 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.2, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.2.4 - Remote Node Filter**.

Use menu 11.2.4 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 32 on page 437](#) for more information on defining the filters.

**Figure 219** Menu 11.2.4: Remote Node Filter

```
Menu 11.2.4 - 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 26

## LAN Setup

This chapter describes how to configure the LAN using **Menu 3 - LAN Setup**.

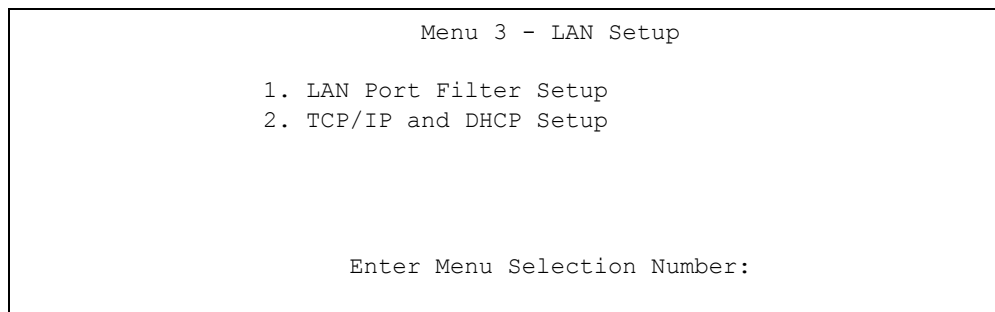
### 26.1 Introduction to LAN Setup

This chapter describes how to configure the ZyWALL for LAN connections.

### 26.2 Accessing the LAN Menus

From the main menu, enter 3 to open **Menu 3 - LAN Setup**.

**Figure 220** Menu 3: LAN Setup



### 26.3 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 221** 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:
```

## 26.4 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 222** 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.

**Figure 223** 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:                             IP Address= 192.168.1.1
  Starting Address= 192.168.1.33           IP Subnet Mask=
  Size of Client IP Pool= 128
  255.255.255.0
First DNS Server= From ISP                 RIP Direction= Both
  IP Address= N/A                         Version= RIP-1
Second DNS Server= From ISP              Multicast= None
  IP Address= N/A                         Edit IP Alias= No
Third DNS Server= From ISP
  IP Address= N/A
DHCP Server Address= N/A

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

```

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

**Table 150** 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 150** 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.

**Table 151** 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, In Only, Out Only</b> or <b>None</b> .
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: <b>RIP-1, 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.	

## 26.4.1 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 224** 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 152** 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 152** 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 27

## Internet Access

This chapter shows you how to configure your ZyWALL for Internet access.

### 27.1 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.

### 27.2 Ethernet Encapsulation

If you choose **Ethernet** in menu 4 you will see the next menu.

**Figure 225** 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 153** 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 14 on page 249</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.	



## 27.3 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 226** Internet Access Setup (PPTP)

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
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 154** 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.

## 27.4 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen.

**Figure 227** 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 155** 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.

## 27.5 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 28

## Remote Node Setup

This chapter shows you how to configure a remote node.

### 28.1 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**.

### 28.2 Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 - Remote Node Setup** (shown below).

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 (see [Chapter 25 on page 381](#)).

**Figure 228** Menu 11: Remote Node Setup

```
Menu 11 - Remote Node Setup

1. ChangeMe (ISP, SUA)
2. -Dial (BACKUP_ISP, SUA)

Enter Node # to Edit:
```

### 28.3 Remote Node Profile Setup

The following explains how to configure the remote node profile menu.

### 28.3.1 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 229** Menu 11.1: Remote Node Profile for Ethernet Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes                       Bridge= No

Encapsulation= Ethernet           Edit IP= No
Service Type= Standard            Session Options:
Service Name= N/A                 Schedules=
Outgoing:                          Edit Filter Sets= No
  My Login= N/A
  My Password= N/A                Edit Traffic Redirect= No
  Retype to Confirm= N/A
  Server= N/A
  Relogin Every (min)= N/A

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

The following table describes the fields in this menu.

**Table 156** 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> .
Service Name	When using <b>PPPoE</b> encapsulation, type the name of your PPPoE service here.
Outgoing	

**Table 156** Menu 11.1: Remote Node Profile for Ethernet Encapsulation (continued)

FIELD	DESCRIPTION
My Login	This field is applicable for <b>PPPoE</b> encapsulation only. Enter the login name assigned by your ISP when the ZyWALL calls this remote node. Some ISPs append this field to the <b>Service Name</b> field above (e.g., jim@poellc) to access the PPPoE server.
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.
Bridge	When bridging is enabled, your ZyWALL will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select <b>Yes</b> to enable and <b>No</b> to disable.
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 38 on page 495</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 28.5 on page 410</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.	

### 28.3.2 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.

**Figure 230** Menu 11.1: Remote Node Profile for PPPoE Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes                       Bridge= No

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

Edit Traffic Redirect= No

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

```

### 28.3.2.1 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.

### 28.3.2.2 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 156 on page 404](#).

### 28.3.2.3 Metric

See [Section 7.2 on page 109](#) for details on the **Metric** field.

**Table 157** 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 38 on page 495</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.

### 28.3.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see [Section 3.2.1.3 on page 72](#) for information on PPTP.

**Figure 231** Menu 11.1: Remote Node Profile for PPTP Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes                        Bridge= No

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

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

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

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

**Table 158** 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 11.2 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 38 on page 495</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.

## 28.4 Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.1.2 - Remote Node Network Layer Options**.



**Figure 232** 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 159** 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 14 on page 249</a> for a full discussion on this feature.

**Table 159** 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 30.2 on page 417</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 7.2 on page 109</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 93</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 93</a> for more information on this feature.
Once you have completed filling in <b>Menu 11.2 Remote Node Network Layer Options</b> , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.	

## 28.5 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 32 on page 437](#). For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 233** 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 234** 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:
```

## 28.6 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**.

**Figure 235** 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 160** 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 109</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 29

## IP Static Route Setup

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

### 29.1 IP Static Route Setup

Enter 12 from the main menu. Select one of the IP static routes as shown next to configure IP static routes in menu 12.1.

**Note:** The first static route entry is for the default WAN route. 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 236** Menu 12: IP Static Route Setup

```
Menu 12 - IP Static Route Setup

1. Reserved
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____

Enter selection number:
```

Now, enter the index number of the static route that you want to configure.

**Figure 237** 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 161** 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 7.2 on page 109</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 30

## Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

### 30.1 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.

#### 30.1.1 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 30.2.1 on page 417](#) 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.

#### 30.1.2 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 238** 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 239** 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 162** 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 30.2.1 on page 417</a> for further discussion). You can configure any of the mapping types described in <a href="#">Chapter 14 on page 249</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 30.2.1 on page 417</a> ). Choose <b>SUA Only</b> if you have just one public WAN IP address for your ZyWALL.	SUA Only

## 30.2 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. **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 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 14 on page 249](#) for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

**Figure 240** 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 LAN IP addresses in NAT menus 15.1 and 15.2.

### 30.2.1 Address Mapping Sets

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

**Figure 241** Menu 15.1: Address Mapping Sets

```

Menu 15.1 - Address Mapping Sets

      1. NAT_SET
     255. SUA (read only)

Enter Menu Selection Number:
    
```

### 30.2.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also [Section 30.1.1 on page 415](#)). The fields in this menu cannot be changed.

**Figure 242** Menu 15.1.255: SUA Address Mapping Rules

```

Menu 15.1.255 - Address Mapping Rules

Set Name= SUA

Idx  Local Start IP   Local End IP   Global Start IP  Global End IP   Type
---  -
1.   0.0.0.0          255.255.255.255  0.0.0.0          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 163** 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).

**Table 163** SUA Address Mapping Rules

FIELD	DESCRIPTION
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.	

### 30.2.1.2 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 243** Menu 15.1.1 Address Mapping Rules

```

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.

### 30.2.1.3 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 164** 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 244** 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 165** 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 14 on page 249</a> . <b>Server</b> allows you to specify multiple servers of different types behind NAT to this computer. See <a href="#">Section 30.4.3 on page 426</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.
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.	

## 30.3 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 - NAT Server Setup** (and configure the address mapping rules for the WAN port).

**Figure 245** Menu 15.2.1: NAT Server Sets

Menu 15.2 - 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:

- 3** 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.x - NAT Server Configuration** (see the next figure).

**Figure 246** 15.2.x: NAT Server Configuration

```

15.2.3 - NAT Server Configuration
                                         Index= 2
-----
Name= 1
Active= Yes
Start port= 21                         End port= 25
IP Address= 192.168.1.33
Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 166** 15.2.x: NAT Server Configuration

FIELD	DESCRIPTION
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.	

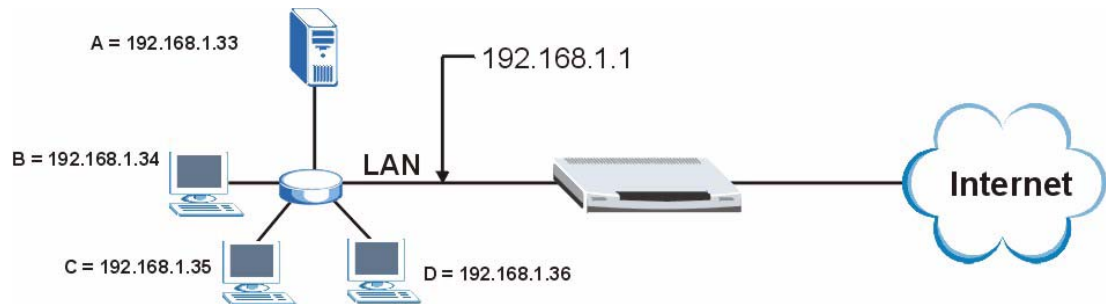
- 4** Enter a port number in the **Start Port** field. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.
- 5** Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.
- 6** 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 247** Menu 15.2: NAT Server Setup

Menu 15.2 - 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 248** Server Behind NAT Example

## 30.4 General NAT Examples

The following are some examples of NAT configuration.

### 30.4.1 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 249 NAT Example 1

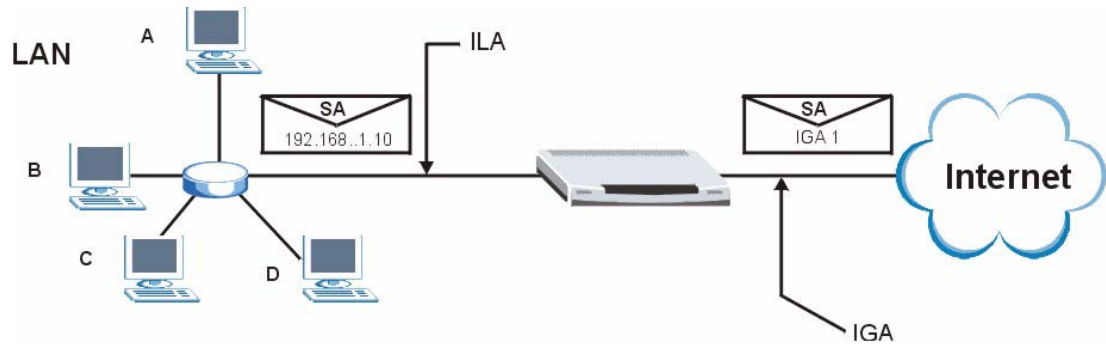


Figure 250 Menu 4: Internet Access &amp; NAT Example

```

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

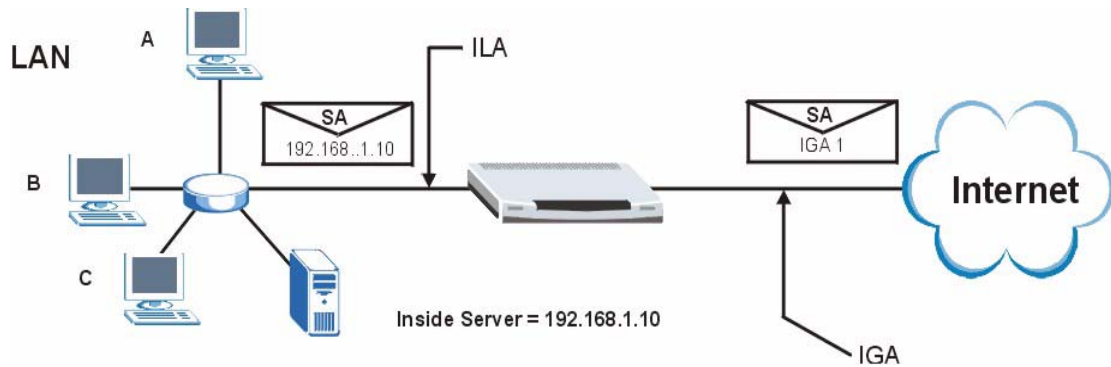
Press ENTER to Confirm or ESC to Cancel:

```

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 30.4 on page 424](#). The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.2 is specifically pre-configured to handle this case.

### 30.4.2 Example 2: Internet Access with a Default Server

Figure 251 NAT Example 2



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

Figure 252 Menu 15.2: Specifying an Inside Server

Menu 15.2 - 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:

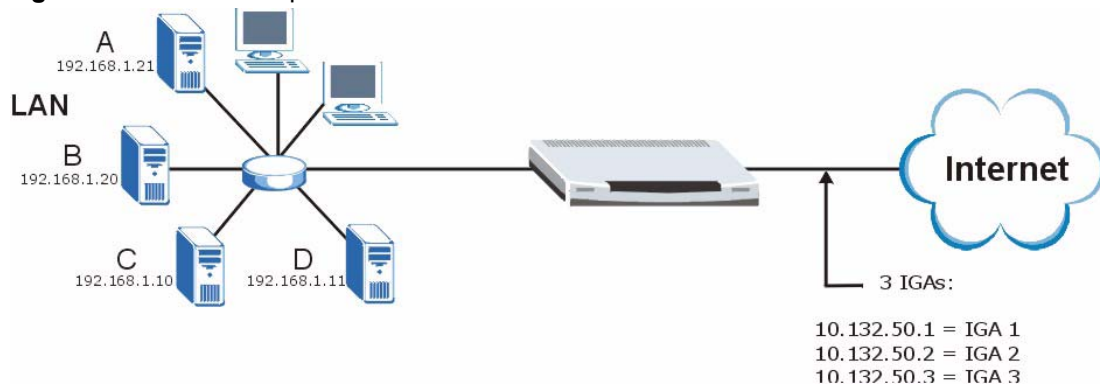
### 30.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

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 the following figure, in which **A** is the web server, **B** is the mail server, **C** is FTP server 1 and **D** is FTP server 2.

**Figure 253** NAT Example 3



**Table 167** NAT Example 3

MAPPING RULES		
FTP1	↔	IGA 1 Type 1:1
FTP2	↔	IGA 2 Type 1:1
Other LAN traffic	↔	IGA 3 Type M-1 (outgoing traffic)
IGA 3	↔	Inside web server and mail server (incoming traffic)

- 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 11.2) in [Figure 254 on page 428](#).
- 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 255 on page 428](#)).
- 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 256 on page 429](#).

**Figure 254** 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 255** 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 256** 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 configure the menu as shown in [Figure 257 on page 430](#).

**Figure 257** Example 3: Menu 15.2

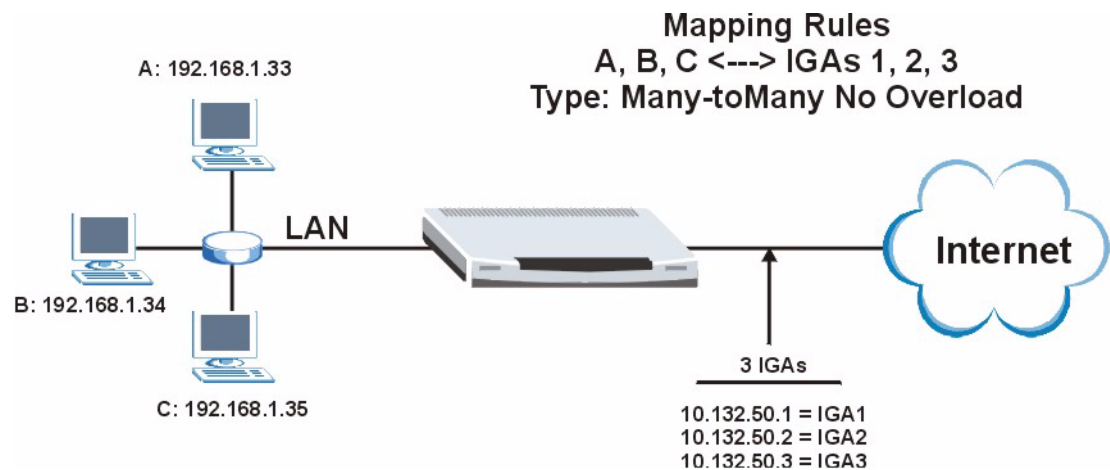
Menu 15.2 - NAT Server Setup				
Default Server: 0.0.0.0				
Rule	Act.	Start Port	End Port	IP Address
001	Yes	80	80	192.168.1.21
002	Yes	25	25	192.168.1.20
003	No	0	0	0.0.0.0
004	No	0	0	0.0.0.0
005	No	0	0	0.0.0.0
006	No	0	0	0.0.0.0
007	No	0	0	0.0.0.0
008	No	0	0	0.0.0.0
009	No	0	0	0.0.0.0
010	No	0	0	0.0.0.0

Select Command= None                      Select Rule= N/A  
Press ENTER to Confirm or ESC to Cancel:

### 30.4.4 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 258** 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 259** 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 260** 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:

## 30.5 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.

### 30.5.1 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**.

**Figure 261** Menu 15.3: Trigger Port Setup

Menu 15.3 - 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 168** Menu 15.3: Trigger Port Setup

FIELD	DESCRIPTION
Rule	This is the rule index number.
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	



# CHAPTER 31

## Introducing the ZyWALL Firewall

This chapter shows you how to get started with the ZyWALL firewall.

