

ZyWALL 1050

Internet Security Gateway

User's Guide

Version 1.00

9/2006

Edition 3

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".

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

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

Certifications

FCC Statement

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

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

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital switch, 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 instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection)

A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

Notices

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

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

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

Viewing Certifications

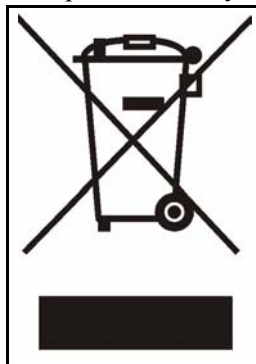
- 1 Go to www.zyxel.com.
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

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.
- 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.
- **CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.** Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.

This product is recyclable. Dispose of it properly.



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 or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been 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 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 for global products, or at 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	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	
COSTA RICA	soporte@zyxel.co.cr	+506-2017878	www.zyxel.co.cr	ZyXEL Costa Rica Plaza Roble Escazú Etapa El Patio, Tercer Piso San José, Costa Rica
	sales@zyxel.co.cr	+506-2015098	ftp.zyxel.co.cr	
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 Česká 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, Zoldomb 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	

METHOD	SUPPORT E-MAIL	TELEPHONE	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
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		
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 5 ^a 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		

Table of Contents

Copyright	3
Certifications	4
Safety Warnings	6
ZyXEL Limited Warranty	7
Customer Support	8
Table of Contents	11
List of Figures	27
List of Tables	37
About This User's Guide	43
Chapter 1	
Introducing the ZyWALL	47
1.1 Overview and Key Default Settings	47
1.2 Front Panel LEDs	48
1.3 Management Overview	48
1.4 Starting and Stopping the ZyWALL	50
1.5 Resetting the ZyWALL	50
Chapter 2	
Features and Applications	53
2.1 Features	53
2.2 Packet Flow	54
2.2.1 Interface to Interface (Through ZyWALL)	55
2.2.2 Interface to Interface (To/From ZyWALL)	55
2.2.3 Interface to Interface (From VPN Tunnel)	55
2.2.4 Interface to Interface (To VPN Tunnel)	55
2.3 Applications	55
2.3.1 VPN Connectivity	56
2.3.2 User-Aware Access Control	56
2.3.3 Multiple WAN Interfaces	57
2.3.4 Device HA	57

Chapter 3	
Web Configurator	59
3.1 Web Configurator Requirements	59
3.2 Web Configurator Access	59
3.3 Web Configurator Main Screen	61
3.3.1 Title Bar	61
3.3.2 Navigation Panel	62
3.3.3 Main Window	64
3.3.4 Status Bar	65
Chapter 4	
Wizard Setup	67
4.1 Wizard Setup Overview	67
4.2 Installation Setup, One ISP	68
4.3 Step 1 Internet Access	69
4.3.1 Ethernet: Auto IP Address Assignment	70
4.3.2 Ethernet: Static IP Address Assignment	70
4.3.3 Step 2 Internet Access Ethernet	72
4.3.4 PPPoE: Auto IP Address Assignment	73
4.3.5 PPPoE: Static IP Address Assignment	74
4.3.6 Step 2 Internet Access PPPoE	76
4.3.6.1 ISP Parameters	76
4.3.6.2 WAN IP Address Assignments	76
4.3.7 PPTP: Auto IP Address Assignment	77
4.3.8 PPTP: Static IP Address Assignment	80
4.3.9 Step 2 Internet Access PPTP	81
4.3.9.1 ISP Parameters	81
4.3.9.2 PPTP Configuration	82
4.3.9.3 WAN IP Address Assignments	82
4.3.10 Step 4 Internet Access - Finish	83
4.4 Device Registration	83
4.5 Installation Setup, Two Internet Service Providers	86
4.5.1 Internet Access Wizard Setup Complete	88
4.6 VPN Setup	88
4.7 VPN Wizards	89
4.7.1 VPN Express Wizard	90
4.8 VPN Express Wizard - Remote Gateway	91
4.8.1 VPN Express Wizard - Policy Setting	92
4.8.2 VPN Express Wizard - Summary	93
4.8.3 VPN Express Wizard - Finish	94
4.8.4 VPN Advanced Wizard	95
4.8.5 VPN Advanced Wizard - Remote Gateway	96
4.8.5.1 Phase 1 Setting	96