### 31.1 Accessing the Firewall Settings

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. The commands provide limited firewall configuration options and are not recommended.

### 31.2 Firewall 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 262** Menu 21: Filter and Firewall Setup

```
Menu 21 - Filter and Firewall Setup

      1. Filter Setup
      2. Firewall Setup

Enter Menu Selection Number:
```

#### 31.2.1 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 263** 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 32

## Filter Configuration

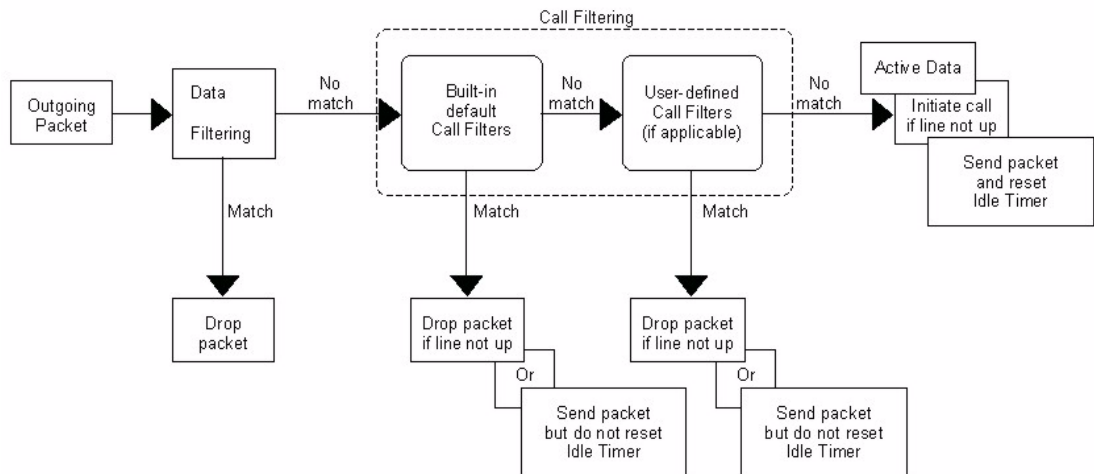
This chapter shows you how to create and apply filters.

### 32.1 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 264** 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.

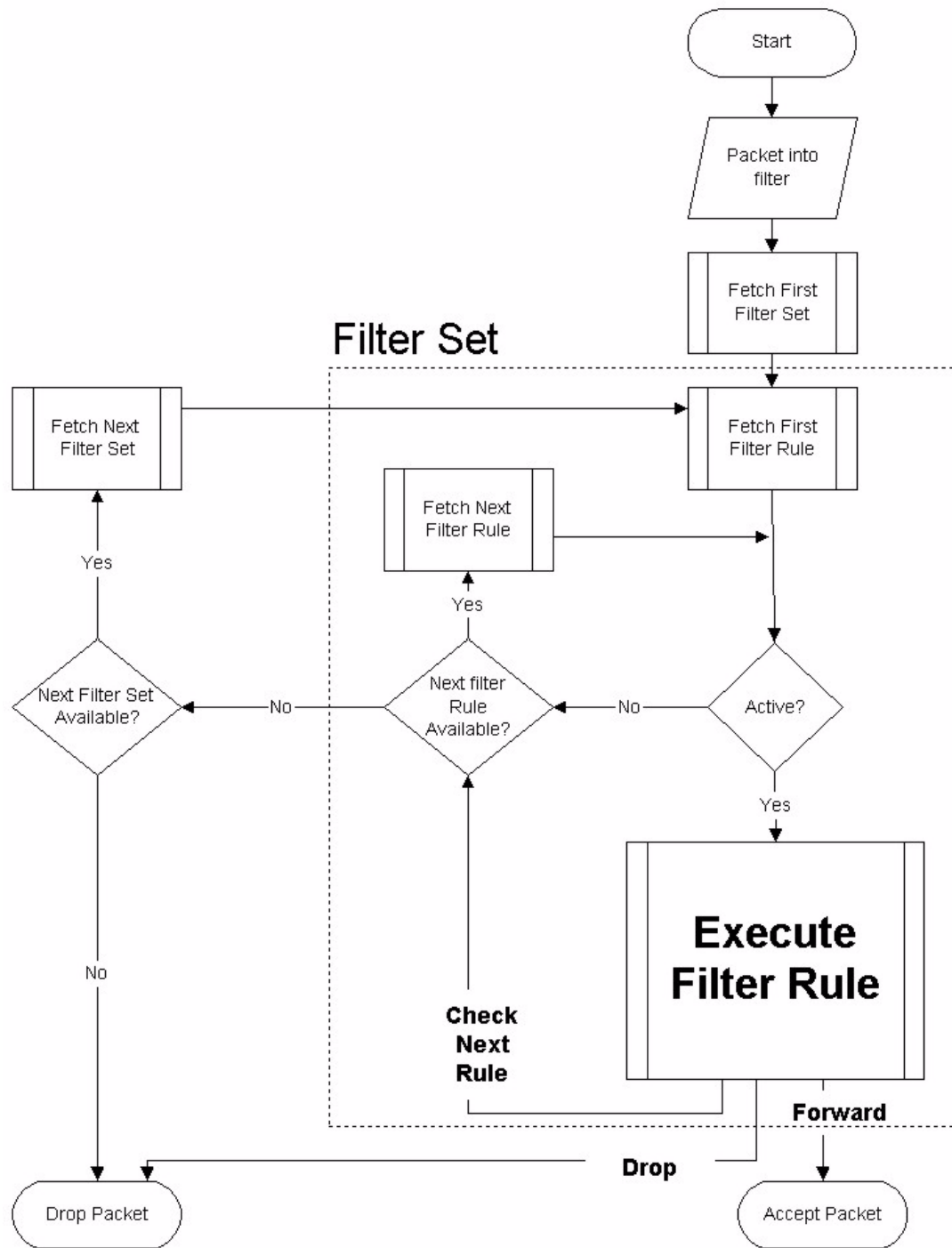
### 32.1.1 The Filter Structure of the ZyWALL

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 269 on page 446](#) for the logic flow when executing an IP filter.

**Figure 265** 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.

## 32.2 Packet Filtering Versus Firewall

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

### 32.2.1 Packet Filtering

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

- 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.

#### 32.2.1.1 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.

### 32.2.2 Firewall

The ZyWALL's firewall restricts 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.

- 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.



### 32.2.2.1 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.

## 32.3 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 266** 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 267** 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 169** 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 170** 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.

### 32.3.1 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.

### 32.3.2 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 268** 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 171** Menu 21.1.1.1: TCP/IP Filter Rule

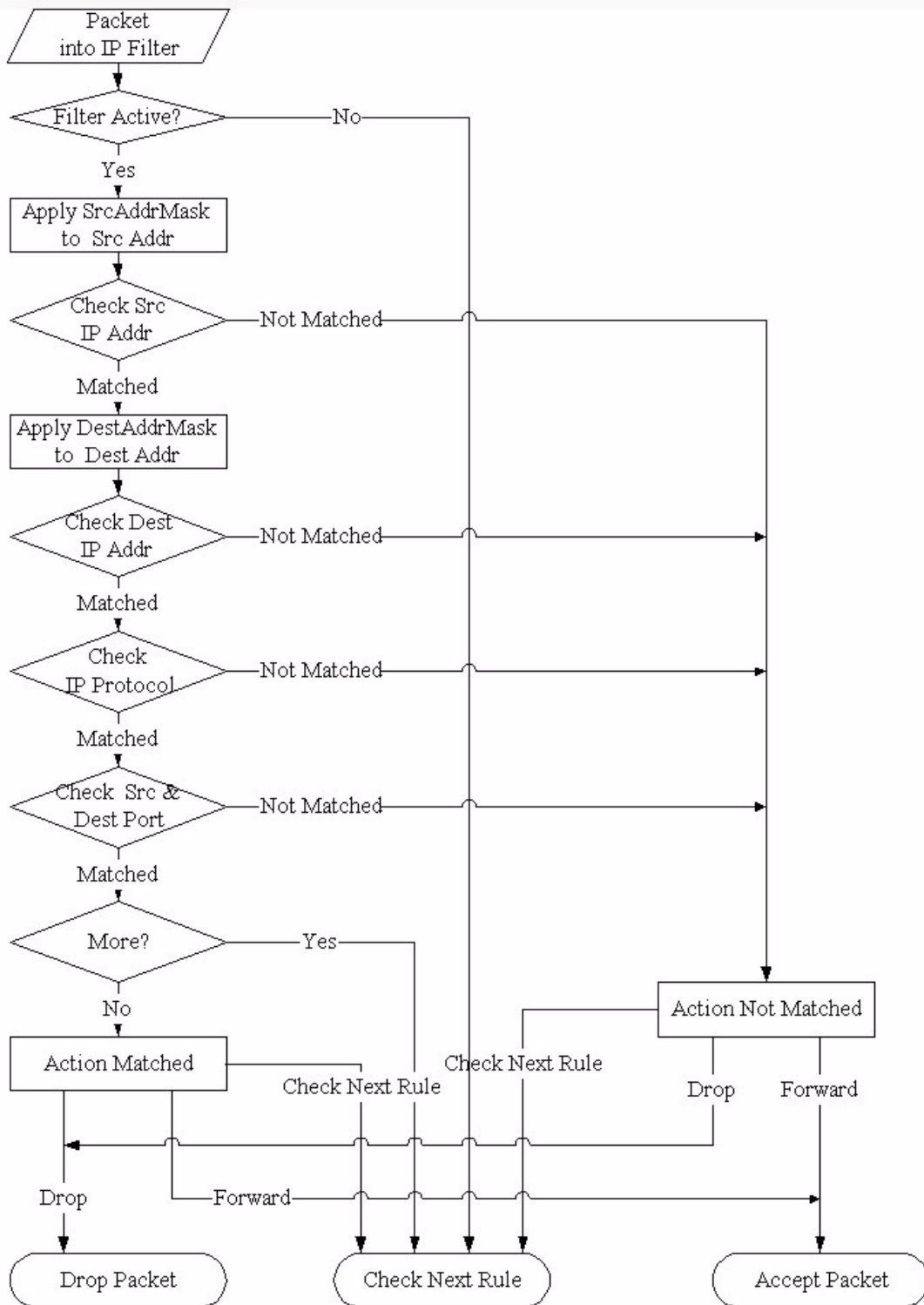
FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to activate the filter rule or <b>No</b> to deactivate it.
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.
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.
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</b> , <b>Equal</b> , <b>Not Equal</b> , <b>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> .

**Table 171** Menu 21.1.1.1: TCP/IP Filter Rule

FIELD	DESCRIPTION
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</b> , <b>Equal</b> , <b>Not Equal</b> , <b>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</b> , <b>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</b> , <b>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 269** Executing an IP Filter



### 32.3.3 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 270** 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 172** 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.

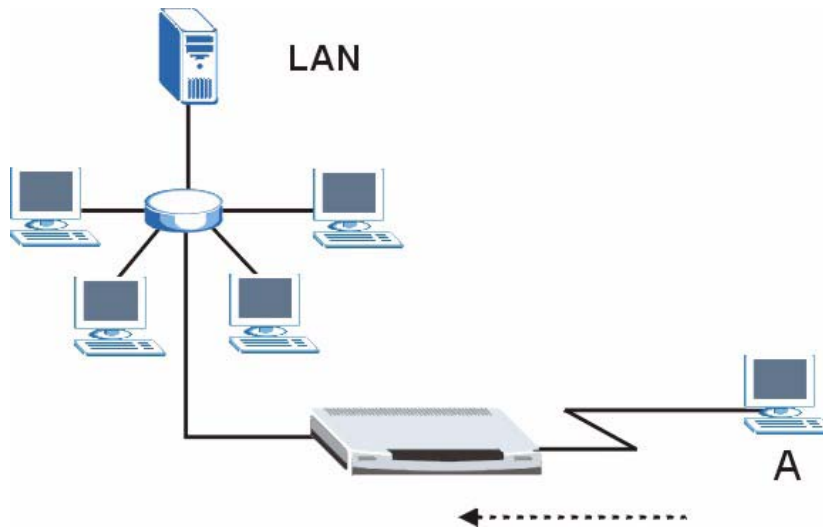
**Table 172** Generic Filter Rule Menu Fields

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> .	

## 32.4 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. In the following figure, **A** is the user who telnets into the LAN, and the arrow indicates the flow of incoming traffic.

**Figure 271** 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 272** 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 273** Example Filter Rules Summary: Menu 21.1.3

Menu 21.1.3 - Filter Rules Summary						
#	A	Type	Filter Rules	M	m	n
-	-	-	-	-	-	-
1	<b>Y</b>	<b>IP</b>	Pr=6, SA=0.0.0.0, DA=0.0.0.0, <b>DP=23</b>	<b>N</b>	<b>D</b>	<b>F</b>
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**).

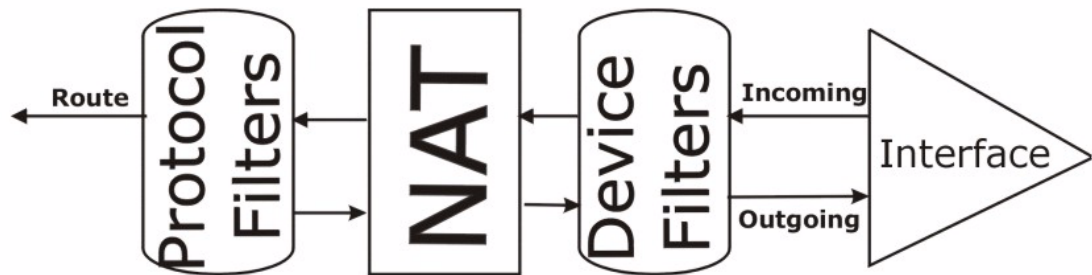
**M = N** means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

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 276 on page 452](#).
- 5 Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.1.4.

## 32.5 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 274** Protocol and Device Filter Sets

## 32.6 Firewall Versus Filters

Firewall configuration is discussed in [Chapter 8 on page 131](#). Further comparisons are also made between filtering, NAT and the firewall.

## 32.7 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.

### 32.7.1 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 275** 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:
```

### 32.7.2 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 276** 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 33

## SNMP Configuration

This chapter explains SNMP configuration menu 22.

### 33.1 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 277** 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 173** 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 173** 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.	

## 33.2 SNMP Traps

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

**Table 174** 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 34

## System Information & Diagnosis

This chapter covers SMT menus 24.1 to 24.4.

### 34.1 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 278** 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:
```

### 34.2 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 279** Menu 24.1: System Maintenance: Status

```

Menu 24.1 - System Maintenance - Status                                07:15:51
                                                                    Fri. Mar. 31, 2006

Port  Status      TxPkts    RxPkts    Cols     Tx B/s    Rx B/s    Up Time
WAN   100M/Full     9521     105390    0         0         760      7:25:33
LAN   100M/Full    13438     10927     0         0         0        7:25:34

Port  Ethernet Address      IP Address      IP Mask      DHCP
WAN   00:13:49:00:00:02     172.23.23.60   255.255.255.0 Client
LAN   00:13:49:00:00:01     192.168.1.1    255.255.255.0 Server

System up Time:      7:25:39

Name: test.domainname
Routing: IP
ZyNOS F/W Version: V4.00(XU.0)b2-2006.3.29 | 03/29/2006

Press Command:

COMMANDS: 1-Drop WAN 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 175** System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Port	This field identifies a port on the ZyWALL.
Status	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.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Cols	This is the number of collisions on this port.
Tx B/s	This field shows the transmission speed in Bytes per second on this port.
Rx B/s	This field shows the reception speed in Bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
Ethernet Address	This is the Ethernet address of the port listed on the left.



**Table 175** System Maintenance: Status Menu Fields (continued)

FIELD	DESCRIPTION
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.
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	This shows the routing protocol - <b>IP</b> for which the ZyWALL is configured. This field is not configurable.
ZyNOS F/W Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

### 34.3 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 280** Menu 24.2: System Information and Console Port Speed

<pre> Menu 24.2 - System Information and Console Port Speed        1. System Information       2. Console Port Speed  Please enter selection: </pre>
--

#### 34.3.1 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 281** 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 176** 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	This shows the routing protocol - <b>IP</b> for which the ZyWALL is configured. This field is not configurable.
ZyNOS F/W Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System.
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.	

### 34.3.2 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 282** 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.
```

## 34.4 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.

### 34.4.1 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 283** 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 284** Examples of Error and Information Messages

```

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):
    
```

### 34.4.2 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 285** 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 177** 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=xxxxxxxxx...x Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG) Data: We will send forty-eight Hex characters to the server Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a 6b6c6d6e6f7071727374 Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000600220008cd4 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
<pre>SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String ); String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04&gt;R01mD IP[...] is the packet header and S04&gt;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&gt;R01mF Mar 03 10:41:29 202.132.155.97 ZyXEL: GEN[00a0c5f502fnord010080] }S05&gt;R01mF Mar 03 10:41:34 202.132.155.97 ZyXEL: IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04&gt;R01mF Mar 03 11:59:20 202.132.155.97 ZyXEL: GEN[00a0c5f502fnord010080] }S05&gt;R01mF Mar 03 12:00:52 202.132.155.97 ZyXEL: GEN[fffffffffff0080] }S05&gt;R01mF Mar 03 12:00:57 202.132.155.97 ZyXEL: GEN[00a0c5f502010080] }S05&gt;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&gt;R01mF</pre>

#### 4 PPP log

PPP Log Message Format
<pre>SdcmdSyslogSend( SYSLOG_PPLOG, SYSLOG_NOTICE, String ); String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing</pre>

#### 5 Firewall log

Firewall Log Message Format
<pre>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: &lt;a,b&gt; 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 - &gt;172.21.1.80 :137  UDP default permit:&lt;2,0&gt; B 08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 192.168.77.88 :520 - &gt;192.168.77.88 :520  UDP default permit:&lt;2,0&gt; B 08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.50 -&gt;172.21.1.50  IGMP&lt;2&gt; default permit:&lt;2,0&gt; B 08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.25 -&gt;172.21.1.25  IGMP&lt;2&gt; default permit:&lt;2,0&gt; B</pre>

### 34.4.3 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 286** Call-Triggering Packet Example

```

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

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

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

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

```

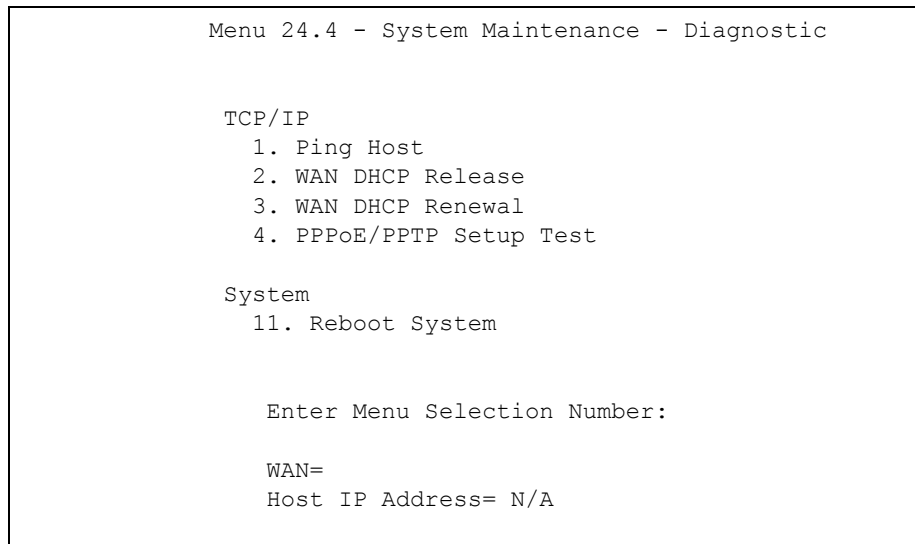
## 34.5 Diagnostic

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

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

- 1 From the main menu, select option 24 to open **Menu 24 - System Maintenance**.
- 2 From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

**Figure 287** Menu 24.4: System Maintenance: Diagnostic



### 34.5.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN. 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.

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

**Table 178** System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the <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.
PPPoE/PPTP 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 27 on page 399</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.



**Table 178** System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
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 35

## 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.

### 35.1 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.

### 35.2 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 179** 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

## 35.3 Backup Configuration

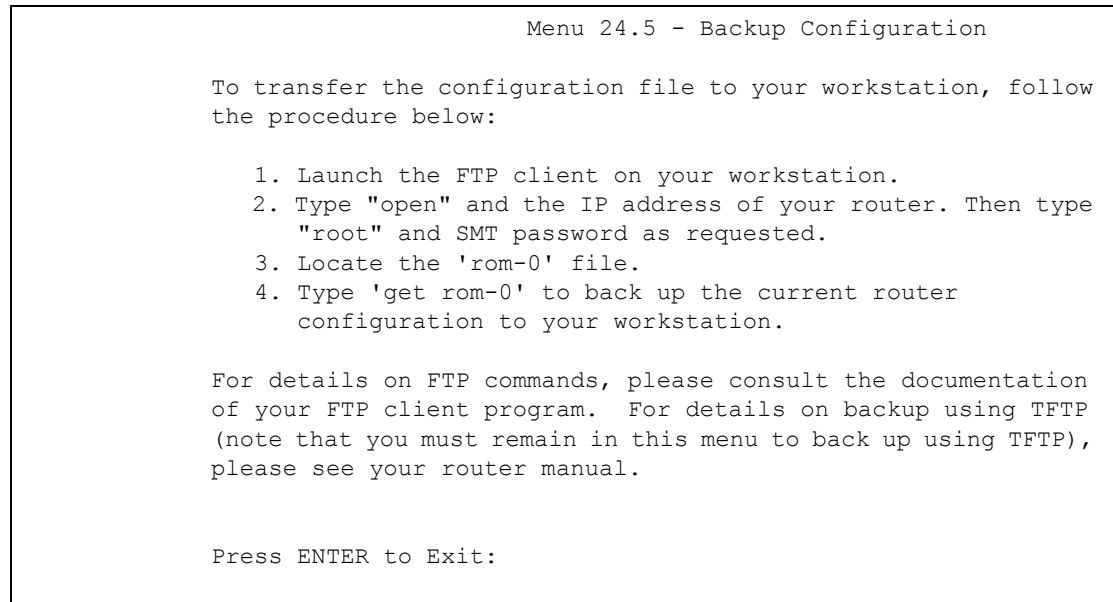
**Note:** The ZyWALL displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 depending on whether you use the console port or Telnet.

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.

### 35.3.1 Backup Configuration

Follow the instructions as shown in the next screen.

**Figure 288** Telnet into Menu 24.5

### 35.3.2 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 user name.
- 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.

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

**Figure 289** 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

```

### 35.3.4 GUI-based FTP Clients

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

**Table 180** 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).

### 35.3.5 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.

### 35.3.6 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.

### 35.3.7 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.

### 35.3.8 GUI-based TFTP Clients

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

**Table 181** 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 35.3.5 on page 470](#) to read about configurations that disallow TFTP and FTP over WAN.

### 35.3.9 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 290** 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 291** 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.



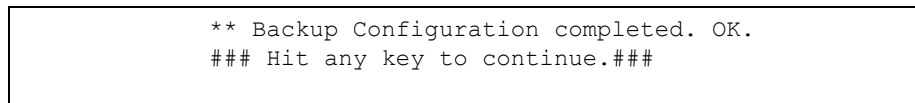
**Figure 292** Backup Configuration Example

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 293** Successful Backup Confirmation Screen

## 35.4 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.

### 35.4.1 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 294** Telnet into Menu 24.6

```
Menu 24.6 -- System Maintenance - Restore Configuration

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

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

For details on backup using TFTP (note that you must remain in this menu
to back up using TFTP), please see your router manual.

Press ENTER to Exit:
```

- 1** Launch the FTP client on your computer.
- 2** Enter “open”, followed by a space and the IP address of your ZyWALL.
- 3** Press [ENTER] when prompted for a user name.
- 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.

## 35.4.2 Restore Using FTP Session Example

**Figure 295** 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 35.3.5 on page 470](#) to read about configurations that disallow TFTP and FTP over WAN.

## 35.4.3 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 296** System Maintenance: Restore Configuration

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

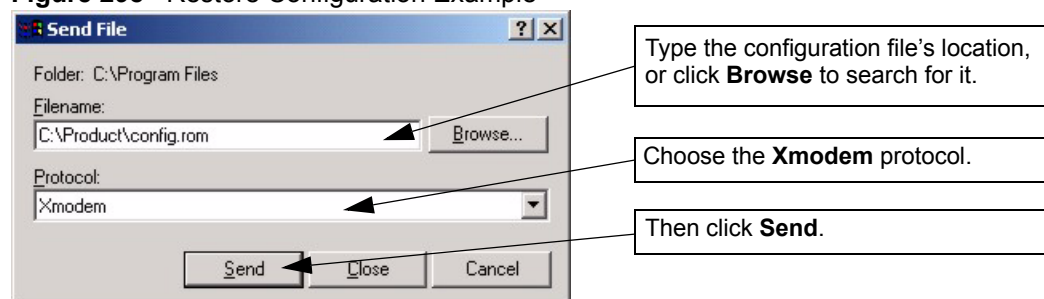
- 2 The following screen indicates that the Xmodem download has started.

**Figure 297** 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 298** 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 299** Successful Restoration Confirmation Screen

```
Save to ROM
Hit any key to start system reboot.
```

## 35.5 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 35.4 on page 473](#) 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.

### 35.5.1 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 300** 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:
```

## 35.5.2 Configuration File Upload

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

**Figure 301** 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

### 35.5.3 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 user name.
- 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.

### 35.5.4 FTP Session Example of Firmware File Upload

**Figure 302** 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 35.3.5 on page 470](#) to read about configurations that disallow TFTP and FTP over WAN.

### 35.5.5 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.

### 35.5.6 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).

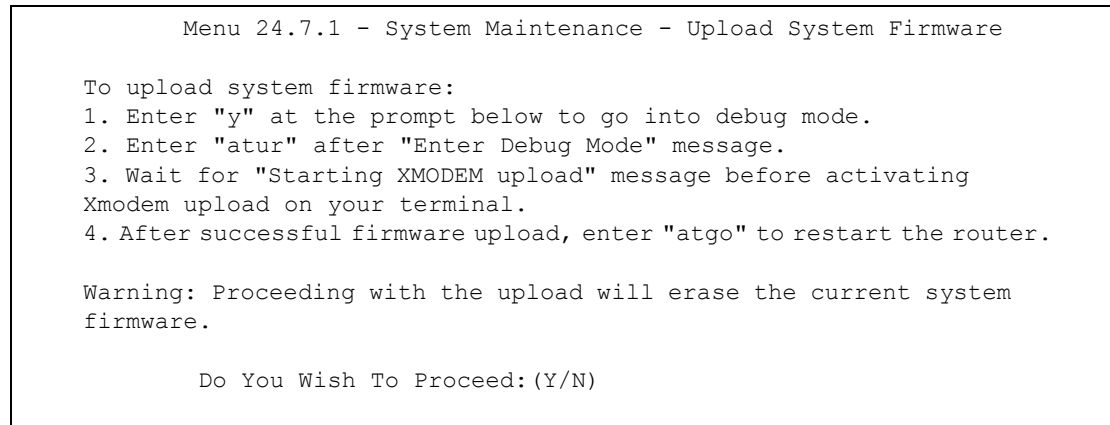
Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

### 35.5.7 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.

### 35.5.8 Uploading Firmware File Via Console Port

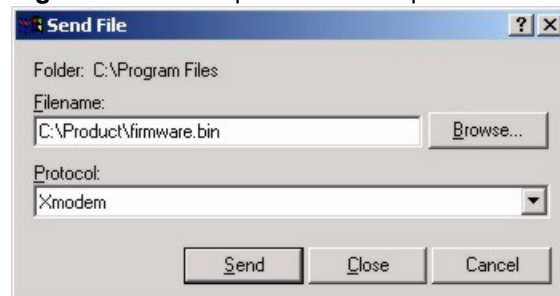
- 1 Select 1 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.1 - System Maintenance - Upload System Firmware, and then follow the instructions as shown in the following screen.

**Figure 303** Menu 24.7.1 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.

### 35.5.9 Example Xmodem Firmware Upload Using HyperTerminal

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

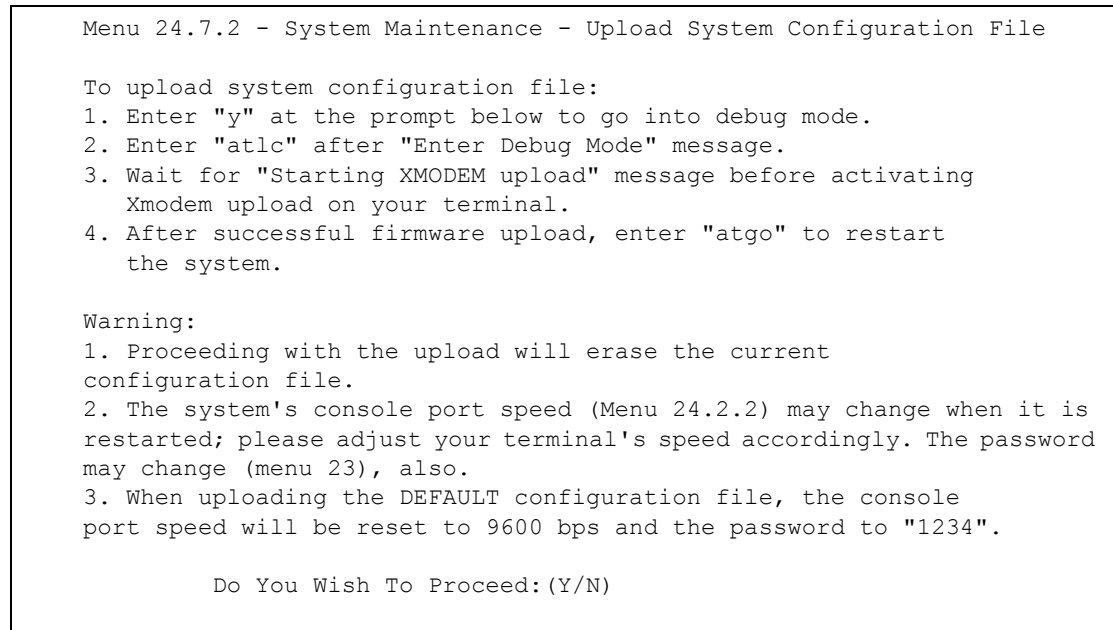
**Figure 304** Example Xmodem Upload

After the firmware upload process has completed, the ZyWALL will automatically restart.

### 35.5.10 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.

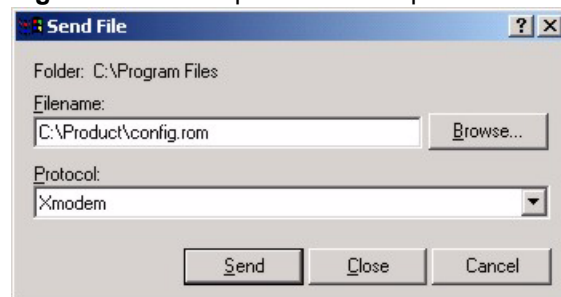


**Figure 305** Menu 24.7.2 As Seen Using the Console Port

- 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.

### 35.5.11 Example Xmodem Configuration Upload Using HyperTerminal

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

**Figure 306** Example Xmodem Upload

After the configuration upload process has completed, restart the ZyWALL by entering "atgo".



# CHAPTER 36

## System Maintenance Menus 8 to 10

This chapter leads you through SMT menus 24.8 to 24.10.