4.8.6 VPN Advanced Wizard - Phase 1	98
4.8.6.1 Phase 2 Setting	99
4.8.7 VPN Advanced Wizard - Phase 2	100
4.8.8 VPN Advanced Wizard - Summary	102
4.8.9 VPN Advanced Wizard - Finish	102

Chapter 5

Configuration Basics 105

5.1 Granular Configuration	105
5.2 Terminology in the ZyWALL	106
5.3 Physical Ports, Interfaces, and Zones	107
5.3.1 Network Topology Example	108
5.4 Feature Configuration Overview	108
5.5 Objects	116
5.6 System Management	117

Chapter 6

Tutorials 119

6.1 Interfaces and Zones	119
6.1.1 Set up Port Grouping	120
6.1.2 Set up Ethernet Interfaces	121
6.1.3 WAN Trunk	124
6.1.4 Zones	128
6.2 VPN	131
6.2.1 Set up the Ethernet Interfaces	131
6.2.2 Set up the Zones for the Ethernet Interfaces	133
6.2.3 Set up the VPN Gateway	133
6.2.4 Set up the VPN Connection	133
6.2.5 Set up the Policy Route for the VPN Tunnel	134
6.2.6 Set up the Zone for the VPN Tunnel	135
6.3 Device HA	136
6.3.1 Set up the Ethernet Interfaces on the Master	137
6.3.2 Set up DNS for the Virtual Router	138
6.3.3 Set up the VRRP Groups on the Master	138
6.3.4 Set up the Password for Synchronization	139
6.3.5 Finish Configuring the Master	139
6.3.6 Set up the Ethernet Interfaces on the Backup	140
6.3.7 Set up the VRRP Groups on the Backup	140
6.3.8 Synchronize the Backup	140
6.4 User-Aware Access Control	141
6.4.1 Set up User Accounts	142
6.4.2 Set up User Groups	142
6.4.3 Set up User Authentication Using the RADIUS Server	143

6.4.4 Set up Web Surfing Policies	144
6.4.5 Set up Bandwidth Restrictions	145
6.4.6 Set up MSN Policies	146
6.4.7 Set up LAN-to-DMZ Policies	147
6.5 Trunks	148
6.5.1 Set up Available Bandwidth on Ethernet Interfaces	149
6.5.2 Change WAN Trunk Algorithm	149
6.6 NAT 1:1 Example	150
6.6.1 Address Objects	150
6.6.2 Interface	151
6.6.3 Policy Route	152
6.6.4 Firewall Rule	152
Chapter 7	
Status	155
7.1 Status Screen	155
7.2 VPN Status	160
7.3 DHCP Table	161
7.4 Statistics	161
Chapter 8	
Registration	163
8.1 myZyXEL.com overview	163
8.1.1 Subscription Services Available on the ZyWALL	163
8.2 Registration	164
8.3 Service	165
Chapter 9	
File Manager	167
9.1 Configuration Files and Shell Scripts Overview	167
9.1.1 Comments in Configuration Files or Shell Scripts	168
9.1.2 Errors in Configuration Files or Shell Scripts	169
9.1.3 ZyWALL Configuration File Details	169
9.1.4 Configuration File Flow at Restart	169
9.2 Configuration File Screen	170
9.3 Firmware Package Screen	172
9.4 Shell Script Screen	174
Chapter 10	
Interface	177
10.1 Interface Overview	177
10.1.1 Types of Interfaces	177
10.1.2 IP Address Assignment	178