### 36.1 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 307** 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:
```

#### 36.1.1 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.

### 36.1.2 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 308** Valid Commands

```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          ether          aux
ip           ipsec          bridge        bm
certificates radius
ras>
```

The following table describes some commands in this screen.

**Table 182** 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.
radius	These commands display RADIUS information and configure RADIUS settings.

## 36.2 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 309** Call Control

```
Menu 24.9 - System Maintenance - Call Control

1.Budget Management
2.Call History

Enter Menu Selection Number:
```

### 36.2.1 Budget Management

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

**Figure 310** Budget Management

Menu 24.9.1 - Budget Management		
Remote Node Period	Connection Time/Total Budget	Elapsed Time/Total
1.ChangeMe	No Budget	No Budget
2.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 183** 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.

### 36.2.2 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 311** 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 184** 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.	

## 36.3 Time and Date Setting

There is a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL. Menu 24.10 allows you to update the time and date settings of your ZyWALL. The real time is then displayed in the logs.

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

**Figure 312** Menu 24: System Maintenance

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

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 313** 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 185** 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 185** 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 37

## Remote Management

This chapter covers remote management found in SMT menu 24.11.

### 37.1 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:

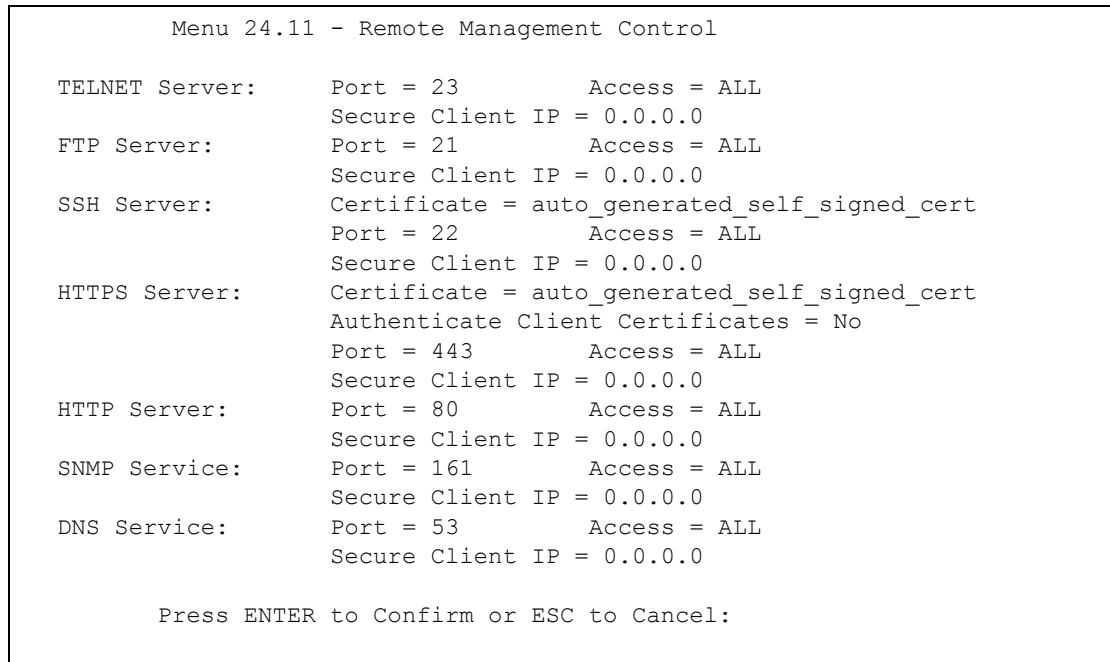
- Internet (WAN only)
- LAN only,
- ALL (LAN&WAN)
- Neither (Disable).

**Note:** When you choose **WAN only**, or **ALL** (LAN & WAN), 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 314** Menu 24.11 – Remote Management Control



The following table describes the fields in this screen.

**Table 186** 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].
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 G on page 557</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.	

### 37.1.1 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 38

## Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

### 38.1 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 315** 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 316** 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 187** 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 187** 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 317** 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 318** 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 39

## 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.

### 39.1 Problems Starting Up the ZyWALL

**Table 188** 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.

### 39.2 Problems with the LAN Interface

**Table 189** 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.

## 39.3 Problems with the WAN Interface

**Table 190** 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 109</a> or <a href="#">Chapter 27 on page 399</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 109</a> or <a href="#">Chapter 25 on page 381</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 69</a> or <a href="#">Chapter 24 on page 375</a> .

## 39.4 Problems Accessing the ZyWALL

**Table 191** 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 54</a> in <a href="#">Chapter 2 on page 53</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>

**Table 191** Troubleshooting Accessing the ZyWALL

PROBLEM	CORRECTIVE ACTION
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> <hr/> <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> <hr/> <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>

### 39.4.1 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.

#### 39.4.1.1 Internet Explorer Pop-up Blockers

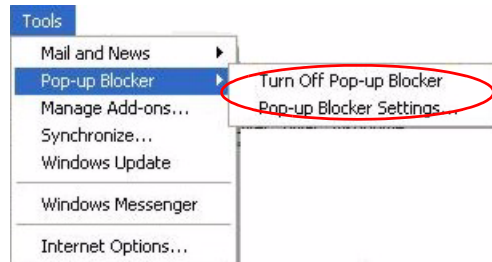
You may have to disable pop-up blocking to log into your device.

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.

### 39.4.1.1.1 Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

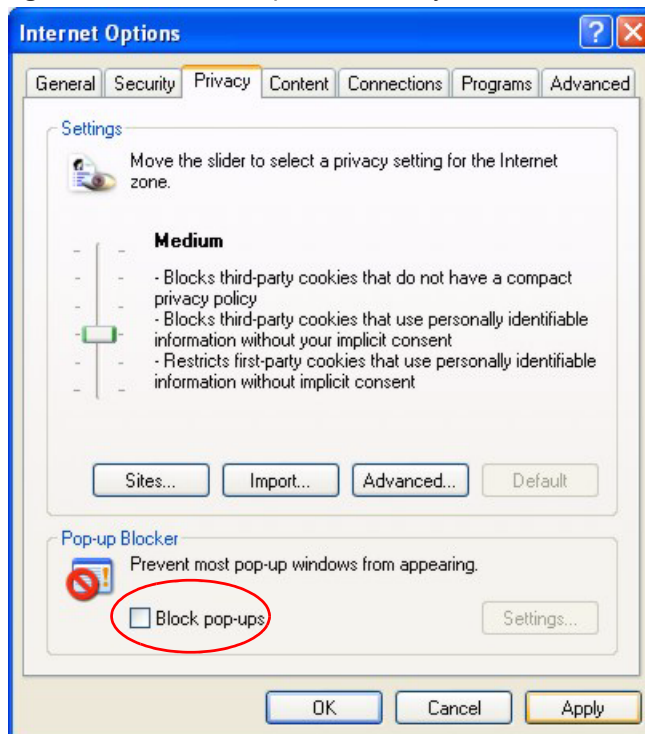
**Figure 319** Pop-up Blocker



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 320** Internet Options: Privacy



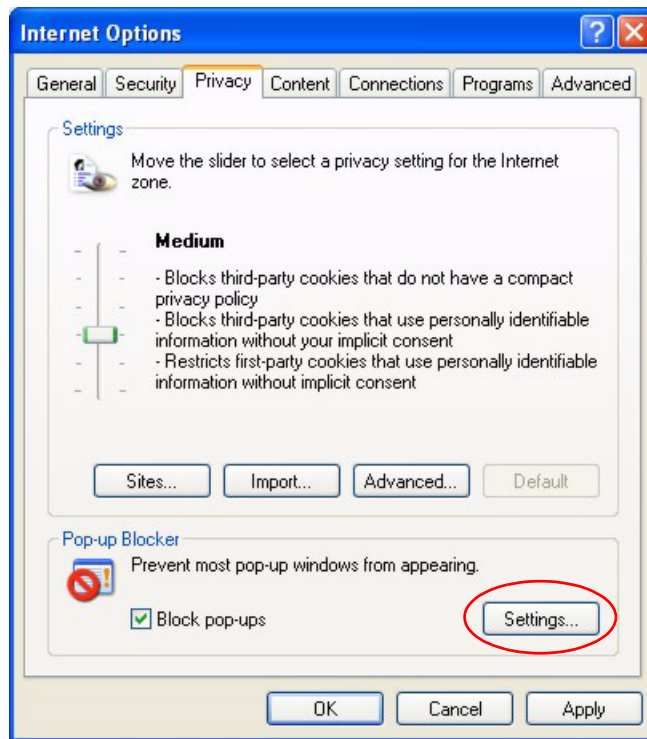
- 3 Click **Apply** to save this setting.

### 39.4.1.1.2 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 > Privacy**.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

**Figure 321** 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 322** Pop-up Blocker Settings

**5** Click **Close** to return to the **Privacy** screen.

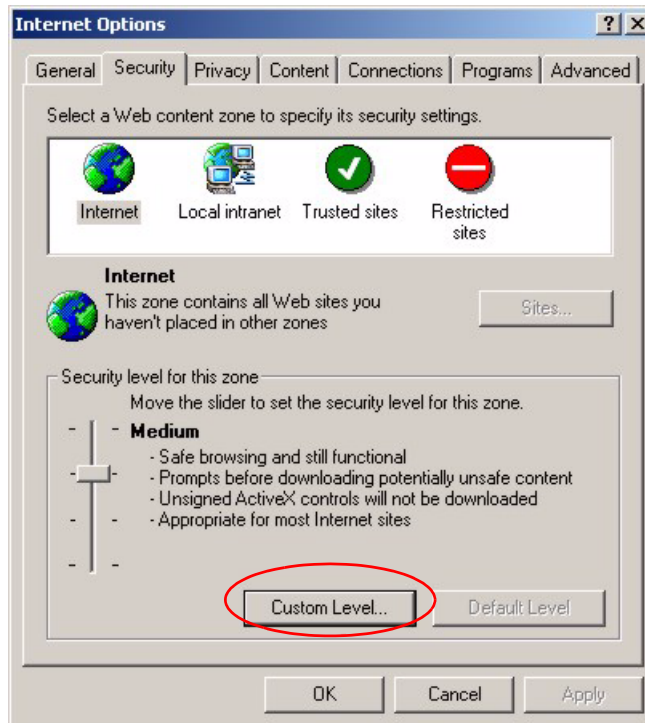
**6** Click **Apply** to save this setting.

### 39.4.1.2 JavaScripts

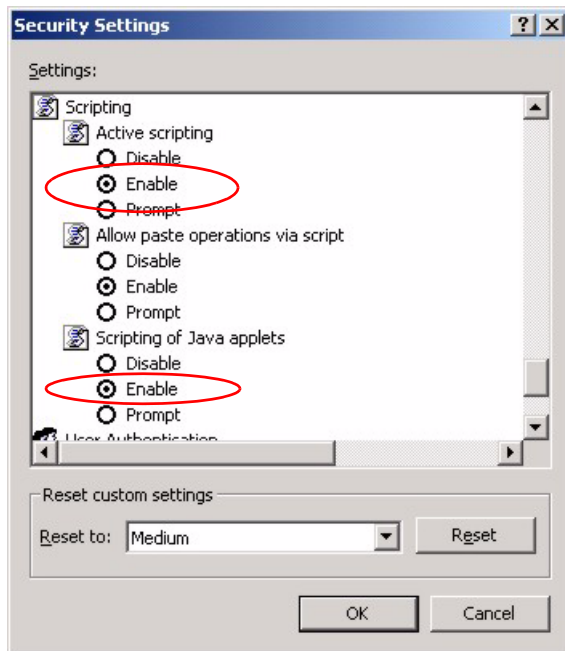
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

**1** In Internet Explorer, click **Tools > Internet Options > Security**.



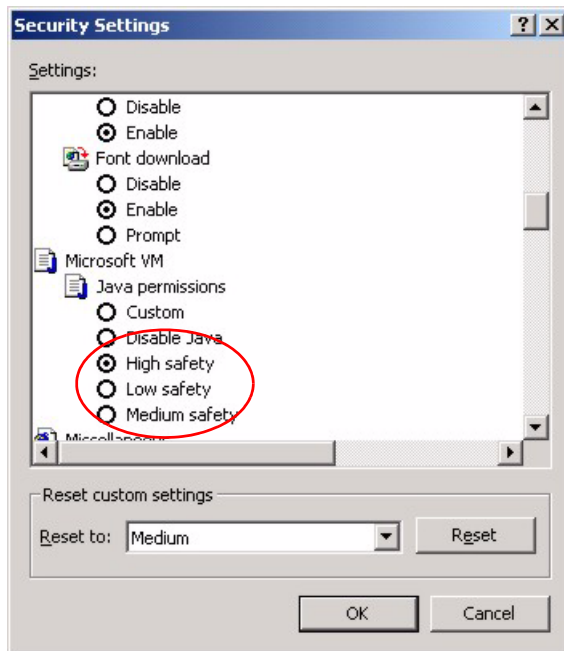
**Figure 323** Internet Options: Security

- 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 324** Security Settings - Java Scripting

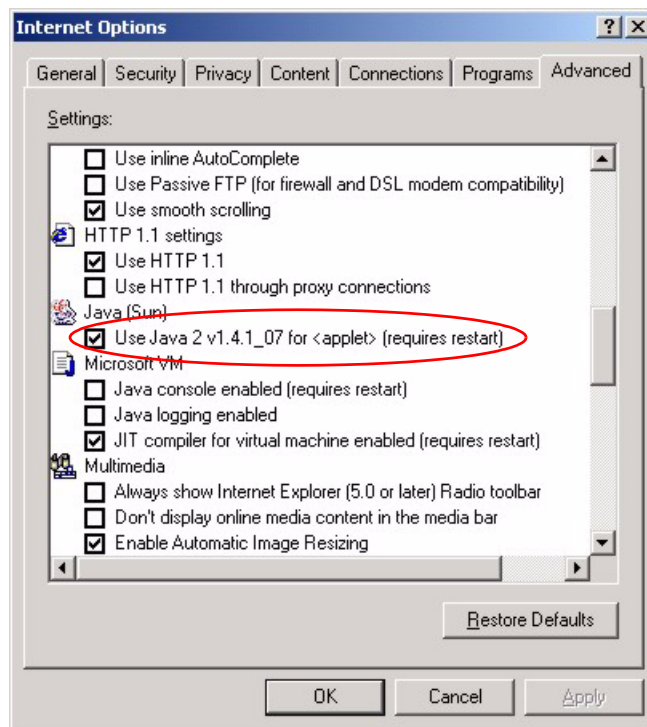
### 39.4.1.3 Java Permissions

- 1 From Internet Explorer, click **Tools > Internet Options > Security**.
- 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 325** Security Settings - Java

#### 39.4.1.3.1 JAVA (Sun)

- 1 From Internet Explorer, click **Tools > Internet Options > Advanced**.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

**Figure 326** Java (Sun)

## 39.5 Packet Flow

The following is the packet check flow on the ZyWALL.

**LAN to WAN:** LAN Data and Call Filtering (in SMT menu 21) -> Firewall -> Remote Node Data Filtering (in SMT menu 21) -> Content Filtering -> NAT

**WAN to LAN:** Remote Node Data Filtering (in SMT menu 21) -> NAT -> Firewall -> LAN 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 192** Device Specifications

Default LAN 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	181(W) x 128(D) x 36(H) mm
Weight	304g
Power Specification	12V DC, 1 A
Ethernet Interface	
LAN	Four LAN auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports.
WAN	One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
Reset Button	Restores factory default settings
Console	RJ-45 port for RS-232 null modem connection
Dial Backup	RJ-45 port for RS-232 connection
Operation Temperature	0° C ~ 50° C
Storage Temperature	-30° C ~ 60° C
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

**Table 193** Performance

CATEGORY	PERFORMANCE
Firewall Throughput	24Mbps
VPN 3DES/AES Throughput	24Mbps
User Licenses	Unlimited

**Table 193** Performance (continued) (continued)

CATEGORY	PERFORMANCE
Concurrent Sessions	3000
Simultaneous IPSec VPN Connections	2

**Table 194** 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 X-Auth User Authentication (Internal Database and External RADIUS) DH1/2, RSA signature
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 Priority-bandwidth utilization Bandwidth Management Static Routes
High Availability (HA)	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
Logging/Monitoring	Centralized Logs Attack alert System status monitoring Syslog

**Table 194** 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 IEEE 802.1X
Other Features	Transparent Firewall (Bridge mode) Dynamic DNS IP Alias Static Routes

**Table 195** Feature Specifications

FEATURE	SPECIFICATION
Number of Static DHCP Table Entries	32
Number of Static Routes	12
Number of Port Forwarding Rules	12
Number of NAT Sessions	3000
Number of Address Mapping Rules	10
Number of Source or Destination IP Address Entries in a Firewall Rule	20
Number of IPSec VPN Tunnels/Security Associations	2
Number of Bandwidth Management Classes	10
Number of Bandwidth Management Class Levels	1
Number of DNS Address Record Entries	30
Number of DNS Name Server Record Entries	16

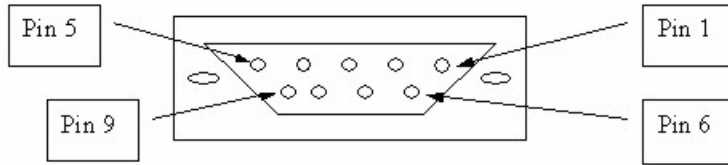
## Cable Pin Assignments

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>1</sup>

The console cable and dial backup cable each have an RJ-45 connector and a DB-9 connector. The pin layout for the DB-9 connector end of the cables is as follows.

1. Pins 2,3 and 5 are used.

**Figure 327** Console/Dial Backup Cable DB-9 End Pin Layout



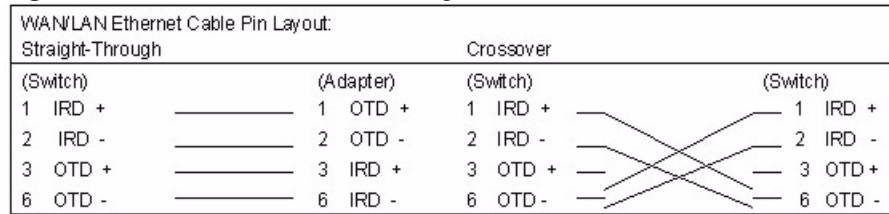
**Table 196** Console Cable Pin Assignments

PIN DEFINITION	RJ-45 END	DB-9M (MALE) END
DSR	1	6
DTR	2	4
TX	3	3
RTS	4	7
GND	5	5
RX	6	2
CTS	7	8
DCD	8	1
	N/A	9

**Table 197** Console Cable Pin Assignments

PIN DEFINITION	RJ-45 END	DB-9M (MALE) END
DTR	1	4
DSR	2	6
RX	3	2
CTS	4	8
GND	5	5
TX	6	3
RTS	7	7
DCD	8	1
	N/A	9



**Figure 328** Ethernet Cable Pin Assignments

## Wall Mounting Specifications

Use two M4 x 30 mm screws to wall-mount the ZyWALL.

The holes for the wall-mounting screws should be 108 mm apart.

## Power Adaptor Specifications

**Table 198** Power Adaptor Specifications

AC Power Adapter Model	PSA18R-120P
Input Power	AC 100~240Volts/50~60Hz/0.5A
Output Power	DC 12Volts/1.5A,
Power Consumption	18W
Safety Standards	UL/EN60950-1, UL (cUL), TUV,CB
Safety Standards	TUV, CE(EN 60950)



# APPENDIX B

## Wall-mounting Instructions

Do the following to hang your ZyWALL on a wall.

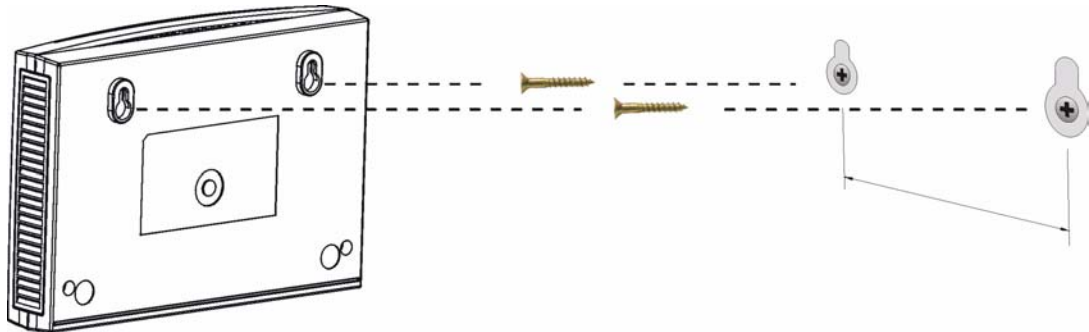
**Note:** See the product specifications appendix for the size of screws to use and how far apart to place them.

- 1 Locate a high position on wall that is free of obstructions. Use a sturdy wall.
- 2 Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

**Note:** Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

- 3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the ZyWALL with the connection cables.
- 5 Align the holes on the back of the ZyWALL with the screws on the wall. Hang the ZyWALL on the screws.

**Figure 329** Wall-mounting Example





# APPENDIX C

## Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

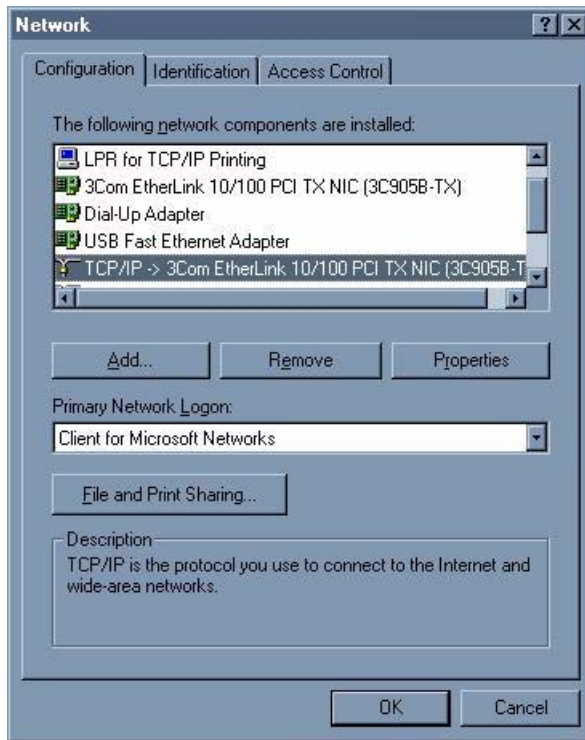
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyWALL's LAN port.

### Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 330** 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:

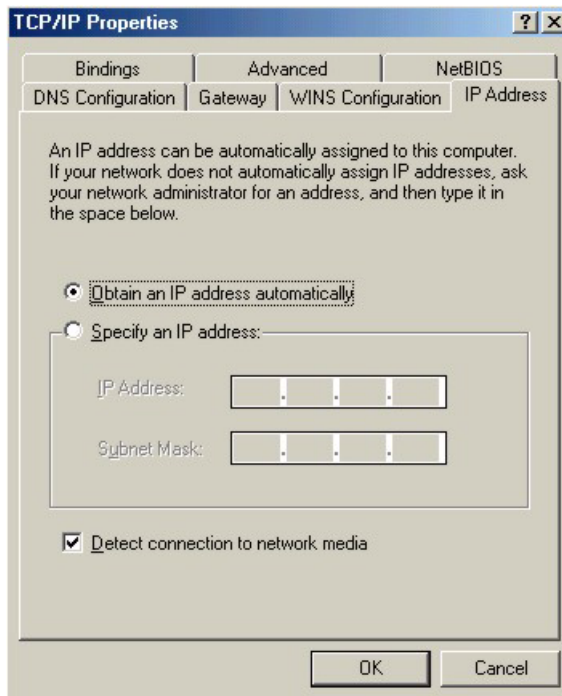
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 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.

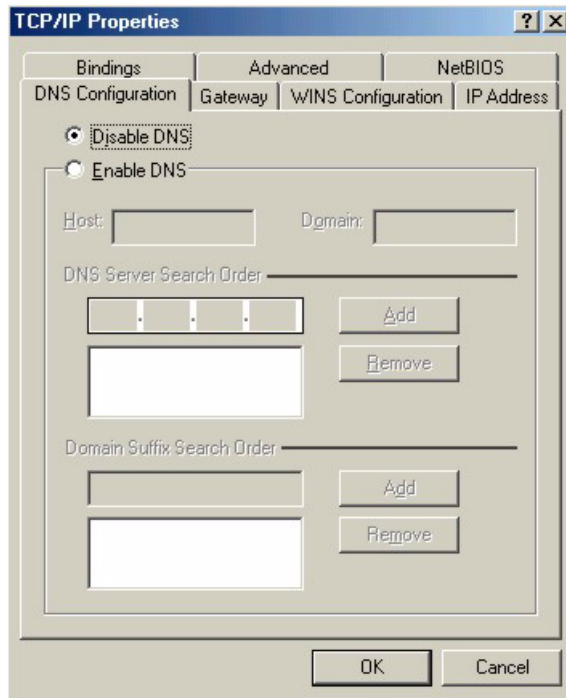
## Configuring

- 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 331** 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 332** Windows 95/98/Me: TCP/IP Properties: DNS Configuration**4** Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

**5** Click **OK** to save and close the **TCP/IP Properties** window.**6** Click **OK** to close the **Network** window. Insert the Windows CD if prompted.**7** Turn on your ZyWALL and restart your computer when prompted.

## Verifying Settings

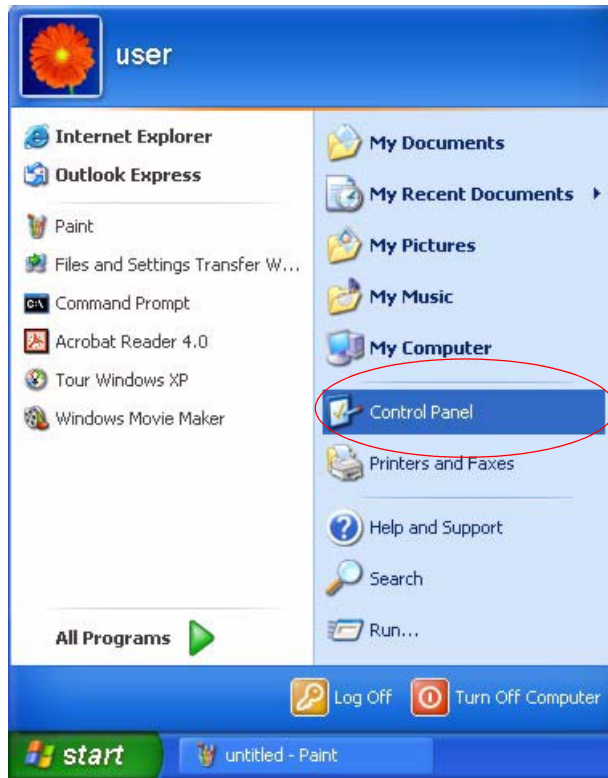
**1** Click **Start** and then **Run**.**2** In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.**3** Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

**1** Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

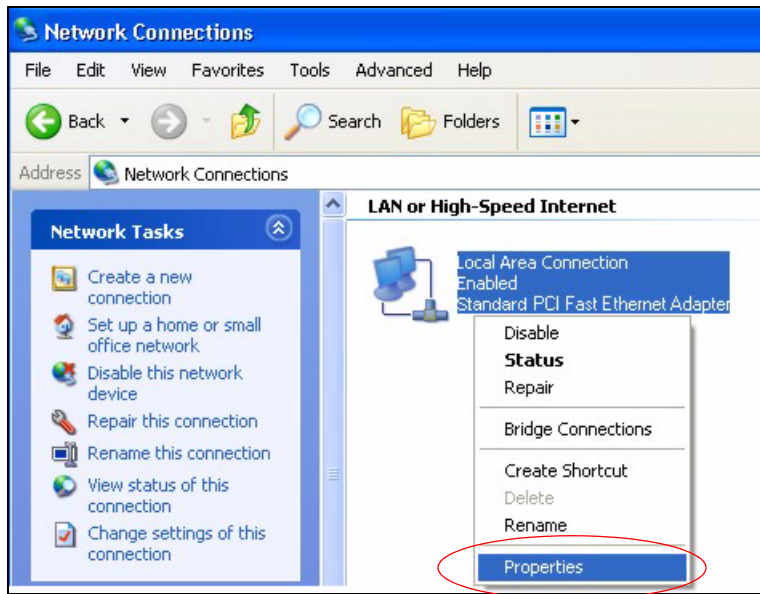


**Figure 333** Windows XP: Start Menu

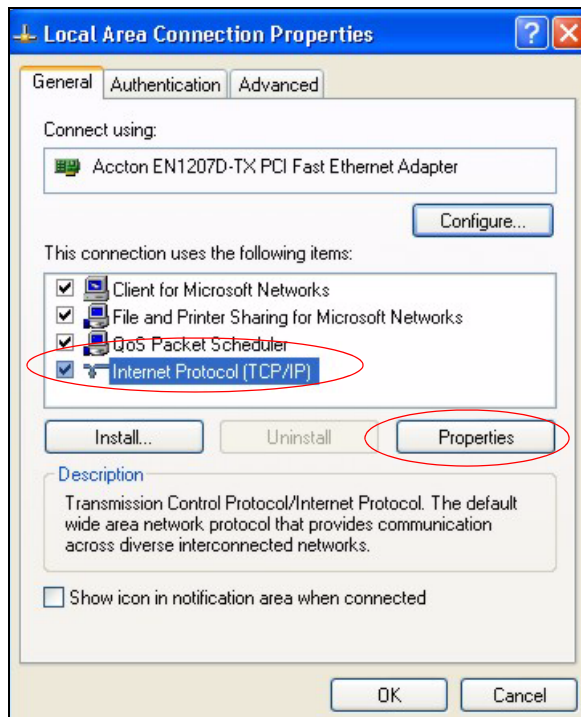
**2** In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

**Figure 334** Windows XP: Control Panel

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

**Figure 335** Windows XP: Control Panel: Network Connections: Properties

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

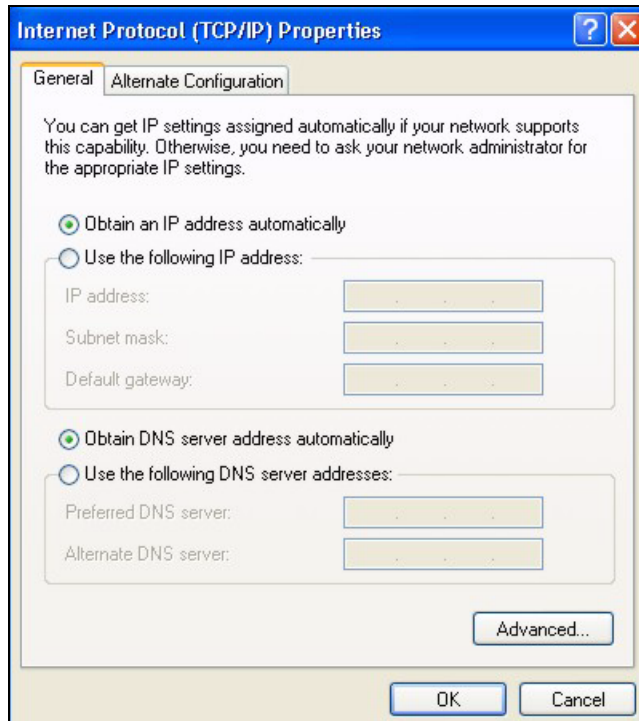
**Figure 336** Windows XP: Local Area Connection Properties

- 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**.

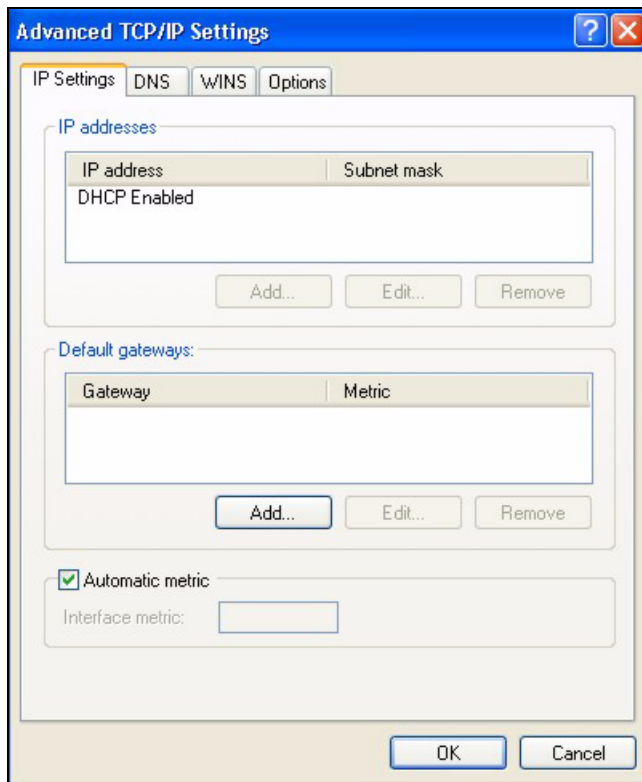
**Figure 337** Windows XP: Internet Protocol (TCP/IP) Properties



- 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:

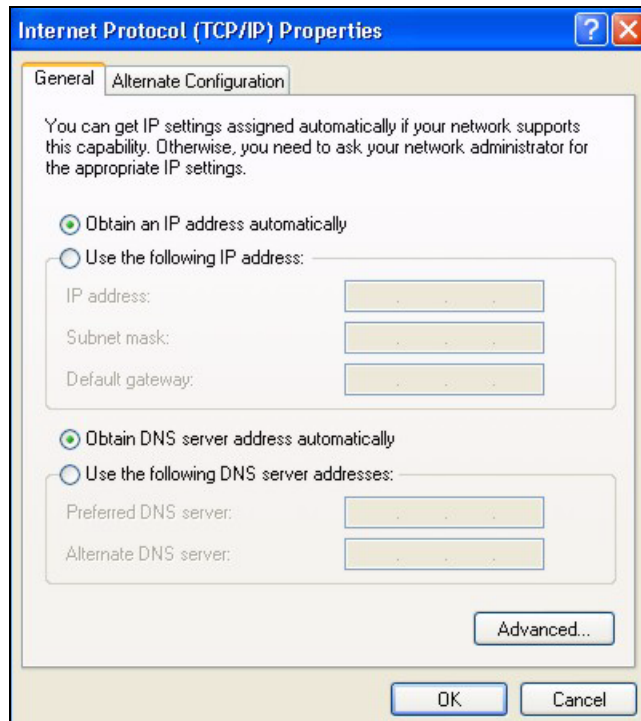
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP 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 338** 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 **> DNS** to order them.