10.1.3 Interface Parameters	180
10.1.4 DHCP Settings	180
10.1.5 Ping Check Settings	182
10.1.6 Relationships Between Interfaces	182
10.2 Ethernet Interfaces	183
10.2.1 Ethernet Interfaces Overview	183
10.2.2 Ethernet Summary Screen	184
10.2.3 Ethernet Edit	185
10.3 Port Grouping	190
10.3.1 Port Grouping Overview	190
10.3.2 Port Grouping Screen	192
10.4 VLAN Interfaces	192
10.4.1 VLAN Overview	193
10.4.2 VLAN Interfaces Overview	194
10.4.3 VLAN Summary Screen	194
10.4.4 VLAN Add/Edit	195
10.5 Bridge Interfaces	199
10.5.1 Bridge Overview	200
10.5.2 Bridge Interface Overview	201
10.5.3 Bridge Summary	201
10.5.4 Bridge Add/Edit	202
10.6 PPPoE/PPTP Interfaces	206
10.6.1 PPPoE/PPTP Overview	207
10.6.2 PPPoE/PPTP Interfaces Overview	207
10.6.3 PPPoE/PPTP Interface Summary	208
10.6.4 PPPoE/PPTP Interface Add/Edit	209
10.7 Auxiliary Interface	211
10.7.1 Auxiliary Interface Overview	211
10.7.2 Auxiliary	211
10.8 Virtual Interfaces	213
10.8.1 Virtual Interfaces Add/Edit	213
Chapter 11	
Trunks	215
11.1 Trunks Overview	215
11.2 Trunk Scenario Examples	215
11.3 Load Balancing Introduction	215
11.4 Load Balancing Algorithms	216
11.4.1 Least Load First	216
11.4.1.1 Least Load First Example 1	216
11.4.2 Weighted Round Robin	217
11.4.3 Spillover	218
11.5 Trunk Summary	218

11.6 Configuring a Trunk	219
Chapter 12	
IPSec VPN	223
12.1 IPSec VPN Overview	223
12.1.1 IPSec SA Overview	224
12.1.1.1 Local Network and Remote Network	224
12.1.1.2 Active Protocol	224
12.1.1.3 Encapsulation	225
12.1.1.4 IPSec SA Proposal and Perfect Forward Secrecy	225
12.1.2 Additional Topics for IPSec SA	226
12.1.2.1 IPSec SA using Manual Keys	226
12.1.2.2 NAT for Inbound and Outbound Traffic	226
12.2 Related Configuration	228
12.3 VPN Connection Screens	229
12.3.1 VPN Connection Summary	229
12.3.2 VPN Connection Add/Edit IKE	230
12.3.3 VPN Connection Add/Edit Manual Key	234
12.4 VPN Gateway Screens	238
12.4.1 IKE SA Overview	238
12.4.1.1 IP Addresses of the ZyWALL and Remote IPSec router	239
12.4.1.2 IKE SA Proposal	239
12.4.1.3 Diffie-Hellman (DH) Key Exchange	240
12.4.1.4 Authentication	241
12.4.2 Additional Topics for IKE SA	242
12.4.2.1 Negotiation Mode	242
12.4.2.2 VPN, NAT, and NAT Traversal	243
12.4.2.3 Extended Authentication	243
12.4.2.4 Certificates	244
12.4.3 VPN Gateway Summary	244
12.4.4 VPN Gateway Add/Edit	245
12.5 VPN Concentrator	250
12.5.1 VPN Concentrator Summary	251
12.5.2 VPN Concentrator Add/Edit	252
12.6 SA Monitor Screen	254
Chapter 13	
Routing Protocol	255
13.1 Routing Protocol Overview	255
13.1.1 RIP Overview	255
13.1.2 Authentication Types	256
13.2 RIP Screen	256
13.3 OSPF Overview	258

13.3.1 OSPF Areas	258
13.3.2 OSPF Routers	259
13.3.3 Virtual Links	260
13.3.4 OSPF Configuration	261
13.4 OSPF Screens	261
13.4.1 OSPF Summary	261
13.4.2 OSPF Area Add/Edit	263
Chapter 14	
Zones	267
14.1 Zones Overview	267
14.1.1 Effect of Zones on Different Types of Traffic	267
14.2 Zone Summary	268
14.3 Zone Add/Edit	269
Chapter 15	
ISP Accounts	271
15.1 ISP Accounts Overview	271
15.2 ISP Account Summary	271
15.3 ISP Account Edit	272
Chapter 16	
Device HA	275
16.1 Virtual Router Redundancy Protocol (VRRP) Overview	275
16.1.1 Additional VRRP Notes	276
16.2 VRRP Group Overview	277
16.3 Device HA Screens	277
16.4 VRRP Group Summary	278
16.5 VRRP Group Add/Edit	279
16.6 Synchronization Overview	281
16.6.1 Synchronize Screen	282
Chapter 17	
DDNS	285
17.1 DDNS Overview	285
17.1.1 DYNDNS Wildcard	285
17.1.2 High Availability (HA)	285
17.1.3 Mail Exchanger	286
17.2 DDNS Screens	286
17.3 DDNS Summary	287
17.4 Dynamic DNS Add/Edit	288

Chapter 18	
Route	291
18.1 Policy Route	291
18.1.1 Benefits	291
18.2 Routing Policy	291
18.2.1 NAT and SNAT	292
18.2.2 Port Triggering	292
18.3 IP Routing Policy Setup	293
18.4 Policy Route Edit	294
18.4.1 Adding a New Service	297
18.5 IP Static Routes	298
18.6 Static Route Summary	299
18.7 Edit a Static Route	299
Chapter 19	
Firewall	301
19.1 Firewall Overview	301
19.2 Firewall Rules	302
19.2.1 Through-ZyWALL Rules	302
19.2.1.1 Global Through-ZyWALL Rules	303
19.2.2 To-ZyWALL Rules	303
19.2.3 Firewall and VPN Traffic	304
19.3 Firewall Rule Example Applications	304
19.4 Alerts	306
19.5 Asymmetrical Routes	306
19.5.1 Virtual Interfaces and Asymmetrical Routes	307
19.6 Configuring the Firewall	307
19.6.1 Through-ZyWALL Rules with Zone Pairs	307
19.6.2 Through Firewall Rules with All Rules	310
19.6.3 To-ZyWALL Rules	312
19.6.4 Edit a Firewall Rule	315
19.7 Firewall Rule Configuration Example	317
Chapter 20	
Application Patrol	321
20.1 Application Patrol Overview	321
20.1.1 Classification of Applications	321
20.1.2 Default Action for Each Application	321
20.1.3 Exceptions to the Default Action	322
20.1.4 Bandwidth Management for Applications	322
20.1.5 Other Applications	322
20.2 Application Patrol Screens	322
20.3 Configuration Summary	323

20.3.1 Configuration Edit	325
20.4 Other Protocol Screen	328
20.4.1 Other Configuration Add/Edit	330
Chapter 21	
IDP	333
21.1 Introduction to IDP	333
21.1.1 Host Intrusions	333
21.1.2 Network Intrusions	333
21.1.3 IDP on the ZyWALL	334
21.2 Protected Zones and Profiles	334
21.3 Configuring IDP General	334
21.4 Introducing IDP Profiles	336
21.4.1 Base Profiles	336
21.5 Profile Summary Screen	337
21.6 Creating New Profiles	338
21.6.1 Procedure To Create a New Profile	338
21.7 Profiles: Packet Inspection	339
21.7.1 Policy Types	339
21.7.2 IDP Service Groups	340
21.7.3 Profile > Packet Inspection > Group View Screen	341
21.7.4 Profile > Packet Inspection > Query View Screen	344
21.7.5 Query Example	346
21.8 Profiles: Traffic Anomaly	348
21.8.1 Port Scanning	348
21.8.1.1 Decoy Port Scans	348
21.8.1.2 Distributed Port Scans	348
21.8.1.3 Port Sweeps	349
21.8.1.4 Filtered Port Scans	349
21.8.2 Flood Detection	349
21.8.2.1 ICMP Flood Attack	349
21.8.2.2 Smurf	350
21.8.2.3 TCP SYN Flood Attack	350
21.8.2.4 LAND Attack	351
21.8.2.5 UDP Flood Attack	351
21.8.3 Profile > Traffic Anomaly Screen	352
21.9 Profiles: Protocol Anomaly	353
21.9.1 HTTP Inspection and TCP/UDP/ICMP Decoders	354
21.9.2 Protocol Anomaly Configuration	356
21.10 Introducing IDP Custom Signatures	358
21.10.1 IP Packet Header	358
21.11 Configuring Custom Signatures	360
21.11.1 Creating or Editing a Custom Signature	362