**Figure 339** 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 ZyWALL and restart your computer (if prompted).

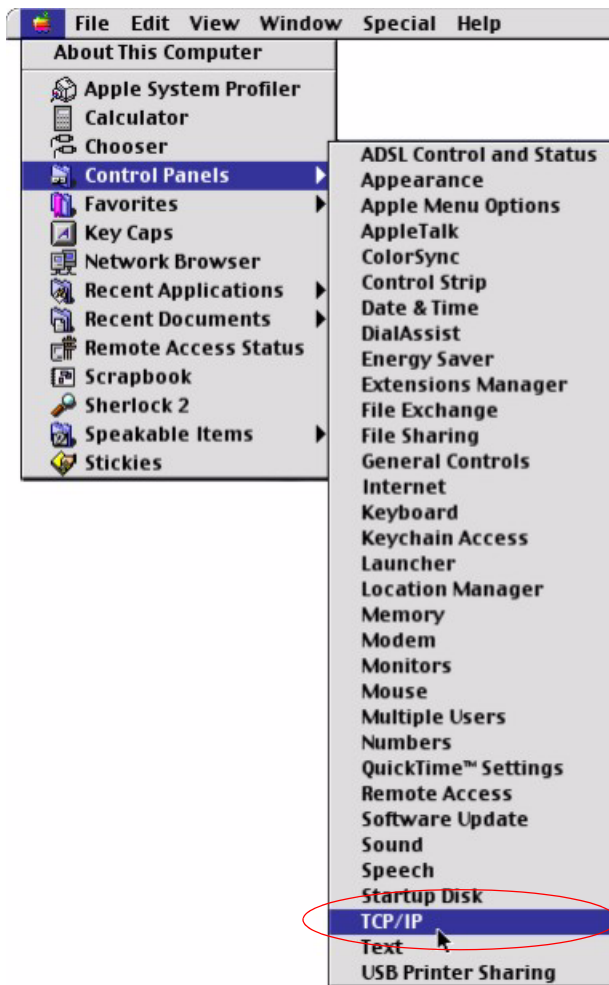
## Verifying Settings

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

## Macintosh OS 8/9

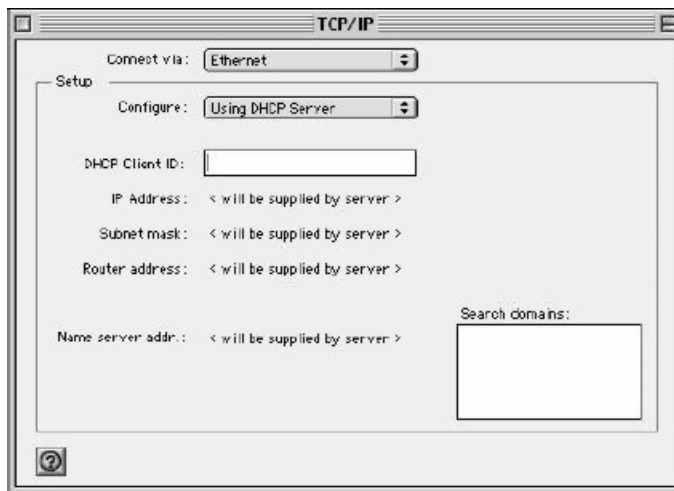
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 340** Macintosh OS 8/9: Apple Menu



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

**Figure 341** Macintosh OS 8/9: TCP/IP



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

- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your ZyWALL in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
- 6 Click **Save** if prompted, to save changes to your configuration.
- 7 Turn on your ZyWALL and restart your computer (if prompted).

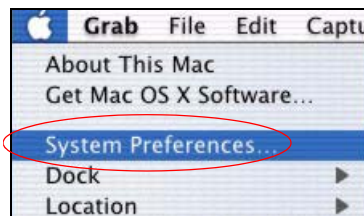
## Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

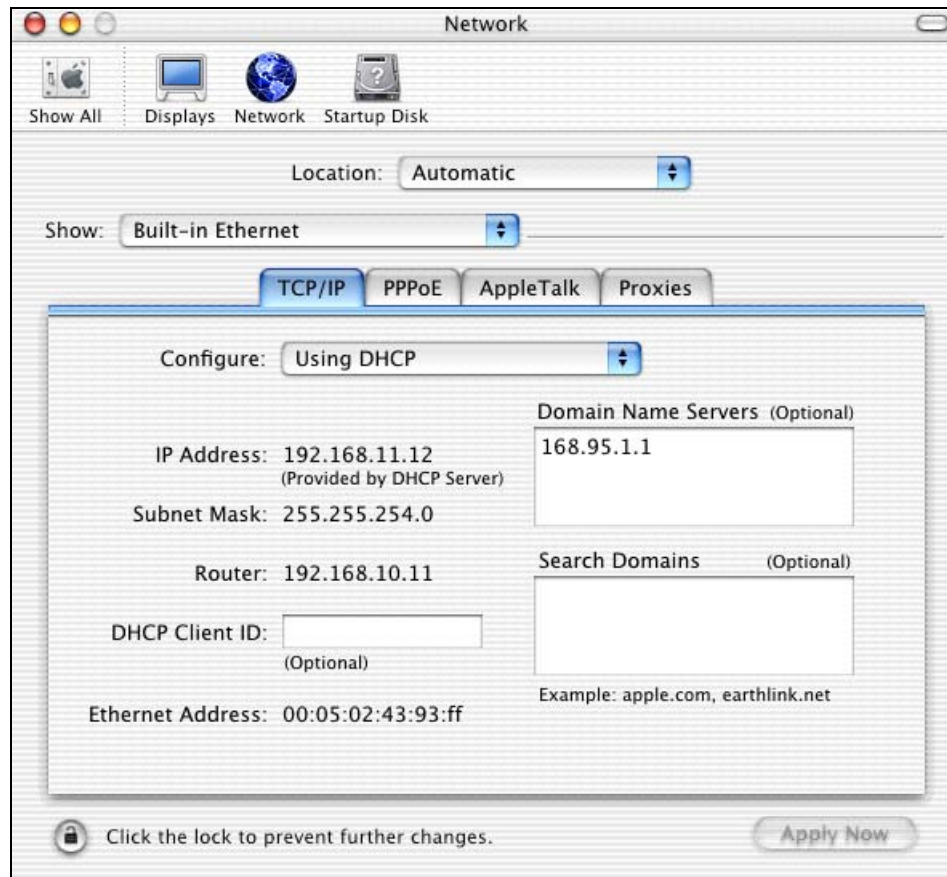
## Macintosh OS X

- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 342** 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 343** Macintosh OS X: Network

**4** For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyWALL in the **Router address** box.

**5** Click **Apply Now** and close the window.

**6** Turn on your ZyWALL and restart your computer (if prompted).

## Verifying Settings

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

## 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.



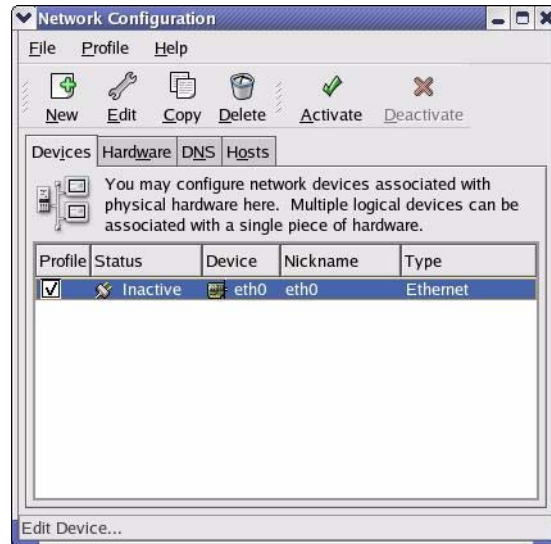
**Note:** Make sure you are logged in as the root administrator.

## 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 344** 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 345** Red Hat 9.0: KDE: Ethernet Device: General

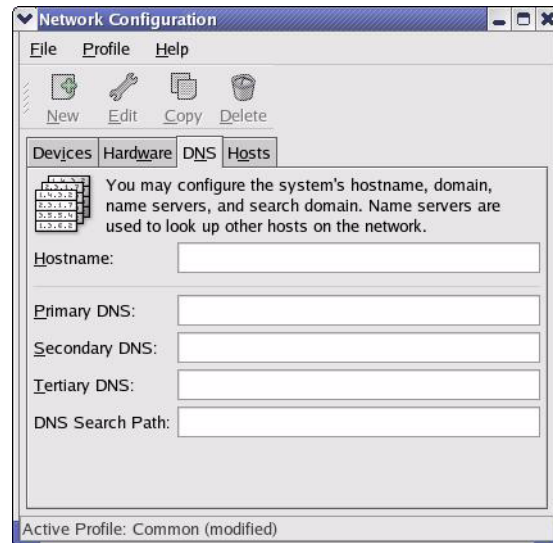


- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

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.

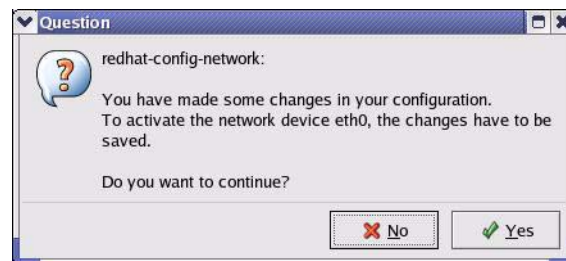
**Figure 346** Red Hat 9.0: KDE: Network Configuration: DNS



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 347** 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 348** 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 349** 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 350** 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 351** 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 352** 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 D

## 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 199** 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 200** 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 201** “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 202** 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 203** 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 204** 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 205** 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 206** 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 207** 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 208** 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 209** 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 210** 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 211** 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 199 on page 533](#)) available for subnetting.

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

**Table 212** 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 E

## Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 213** Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also 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. <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
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 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.

**Table 213** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (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.
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.

**Table 213** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
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.





# APPENDIX F

## 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.

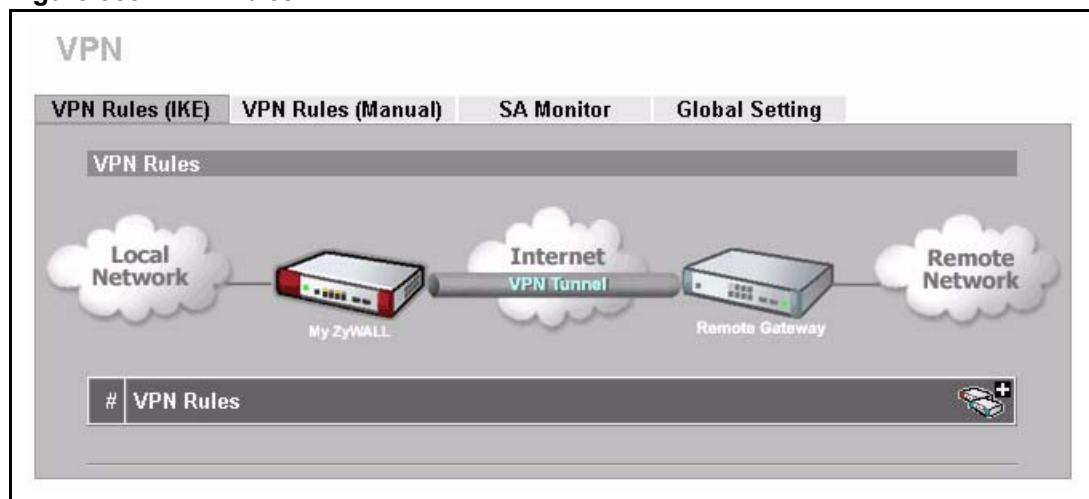
The following pages show a typical configuration that builds a tunnel between two private networks. One network is the headquarters (HQ) and the other is a branch office. Both sites have static (fixed) public addresses. Replace the **Remote Gateway Address** and **Local/Remote Starting IP Address** settings 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 353** 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 354 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 355** 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 356 Headquarters VPN Rule

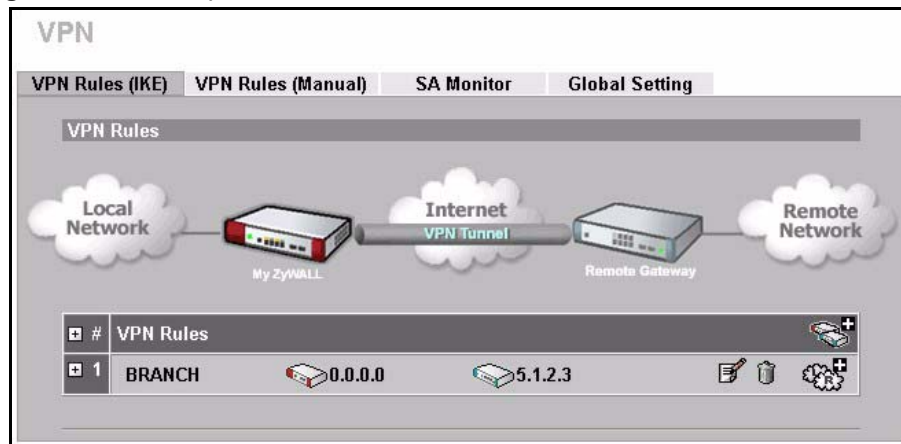
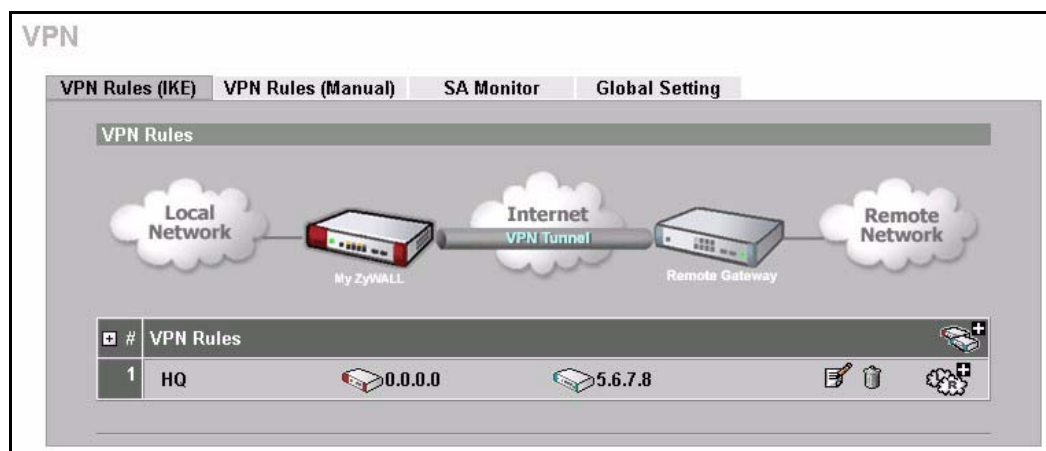


Figure 357 Branch Office VPN Rule



- 4 Configure the screens in the headquarters and the branch office as follows and click **Apply**.

Figure 358 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
- Perfect Forward Secrecy (PFS): NONE
- Enable Replay Detection
- Enable Multiple Proposals

Apply Cancel

Figure 359 Branch Office Network Policy Edit

**VPN - NETWORK POLICY - EDIT**

**Property**

Active Activate the network policy.

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

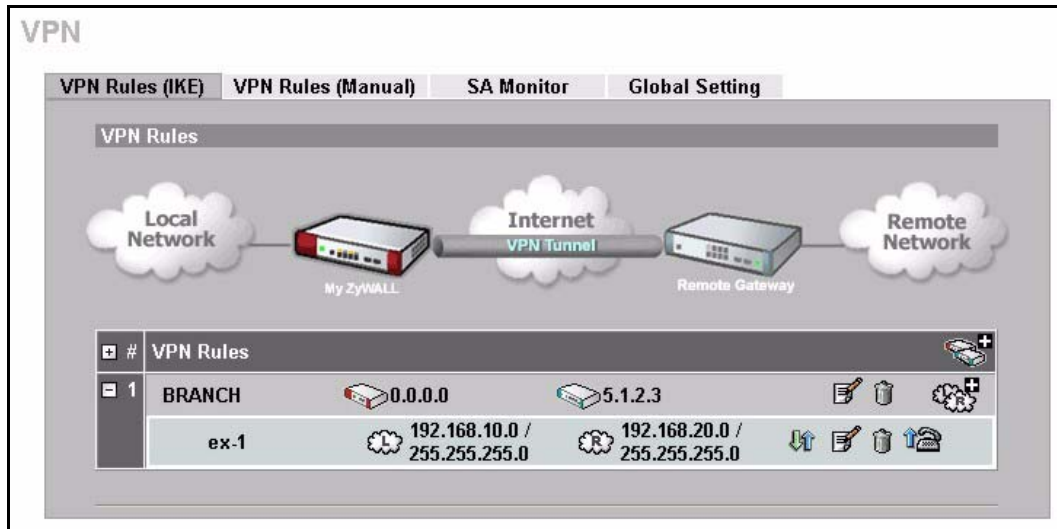
Enable Multiple Proposals

IP addresses on different subnets.

## Dialing the VPN Tunnel via Web Configurator

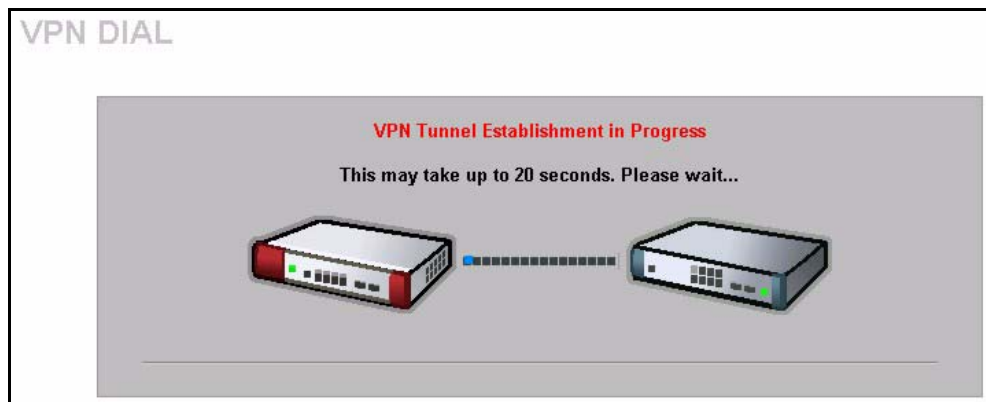
To test whether the IPSec routers can build the VPN tunnel, click the dial (📞) icon in the **VPN Rules (IKE)** screen to have the IPSec routers set up the tunnel.

**Figure 360** VPN Rule Configured



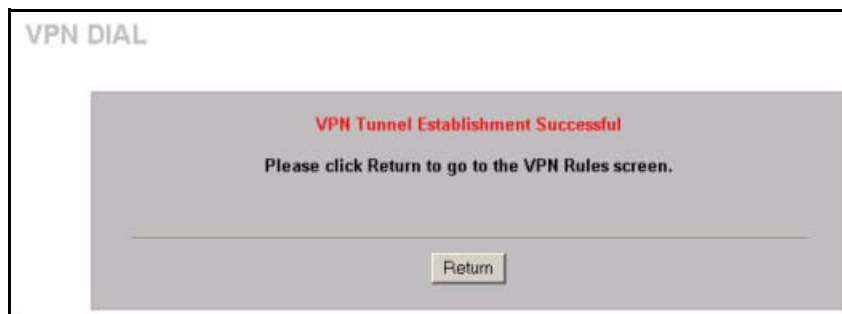
The following screen displays.

**Figure 361** VPN Dial



This screen displays later if the IPSec routers can build the VPN tunnel.

**Figure 362** 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 N on page 587](#) for information on the log messages.

Figure 363 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][NOTFY: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][NOTFY: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 364** 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 354 on page 547](#).