21.11.2 Custom Signature Example	366
21.11.2.1 Understand the Vulnerability	367
21.11.2.2 Analyze Packets	367
21.11.3 Applying Custom Signatures	370
21.11.4 Verifying Custom Signatures	370
21.11.5 Snort Signatures	371
21.12 Updating IDP Signatures	372
Chapter 22	
Content Filtering Screens	375
22.1 Content Filtering Overview	375
22.1.1 Content Filtering Policies	375
22.1.2 Content Filtering Profiles	375
22.1.2.1 Category-based Blocking	375
22.1.2.2 Restrict Web Features	375
22.1.2.3 Customize Web Site Access	376
22.1.3 Content Filtering Configuration Guidelines	376
22.2 Content Filter General Screen	376
22.3 Content Filter Policy Screen	379
22.4 Content Filtering Profile Screen	380
22.5 External Web Filtering Service	381
22.6 Content Filter Categories Screen	382
22.7 Content Filter Customization Screen	388
22.8 Keyword Blocking URL Checking	391
22.9 Content Filter Cache Screen	391
Chapter 23	
Content Filtering Reports	395
23.1 Viewing Content Filtering Reports	395
23.2 Web Site Submission	400
Chapter 24	
Virtual Servers	403
24.1 Virtual Server Overview	403
24.2 Virtual Server Example	404
24.3 Virtual Server Screens	404
24.4 Virtual Server Summary Screen	404
24.4.1 Virtual Server Add/Edit	405
Chapter 25	
HTTP Redirect	409
25.1 HTTP Redirect Overview	409
25.1.1 Web Proxy Server	409

25.2 HTTP Redirect, Firewall and Policy Route	409
25.3 Configuring HTTP Redirect	410
25.4 HTTP Redirect Edit	411

Chapter 26

VoIP Pass Through..... 413

26.1 VoIP Pass Through and the ZyWALL	413
26.1.1 Application Layer Gateway (ALG) and NAT	413
26.1.2 ALG and Trunks	413
26.1.3 H.323	414
26.1.4 RTP	414
26.1.4.1 H.323 ALG Details	414
26.1.5 SIP	415
26.1.5.1 SIP ALG Details	415
26.1.5.2 SIP Signaling Session Timeout	416
26.2 Peer-to-Peer Calls and the ZyWALL	416
26.2.1 VoIP Calls from the WAN with Multiple Outgoing Calls	416
26.2.2 VoIP with Multiple WAN IP Addresses	417
26.3 VoIP PassThru Screen	417
26.4 WAN to LAN SIP Peer-to-peer Calls Example	419

Chapter 27

User/Group 423

27.1 User Account Overview	423
27.1.1 User Types	423
27.1.2 Ext-User Accounts	423
27.1.2.1 Setting up User Attributes in an External Server	424
27.1.2.2 Creating a Large Number of Ext-User Accounts	425
27.1.3 User Groups	425
27.1.4 Access Users and the ZyWALL	425
27.1.5 Force User Authentication Policy	425
27.2 User Summary	426
27.2.1 User Add/Edit	426
27.2.1.1 Rules for User Names	428
27.3 Group Summary	428
27.3.1 Group Add/Edit	429
27.4 Setting Screen	431
27.4.1 Force User Authentication Policy Add/Edit	433
27.5 Web Configurator for Non-Admin Users	434

Chapter 28

Addresses 437

28.1 Address Overview	437
-----------------------------	-----

28.2 Address Screens	437
28.2.1 Address Summary	437
28.2.2 Address Add/Edit	438
28.3 Address Group Screens	439
28.3.1 Address Group Summary	439
28.3.2 Address Group Add/Edit	440
Chapter 29	
Services	443
29.1 Services Overview	443
29.1.1 IP Protocols	443
29.1.2 Service Objects and Service Groups	444
29.2 Service Summary Screen	444
29.2.1 Service Add/Edit	445
29.3 Service Group Summary Screen	446
29.3.1 Service Group Add/Edit	446
Chapter 30	
Schedules	449
30.1 Schedule Overview	449
30.2 Schedule Screens	449
30.2.1 Schedule Summary	449
30.2.2 One-Time Schedule Add/Edit	451
30.2.3 Recurring Schedule Add/Edit	452
Chapter 31	
AAA Server	455
31.1 AAA Server Overview	455
31.2 LDAP	455
31.2.1 LDAP Directory Structure	456
31.2.2 Distinguished Name (DN)	457
31.2.2.1 Base DN	457
31.2.2.2 Bind DN	457
31.2.3 Configuring LDAP Default	457
31.3 LDAP Group Summary	458
31.3.1 Creating an LDAP Group	460
31.4 RADIUS Server	461
31.5 Configuring a Default RADIUS Server	461
31.6 Configuring a Group of RADIUS Servers	462
31.6.1 Adding a RADIUS Server Member	464

Chapter 32	
Authentication Objects	465
32.1 Authentication Objects Overview	465
32.2 Viewing Authentication Objects	465
32.3 Creating an Authentication Object	466
32.3.1 Example: Selecting a VPN Authentication Method	467
Chapter 33	
Certificates	469
33.1 Certificates Overview	469
33.1.1 Advantages of Certificates	470
33.2 Self-signed Certificates	470
33.3 Factory Default Certificate	470
33.3.1 Certificate File Formats	470
33.4 Certificate Configuration Screens Summary	471
33.5 Verifying a Certificate	471
33.5.1 Checking the Fingerprint of a Certificate on Your Computer	471
33.6 My Certificates Screen	472
33.6.1 My Certificates Add Screen	474
33.6.2 My Certificate Edit Screen	477
33.6.3 My Certificate Import Screen	480
33.7 Trusted Certificates Screen	481
33.7.1 OCSP	482
33.8 Trusted Certificates Edit Screen	483
33.9 Trusted Certificates Import Screen	487
Chapter 34	
System	489
34.1 System Overview	489
34.2 Host Name	489
34.3 Time and Date	490
34.3.1 Pre-defined NTP Time Servers List	492
34.3.2 Updating the Time	492
34.3.3 Time Server Synchronization	492
34.4 Console Port Speed	494
34.5 DNS Overview	494
34.5.1 DNS Server Address Assignment	494
34.5.2 DNS Servers	495
34.5.3 Configuring DNS	495
34.5.4 Address Record	497
34.5.5 PTR Record	498
34.5.6 Adding an Address/PTR Record	498
34.5.7 Domain Zone Forwarder	498

34.5.8 Adding a Domain Zone Forwarder	499
34.5.9 MX Record	499
34.5.10 Adding a MX Record	500
34.5.11 DNS Service Control	500
Chapter 35	
System Remote Management	503
35.1 Remote Management Overview	503
35.1.1 Remote Management Limitations	503
35.1.2 System Timeout	504
35.2 Introduction to HTTPS	504
35.3 Configuring WWW	505
35.4 Service Control Rules	508
35.5 HTTPS Example	509
35.5.1 Internet Explorer Warning Messages	509
35.5.2 Netscape Navigator Warning Messages	510
35.5.3 Avoiding Browser Warning Messages	511
35.5.4 Login Screen	511
35.6 SSH	513
35.6.1 How SSH Works	513
35.6.2 SSH Implementation on the ZyWALL	514
35.6.3 Requirements for Using SSH	514
35.6.4 Configuring SSH	514
35.7 Secure Telnet Using SSH Examples	515
35.7.1 Example 1: Microsoft Windows	516
35.7.2 Example 2: Linux	516
35.8 Telnet	517
35.8.1 Configuring Telnet	517
35.9 Configuring FTP	519
35.10 SNMP	520
35.10.1 Supported MIBs	522
35.10.2 SNMP Traps	522
35.10.3 Configuring SNMP	522
Chapter 36	
Logs.....	525
36.1 View Log Screen	525
36.2 Log Settings Screens	527
36.3 Log Settings Summary	528
36.3.1 Log Settings Edit E-mail	529
36.3.2 Log Settings Edit syslog	532
36.3.3 Active Log Summary	534

Chapter 37	
Reports	537
37.1 Report Screen	537
37.2 Session Screen	540
Chapter 38	
Reboot	543
Appendix A	
Product Specifications	545
Appendix B	
Common Services	547
Appendix C	
Open Software Announcements	551
Index	581