```
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 G

## 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 365** 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 366** Login Screen



**2** Click **Install Certificate** to open the **Install Certificate** wizard.

**Figure 367** Certificate General Information before Import



**3** Click **Next** to begin the **Install Certificate** wizard.

**Figure 368** Certificate Import Wizard 1

**4** Select where you would like to store the certificate and then click **Next**.

**Figure 369** Certificate Import Wizard 2

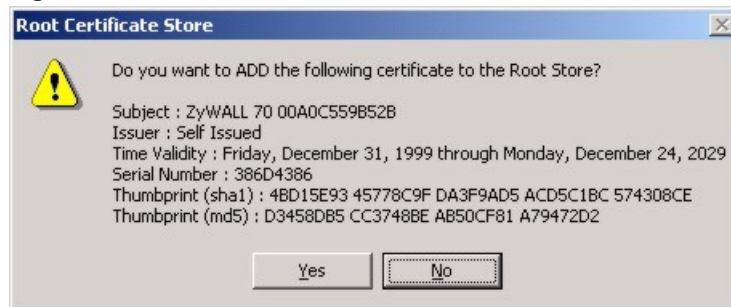
**5** Click **Finish** to complete the **Import Certificate** wizard.

**Figure 370** Certificate Import Wizard 3



**6** Click **Yes** to add the ZyWALL certificate to the root store.

**Figure 371** Root Certificate Store





**Figure 372** 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 373** ZyWALL Trusted CA Screen



The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

## Installing the CA's Certificate

- 1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

**Figure 374** 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 375** 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 376** Personal Certificate Import Wizard 2

- 3 Enter the password given to you by the CA.

**Figure 377** Personal Certificate Import Wizard 3

The screenshot shows the 'Certificate Import Wizard' window at the 'Password' step. The title bar reads 'Certificate Import Wizard'. The main text says 'To maintain security, the private key was protected with a password.' Below this, it asks 'Type the password for the private key.' There is a text box labeled 'Password:'. Below the text box are two checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' and 'Mark the private key as exportable'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- 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 378** Personal Certificate Import Wizard 4

The screenshot shows the 'Certificate Import Wizard' window at the 'Certificate Store' step. The title bar reads 'Certificate Import Wizard'. The main text says 'Certificate stores are system areas where certificates are kept.' Below this, it says 'Windows can automatically select a certificate store, or you can specify a location for'. There are two radio buttons: 'Automatically select the certificate store based on the type of certificate' (which is selected) and 'Place all certificates in the following store'. Below the second radio button is a text box labeled 'Certificate store:' and a 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- 5 Click **Finish** to complete the wizard and begin the import process.

**Figure 379** Personal Certificate Import Wizard 5

- 6 You should see the following screen when the certificate is correctly installed on your computer.

**Figure 380** Personal Certificate Import Wizard 6

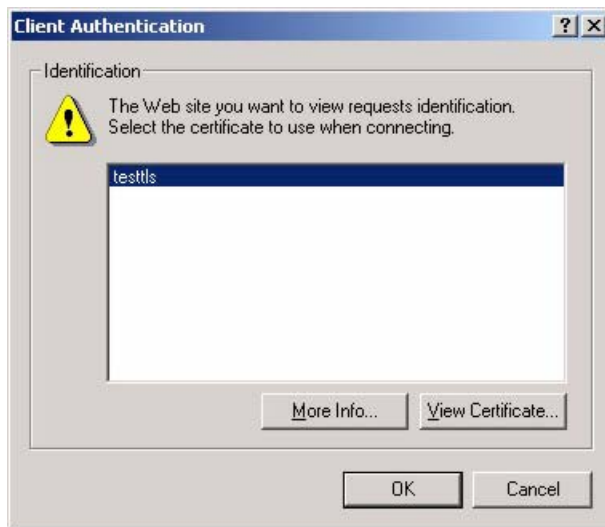
## Using a Certificate When Accessing the ZyWALL Example

Use the following procedure to access the ZyWALL via HTTPS.

- 1 Enter 'https://ZyWALL IP Address/' in your browser's web address field.

**Figure 381** 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 382** SSL Client Authentication

3 You next see the ZyWALL login screen.

**Figure 383** ZyWALL Secure Login Screen





# APPENDIX H

## 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 I

## Firewall Commands

The following describes the firewall commands. See [Appendix H on page 569](#) for information on the command structure.

**Table 214** 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 214** 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 214** 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 214** 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 214** 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 J

## NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See [Appendix H on page 569](#) 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 between Ethernet interfaces.
- 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  
IPSec Packets: Forward  
Trigger Dial: Disabled
```

The filter types and their default settings are as follows.

**Table 215** 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
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  
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 3 on` This command blocks IPSec NetBIOS packets.

`sys filter netbios config 4 off` This command stops NetBIOS commands from initiating calls.

# APPENDIX K

## Certificates Commands

The following describes the certificate commands. See [Appendix H on page 569](#) for information on the command structure.

All of these commands start with certificates.

**Table 216** 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 216** 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 216** 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 216** 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 L

## 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 H on page 569](#) for information on the command structure.

**Table 217** 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 M

## 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 384** 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 385** 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 N

## Log Descriptions

This appendix provides descriptions of example log messages.

**Table 218** 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 218** 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.
%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 219** System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.
Dial Backup starts	Dial backup started working.
Dial Backup ends	Dial backup stopped working.

**Table 219** System Error Logs (continued)

LOG MESSAGE	DESCRIPTION
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 220** 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 221** 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.

**Table 221** TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
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 222** 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 236 on page 601](#).

**Table 223** 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.

**Table 223** ICMP Logs (continued)

LOG MESSAGE	DESCRIPTION
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 224** 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 225** PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

**Table 226** UPnP Logs

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

**Table 227** 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" check box, the system forwards the web content.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The ZyWALL cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The ZyWALL cannot issue a query because TCP/IP socket creation failed, port:port number.
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

For type and code details, see [Table 236 on page 601](#).

**Table 228** 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.



**Table 228** Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
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.
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.

**Table 228** Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
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 229** 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 230** 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.

**Table 230** IPSec Logs (continued)

LOG MESSAGE	DESCRIPTION
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 231** IKE Logs

LOG MESSAGE	DESCRIPTION
Active connection allowed exceeded	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
Start Phase 2: Quick Mode	Phase 2 Quick Mode has started.
Verifying Remote ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
Verifying Local ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
IKE Packet Retransmit	The router retransmitted the last packet sent because there was no response from the peer.
Failed to send IKE Packet	An Ethernet error stopped the router from sending IKE packets.
Too many errors! Deleting SA	An SA was deleted because there were too many errors.
Phase 1 IKE SA process done	The phase 1 IKE SA process has been completed.
Duplicate requests with the same cookie	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
IKE Negotiation is in process	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
No proposal chosen	Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
Local / remote IPs of incoming request conflict with rule <%d>	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.

**Table 231** IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Cannot resolve Secure Gateway Addr for rule <%d>	The router couldn't resolve the IP address from the domain name that was used for the secure gateway address.
Peer ID: <peer id> <My remote type> -<My local type>	The displayed ID information did not match between the two ends of the connection.
vs. My Remote <My remote> - <My remote>	The displayed ID information did not match between the two ends of the connection.
vs. My Local <My local>-<My local>	The displayed ID information did not match between the two ends of the connection.
Send <packet>	A packet was sent.
Recv <packet>	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
Recv <Main or Aggressive> Mode request from <IP>	The router received an IKE negotiation request from the peer address specified.
Send <Main or Aggressive> Mode request to <IP>	The router started negotiation with the peer.
Invalid IP <Peer local> / <Peer local>	The peer's "Local IP Address" is invalid.
Remote IP <Remote IP> / <Remote IP> conflicts	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Phase 1 ID type mismatch	This router's "Peer ID Type" is different from the peer IPsec router's "Local ID Type".
Phase 1 ID content mismatch	This router's "Peer ID Content" is different from the peer IPsec router's "Local ID Content".
No known phase 1 ID type found	The router could not find a known phase 1 ID in the connection attempt.
ID type mismatch. Local / Peer: <Local ID type/Peer ID type>	The phase 1 ID types do not match.
ID content mismatch	The phase 1 ID contents do not match.
Configured Peer ID Content: <Configured Peer ID Content>	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
Incoming ID Content: <Incoming Peer ID Content>	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
Unsupported local ID Type: <%d>	The phase 1 ID type is not supported by the router.
Build Phase 1 ID	The router has started to build the phase 1 ID.
Adjust TCP MSS to %d	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
Rule <%d> input idle time out, disconnect	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
XAUTH succeed! Username: <Username>	The router used extended authentication to authenticate the listed user name.

**Table 231** IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
XAUTH fail! Username: <Username>	The router was not able to use extended authentication to authenticate the listed user name.
Rule[%d] Phase 1 negotiation mode mismatch	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
Rule [%d] Phase 1 encryption algorithm mismatch	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication algorithm mismatch	The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication method mismatch	The listed rule's IKE phase 1 authentication method did not match between the router and the peer.
Rule [%d] Phase 1 key group mismatch	The listed rule's IKE phase 1 key group did not match between the router and the peer.
Rule [%d] Phase 2 protocol mismatch	The listed rule's IKE phase 2 protocol did not match between the router and the peer.
Rule [%d] Phase 2 encryption algorithm mismatch	The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 2 authentication algorithm mismatch	The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 2 encapsulation mismatch	The listed rule's IKE phase 2 encapsulation did not match between the router and the peer.
Rule [%d]> Phase 2 pfs mismatch	The listed rule's IKE phase 2 perfect forward secret (pfs) setting did not match between the router and the peer.
Rule [%d] Phase 1 ID mismatch	The listed rule's IKE phase 1 ID did not match between the router and the peer.
Rule [%d] Phase 1 hash mismatch	The listed rule's IKE phase 1 hash did not match between the router and the peer.
Rule [%d] Phase 1 preshared key mismatch	The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer.
Rule [%d] Tunnel built successfully	The listed rule's IPsec tunnel has been built successfully.
Rule [%d] Peer's public key not found	The listed rule's IKE phase 1 peer's public key was not found.
Rule [%d] Verify peer's signature failed	The listed rule's IKE phase 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.

**Table 231** IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%d] phase 2 mismatch	The listed rule's IKE phase 2 did not match between the router and the peer.
Rule [%d] Phase 2 key length mismatch	The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.
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 232** 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.

**Table 232** PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
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 233 on page 599</a> for the corresponding descriptions of the codes.

**Table 233** 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.

**Table 233** Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
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 234** 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
Local User Database does not support authentication 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.



**Table 234** 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
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 235** 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.
(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.

**Table 236** 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

**Table 236** ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	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

## 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 237** 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 ("DEV" would be the ZyWALL itself).
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.

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 238** RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal

**Table 238** RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
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

This section provides some general examples of how to use the log commands. The items that display with your device may vary but the basic function should be the same.

Go to the command interpreter interface. [Appendix H on page 569](#) explains how to access and use the commands.

## Configuring What You Want the ZyWALL to Log

This is a generic example of how to use the commands to configure your device to log specific things. These commands may display some different items but the basic function should be as follows.

- 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 386** 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			

- 3 Use `sys logs category` followed by a log category to display the parameters that are available for the category.

**Figure 387** 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 [45](#)

## A

Action for Matched Packets [142](#)

Active [386, 388, 404](#)

Active Protocol [187](#)

AH [187](#)

and Authentication Algorithms [188](#)

and Encapsulation [189](#)

and Encryption Algorithms [188](#)

and NAT [190](#)

ESP [187](#)

Address Assignment [111, 285](#)

Adjust TCP Maximum Segment Size [212](#)

AH [187](#)

and Authentication Algorithms [188](#)

and Encryption Algorithms [188](#)

and NAT [190](#)

and Transport Mode [189](#)

ALG [46, 333](#)

Allocated Budget [387, 407](#)

Alternative Subnet Mask Notation [535](#)

Anti-Probing [142](#)

Application Layer Gateway [46, 333](#)

Applications [50](#)

AT Command [383, 384](#)

AT command [468](#)

Authen [386, 407](#)

Authentication [386, 406, 407](#)

Authentication Algorithms [188](#)

and Active Protocol [188](#)

MD5 [188](#)

SHA1 [188](#)

Authentication Header. See AH

Authentication Protocol [406](#)

Auto-negotiation [45](#)

## B

Backup [364, 468](#)

Backup VPN Connection [191](#)

Backup WAN [45](#)

Bandwidth Borrowing [274](#)

Bandwidth Class [269](#)

Bandwidth Filter [269, 280](#)

Bandwidth Management [46, 269](#)

Bandwidth Management Statistics [281](#)

Bandwidth Manager Class Configuration [278](#)

Bandwidth Manager Class Setup [277](#)

Bandwidth Manager Monitor [282](#)

Bandwidth Manager Summary [275](#)

Bridge Protocol Data Units (BPDUs) [105](#)

Bridging [405](#)

Budget Management [485, 486](#)

## C

Call Back Delay [385](#)

Call Control [485](#)

Call History [486, 487](#)

Call Scheduling [48, 495](#)

Max Number of Schedule Sets [495](#)

PPPoE [497](#)

Precedence [495](#)

Call-Triggering Packet [463](#)

Central Network Management [49](#)

Certificate [197](#)

Certificates

and IKE SA [183, 184](#)

Certifications [4](#)

Notice 1 [4](#)

Viewing [4](#)

Changing the Password [373](#)

CHAP [386, 407](#)

Command Interpreter Mode [483](#)

Command Line [469](#)

Community [453](#)

Configuration [65, 95](#)

Configuration File

Backup [468](#)

Connection ID/Name [408](#)  
Console Port [457](#), [458](#), [459](#)  
    Configuration File Upload [480](#)  
    File Backup [472](#)  
    File Upload [479](#)  
    Restoring Files [475](#)  
Contact Information [8](#)  
Content Filter Categories [158](#)  
Content Filter General [155](#)  
Content Filtering [47](#), [155](#)  
    Customizing [165](#)  
    Days and Times [155](#)  
    Filter List [155](#)  
    Restrict Web Features [155](#)  
Copyright [3](#)  
Customer Support [8](#)

## D

DDNS  
    Configuration [377](#)  
DDNS Type [379](#)  
Default [366](#)  
Denial of Service [131](#), [143](#), [146](#), [435](#)  
Denial of Services  
    Thresholds [145](#)  
DHCP [65](#), [95](#), [96](#), [97](#), [106](#), [294](#), [351](#), [395](#)  
DHCP (Dynamic Host Configuration Protocol) [49](#)  
DHCP Ethernet Setup [394](#)  
DHCP Table [65](#)  
Diagnostic [463](#)  
Dial Timeout [385](#)  
Diffie-Hellman Key Group [183](#)  
    Perfect Forward Secrecy (PFS) [185](#)  
Disclaimer [3](#)  
DNS [317](#)  
DNS Server  
    For VPN Host [286](#)  
Domain Name [111](#), [351](#), [457](#), [458](#)  
DoS (Denial of Service) [47](#)  
Drop Timeout [385](#)  
DSL Modem [50](#), [405](#)  
DTR [127](#), [384](#)  
Dynamic DNS [294](#)  
Dynamic DNS Support [48](#)  
DYNDNS Wildcard [286](#), [294](#)

## E

Edit IP [387](#), [405](#)  
Enable Wildcard [379](#)  
Encapsulating Security Payload. See ESP.  
Encapsulation [400](#), [404](#), [408](#)  
    and Active Protocol [189](#)  
    and NAT [190](#)  
    Transport Mode [189](#)  
    Tunnel Mode [189](#)  
    VPN [189](#)  
Encryption Algorithms [188](#)  
    3DES [188](#)  
    AES [188](#)  
    and Active Protocol [188](#)  
    DES [188](#)  
Entering Information [369](#)  
ESP [187](#)  
    and Authentication Algorithms [188](#)  
    and Encryption Algorithms [188](#)  
    and NAT [190](#)  
    and Transport Mode [189](#)  
Ethernet [69](#), [71](#), [112](#)  
Ethernet Encapsulation [399](#), [404](#), [411](#)  
Extended Authentication  
    IKE SA [185](#)

## F

Factory Default [382](#)  
Fairness-based Scheduler [271](#)  
FCC Interference Statement [4](#)  
Filename Conventions [467](#)  
Filter [392](#), [410](#), [437](#)  
    Applying [451](#)  
    Configuration [437](#)  
    Configuring [441](#)  
    Example [448](#)  
    Generic Filter Rule [446](#)  
    Generic Rule [447](#)  
    NAT [450](#)  
    Remote Node [452](#)  
Filters  
    Executing a Filter Rule [438](#)  
    IP Filter Logic Flow [445](#)  
Firewall [47](#)  
    Access Methods [435](#)  
    Activating [435](#)  
    Address Type [141](#)  
    Creating/Editing Rules [139](#)  
    Custom Ports See Custom Ports [148](#)  
    Firewall Vs Filters [440](#)



SMT Menus [435](#)  
 When To Use [441](#)  
 Firewall Threshold [145](#)  
 Firmware File  
 Maintenance [467](#)  
 Flow Control [367](#)  
 FTP [294](#), [297](#), [312](#), [469](#), [493](#)  
 File Upload [478](#)  
 GUI-based Clients [470](#)  
 Restoring Files [473](#)  
 FTP File Transfer [476](#)  
 FTP Restrictions [297](#), [470](#), [493](#)  
 FTP Server [50](#), [427](#)  
 Full Network Management [50](#)

## G

Gateway IP Addr [409](#)  
 Gateway IP Address [400](#), [414](#)  
 Gateway Policy [193](#), [194](#)  
 General Setup [351](#), [375](#)  
 Global [249](#)

## H

Hidden Menus [368](#)  
 Host [353](#), [379](#)  
 Host IDs [533](#)  
 How SSH works [306](#)  
 How STP Works [105](#)  
 HTTPS [47](#), [298](#)  
 HTTPS Example [300](#)  
 HyperTerminal [480](#), [481](#)  
 HyperTerminal program [472](#), [475](#)

## I

IANA [94](#)  
 Idle Timeout [387](#), [406](#), [407](#)  
 IEEE 802.1x [48](#)  
 IGMP [96](#)  
 IKE SA  
 Aggressive Mode [182](#)  
 and Certificates [183](#), [184](#)  
 and RADIUS [185](#)  
 Authentication Algorithms [188](#)

Client Mode (Extended Authentication) [185](#)  
 Content [184](#)  
 Diffie-Hellman Key Group [183](#)  
 Encryption Algorithms [188](#)  
 Extended Authentication [185](#)  
 ID Type [184](#)  
 IP Address, Remote IPSec Router [183](#)  
 IP Address, ZyXEL Device [183](#)  
 Local Identity [184](#)  
 Main Mode [181](#)  
 NAT Traversal [190](#)  
 Negotiation Mode [180](#)  
 Password [185](#)  
 Peer Identity [184](#)  
 Pre-shared Key [183](#)  
 Proposal [183](#)  
 SA Life Time [191](#)  
 Server Mode (Extended Authentication) [185](#)  
 User Name [185](#)  
 IKE SA. See also VPN.  
 Incoming Protocol Filters [397](#)  
 Initial Screen [367](#)  
 Inside [249](#)  
 Inside Global Address [249](#)  
 Inside Local Address [249](#)  
 Internet Access [69](#)  
 ISP's Name [400](#)  
 Internet Access Setup [399](#), [400](#), [415](#)  
 Internet Assigned Numbers Authority See IANA [94](#)  
 Internet Protocol Security. See IPSec.  
 Introduction to Filters [437](#)  
 IP Address [65](#), [93](#), [97](#), [106](#), [111](#), [258](#), [260](#), [261](#), [396](#),  
[397](#), [400](#), [409](#), [422](#)  
 Remote [389](#)  
 IP Address Assignment [400](#), [409](#)  
 IP Addressing [533](#)  
 IP Alias [49](#), [397](#)  
 IP Alias Setup [397](#)  
 IP Classes [533](#)  
 IP Multicast [48](#)  
 Internet Group Management Protocol (IGMP) [48](#)  
 IP Pool [98](#), [395](#)  
 IP Pool Setup [95](#)  
 IP protocol type [141](#)  
 IP Static Route [413](#), [414](#)  
 Active [414](#)  
 Destination IP Address [414](#)  
 IP Subnet Mask [414](#)  
 Name [414](#)  
 Route Number [414](#)  
 IP Subnet Mask [389](#), [397](#)  
 Remote [389](#)  
 IPSec [179](#)  
 IPSec HA [191](#)

IPSec High Availability [191](#)  
IPSec SA  
  Active Protocol [185, 187](#)  
  and NetBIOS [186](#)  
  Authentication Algorithms [188](#)  
  Authentication Key (for manual keys) [186](#)  
  Encapsulation [185, 189](#)  
  Encryption Algorithms [188](#)  
  Encryption Key (for manual keys) [186](#)  
  IP Addresses with Manual Keys [183](#)  
  Manual Keys [186](#)  
  Nail Up [191](#)  
  Overlapping Policies [186](#)  
  Perfect Forward Secrecy (PFS) [185](#)  
  Proposal [185](#)  
  Replay Detection [186](#)  
  SA Life Time [191](#)  
  Security Parameter Index (SPI) (for manual keys) [186](#)  
  Transport Mode [189](#)  
  Tunnel Mode [189](#)  
  when IKE SA is disconnected [191](#)  
IPSec SA. See also VPN.  
IPSec standard [46](#)  
IPSec VPN Capability [46, 47](#)  
IPSec. See also VPN.  
ISP Parameters [69](#)  
ISP's Name [400](#)

## L

LAN IP Address [346, 348](#)  
LAN Port Filter Setup [393](#)  
LAN Setup [393, 394](#)  
Link type [60](#)  
Local [249](#)  
Log [459](#)  
Log Facility [460](#)  
Logging [50](#)  
Login Name [400](#)  
Login Screen [368](#)

## M

MAC Address [382](#)  
Main Menu [369](#)  
Main Menu Commands [368](#)  
Management Information Base (MIB) [314](#)  
Many to Many No Overload [252](#)  
Many to Many Overload [252](#)

Many to One [252](#)  
Max Age [105](#)  
Maximize Bandwidth Usage [271, 276](#)  
Maximum Incomplete High [146](#)  
Maximum Incomplete Low [146](#)  
Metric [109, 267, 389, 407, 410, 414](#)  
Multicast [95, 96, 98, 390, 396, 410](#)  
Multimedia [335](#)  
My IP Addr [408](#)  
My Login [386, 405](#)  
My Login Name [400](#)  
My Password [386, 400, 405](#)  
My Server IP Addr [408](#)  
My WAN Address [389](#)  
myZyXEL.com [89](#)

## N

Nailed-Up Connection [407](#)  
Nailed-up Connection [406](#)  
Nailed-Up Connections [408](#)  
NAT [94, 258, 259, 389, 409, 410, 450](#)  
  and Active Protocol (VPN) [190](#)  
  and AH (VPN) [190](#)  
  and Encapsulation (VPN) [190](#)  
  and ESP (VPN) [190](#)  
  and VPN [190](#)  
  Application [251](#)  
  Applying NAT in the SMT Menus [415](#)  
  Configuring [417](#)  
  Definitions [249](#)  
  Examples [424](#)  
  How NAT Works [250](#)  
  Mapping Types [252](#)  
  NAT Unfriendly Application Programs [430](#)  
  Ordering Rules [420](#)  
  Port Restricted Cone [252](#)  
  What NAT does [250](#)  
NAT Routers [335](#)  
NAT Traversal [190, 321, 323](#)  
Navigation Panel [61](#)  
NetBIOS  
  and VPN [186](#)  
Network Address Translation [400](#)  
Network Address Translation (NAT) [49](#)  
Network Address Translators [335](#)  
Network Policy [194, 200](#)

**O**

Offline [379](#)  
 One Minute High [146](#)  
 One Minute Low [145](#)  
 One to One [252](#)  
 Outgoing Protocol Filters [398](#)  
 Outside [249](#)

**P**

Packet Filtering [48, 440](#)  
 PAP [386, 407](#)  
 Password [352, 368, 373, 400, 453](#)  
 Path cost [104](#)  
 Perfect Forward Secrecy (PFS)  
   Diffie-Hellman Key Group [185](#)  
 Period(hr) [387, 407](#)  
 Ping [464](#)  
 Point-to-Point Tunneling Protocol [72](#)  
 Point-to-Point Tunneling Protocol See PPTP [119](#)  
 Port Forwarding [49](#)  
 Port Restricted Cone NAT [252](#)  
 Power Adaptor [513](#)  
 Power Adaptor Specifications [513](#)  
 PPP [387](#)  
 PPPoE [48, 69, 71](#)  
 PPPoE Encapsulation [399, 402, 404, 405, 406, 407, 411](#)  
 PPTP [69, 72, 73, 119](#)  
   Client [401](#)  
   Configuring a Client [401](#)  
 PPTP Encapsulation [48, 72](#)  
 Pre-Shared Key [197](#)  
 Priority-based Scheduler [271](#)  
 Private [267, 389, 410, 414](#)  
 Private IP Address [111](#)  
 Product Registration [7](#)  
 Proportional Bandwidth Allocation [270](#)  
 Protocol Filters [397](#)  
   Incoming [397](#)  
   Outgoing [397](#)  
 Protocol/Port [346, 347](#)

**Q**

Quick Start Guide [53](#)

**R**

RADIUS [48, 243](#)  
   and IKE SA [185](#)  
     Shared Secret Key [244](#)  
 RADIUS Message Types [244](#)  
 RADIUS Messages [244](#)  
 Rapid STP [104](#)  
 Real time Transport Protocol [334](#)  
 Redundant VPN Connection [191](#)  
 Registration  
   Product [7](#)  
 Related Documentation [43](#)  
 Relay [395](#)  
 Rem IP Address [389](#)  
 Rem Node Name [386, 388, 404](#)  
 Remote Authentication Dial In User Service See  
   RADIUS [48](#)  
 Remote Management [491](#)  
   and VPN [180](#)  
 Remote Management Limitations [297](#)  
 Remote Node [403](#)  
 Remote Node Filter [391, 410](#)  
 Reports [345](#)  
 Required fields [369](#)  
 Reset Button [46](#)  
 Resetting the Time [356](#)  
 Resetting the ZyWALL [54](#)  
 Restore [364](#)  
 Restore Configuration [473](#)  
 Retry Count [385](#)  
 Retry Interval [385](#)  
 RFC 1889 [334](#)  
 RFC 3489 [335](#)  
 RIP [95, 389, 396, 397, 410](#)  
   Direction [397](#)  
   Version [397, 410](#)  
 RoadRunner Support [50](#)  
 Root bridge [104](#)  
 Root Class [277](#)  
 Route [405](#)  
 RTP [334](#)  
 Rules [131](#)  
   Creating Custom [131](#)

**S**

SA  
 Life Time [191](#)

Safety Warnings [6](#)  
Schedule Sets  
  Duration [496](#)  
Scheduler [271](#), [276](#)  
Schedules [405](#), [407](#), [408](#)  
Screws [513](#)  
Secure FTP Using SSH Example [310](#)  
Secure Telnet Using SSH Example [308](#)  
Server [253](#), [355](#), [356](#), [400](#), [405](#), [417](#), [419](#), [421](#), [422](#), [424](#),  
  [426](#), [427](#), [489](#)  
Server IP [405](#)  
Service Name [407](#)  
Service Type [147](#), [148](#), [400](#), [404](#)  
Services [258](#)  
Session Initiation Protocol [335](#)  
Set Up a Schedule [495](#)  
SIP Application Layer Gateway [46](#)  
SMT [368](#)  
SMT Menu Overview [371](#)  
SNMP [49](#), [313](#)  
  Community [453](#)  
  Configuration [453](#)  
  Get [314](#)  
  Manager [314](#)  
  MIBs [315](#)  
  Trap [314](#)  
  Trusted Host [453](#)  
SNMP (Simple Network Management Protocol) [49](#)  
Source Address [141](#)  
Spanning Tree Protocol [104](#)  
SSH [47](#), [306](#)  
SSH Implementation [307](#)  
Stateful Inspection [47](#), [131](#), [133](#)  
Static Route [265](#)  
STP (Spanning Tree Protocol) [46](#)  
STP Port States [105](#)  
STP See Spanning Tree Protocol [104](#)  
STP Terminology [104](#)  
SUA (Single User Account) [253](#), [415](#)  
Sub-class Layers [277](#)  
Subnet Mask [93](#), [97](#), [106](#), [141](#), [389](#), [396](#), [400](#), [409](#), [414](#)  
Subnet Masks [534](#)  
Subnetting [534](#)  
Supporting Disk [43](#)  
Syntax Conventions [44](#)  
Syslog [150](#), [153](#)  
Syslog IP Address [460](#)  
System Information [455](#), [457](#)  
System Maintenance [455](#), [456](#), [457](#), [458](#), [459](#), [460](#), [463](#),  
  [464](#), [468](#), [471](#), [479](#), [480](#), [483](#), [485](#), [486](#), [488](#), [489](#)  
System Management Terminal [368](#)

System Name [352](#), [375](#)  
System Statistics [64](#)  
System Status [455](#)  
System Timeout [298](#)

## T

TCP Maximum Incomplete [146](#)  
TCP/IP [311](#), [388](#), [394](#), [396](#), [408](#), [443](#), [444](#), [445](#), [447](#), [450](#)  
  Setup [396](#)  
TCP/IP and DHCP Setup [394](#)  
TCP/IP filter rule [443](#)  
Telnet [311](#)  
Telnet Configuration [311](#)  
Terminal Emulation [367](#)  
TFTP [471](#)  
  File Upload [478](#)  
  GUI-based Clients [472](#)  
TFTP and FTP over WAN [470](#)  
TFTP Restrictions [297](#), [470](#), [493](#)  
Three-Way Handshake [144](#)  
Threshold [145](#)  
Time and Date [46](#)  
Time and Date Setting [487](#), [488](#)  
Time Zone [353](#), [490](#)  
Timeout [387](#), [401](#), [402](#), [407](#)  
Trace [459](#)  
Tracing [50](#)  
Trademarks [3](#)  
Traffic Redirect [49](#), [122](#)  
Transport Mode [189](#)  
Triangle Route Solutions [149](#)  
Trigger Port Forwarding [432](#)  
Trivial File Transfer Protocol [471](#)

## U

Universal Plug and Play (UPnP) [321](#), [322](#)  
UNIX Syslog [460](#)  
Upload Firmware [476](#)  
UPnP [47](#), [321](#)  
UPnP Examples [324](#)  
UPnP Port Mapping [323](#)  
Use Server Detected IP [380](#)  
User Name [377](#)  
User Profiles [243](#)

**V**ZyNOS F/W Version [458](#), [468](#)

- Virtual Private Network [46](#)
- Virtual Private Network. See VPN.
- VPN [119](#), [179](#)
  - Active Protocol [187](#)
  - and NAT [190](#)
  - and Remote Management [180](#)
  - Established in Two Phases [179](#)
  - IKE SA. See IKE SA.
  - IPSec [179](#)
  - IPSec SA. See IPSec SA.
  - Local Network [179](#)
  - Manual Keys [180](#)
  - Proposal [181](#)
  - Remote IPSec Router [179](#)
  - Remote Network [179](#)
  - Security Association (SA) [179](#)
- VPN Application [51](#)
- VPN HA [191](#)
- VPN. See also IKE SA, IPSec SA. [179](#)
- VT100 [367](#)

**W**

- Wall Mounting Specifications [513](#)
- Wall-mounting Screws [513](#)
- WAN DHCP [464](#)
- WAN Setup [112](#), [381](#)
- Warranty [7](#)
  - Note [7](#)
- Web Configurator [53](#), [55](#), [133](#), [436](#)
- Web Site Hits [346](#), [347](#)
- Wizard Setup [69](#)
- WWW [299](#)
- www.dyndns.org [379](#)

**X**

- Xmodem
  - File Upload [480](#)
- XMODEM Protocol [468](#)

**Z**

- ZyNOS [458](#), [468](#)