List of Figures

Figure 1 Front Panel Ports	47
Figure 2 Front Panel	48
Figure 3 Managing the ZyWALL: Web Configurator	49
Figure 4 Managing the ZyWALL: Command-Line Interface	49
Figure 5 Applications: VPN Connectivity	56
Figure 6 Applications: User-Aware Access Control	57
Figure 7 Applications: Multiple WAN Interfaces	57
Figure 8 Applications: Device HA	58
Figure 9 Login Screen	60
Figure 10 Update Admin Info Screen	60
Figure 11 Main Screen	61
Figure 12 Message Bar	65
Figure 13 CLI Messages	65
Figure 14 Wizard Setup Welcome	68
Figure 15 Internet Access: Step 1	69
Figure 16 Ethernet Encapsulation: Auto: Finish	70
Figure 17 Ethernet Encapsulation: Static	71
Figure 18 Ethernet Encapsulation: Static: Finish	72
Figure 19 PPPoE Encapsulation: Auto	73
Figure 20 PPPoE Encapsulation: Auto: Finish	74
Figure 21 PPPoE Encapsulation: Static	75
Figure 22 PPPoE Encapsulation: Static: Finish	77
Figure 23 PPTP Encapsulation: Auto	78
Figure 24 PPTP Encapsulation: Auto: Finish	79
Figure 25 PPTP Encapsulation: Static	80
Figure 26 PPTP Encapsulation: Static: Finish	83
Figure 27 Registration	84
Figure 28 Registration: Registered Device	85
Figure 29 Internet Access: Step 1: First WAN Interface	86
Figure 30 Internet Access: Step 3: Second WAN Interface	87
Figure 31 Internet Access: Finish	88
Figure 32 VPN Wizard: Wizard Type	89
Figure 33 VPN Express Wizard: Step 2	90
Figure 34 VPN Express Wizard: Step 3	91
Figure 35 VPN Express Wizard: Step 4	93
Figure 36 VPN Express Wizard: Step 6	94
Figure 37 VPN Advanced Wizard: Step 2	95
Figure 38 VPN Advanced Wizard: Step 3	97

Figure 39 VPN Advanced Wizard: Step 4	99
Figure 40 VPN Advanced Wizard: Step 5	101
Figure 41 VPN Wizard: Step 6: Advanced	103
Figure 42 Interfaces and Zones: Example	108
Figure 43 Status > Interface Status Summary, Initial	120
Figure 44 Network > Interface > Port Grouping, Initial	120
Figure 45 Network > Interface > Port Grouping, Drag-and-Drop	121
Figure 46 Status > Interface Status Summary, After Port Grouping	121
Figure 47 Network > Interface > Ethernet, Initial	122
Figure 48 Network > Interface > Ethernet > ge3	122
Figure 49 Network > Interface > Ethernet > ge5 > IP Address Assignment	123
Figure 50 Network > Interface > Ethernet > ge5 > DHCP Setting	123
Figure 51 Status > Interface Status Summary, After Ethernet Interfaces	124
Figure 52 Network > Interface > Trunk, Initial	124
Figure 53 Network > Interface > Trunk > add, Initial	125
Figure 54 Network > Interface > Trunk > add, Add Member	125
Figure 55 Network > Interface > Trunk > add, Edit Member	125
Figure 56 Network > Interface > Trunk > add, Member ge3	126
Figure 57 Network > Interface > Trunk > add, Final	126
Figure 58 Network > Interface > Trunk, Final	126
Figure 59 Policy > Route > Policy Route	127
Figure 60 Status > Interface Status Summary, After Trunks	128
Figure 61 Network > Zone, Initial	128
Figure 62 Network > Zone > DMZ, Initial	129
Figure 63 Network > Zone > DMZ, Final	129
Figure 64 Network > Zone > WAN, Initial	129
Figure 65 Network > Zone > WAN, Edit Member	130
Figure 66 Network > Zone > WAN, Final	130
Figure 67 Status > Interface Status Summary, After Zones	131
Figure 68 VPN Example	131
Figure 69 Network > Interface > Ethernet > ge3 > IP Address	132
Figure 70 Network > Interface > Ethernet > ge1 > IP Address	132
Figure 71 Network > Interface > Ethernet > ge1 > DHCP Settings	132
Figure 72 Network > IPSec VPN > VPN Gateway > add	133
Figure 73 Object > Address > Address > add	134
Figure 74 Network > IPSec VPN > VPN Connection > add	134
Figure 75 Policy > Route > Policy Route	135
Figure 76 Policy > Route > Policy Route > add	135
Figure 77 Network > Zone > add	136
Figure 78 Device HA Example	136
Figure 79 Network > Interface > Ethernet > ge1 > IP Address	137
Figure 80 Network > Interface > Ethernet > ge1 > DHCP Settings	137
Figure 81 Network > Device HA > VRRP Group > add	138

Figure 82 Status > Interface Status Summary	139
Figure 83 Network > Device HA > VRRP Group > add	139
Figure 84 Network > Device HA > Synchronize	139
Figure 85 Network > Device HA > VRRP Group > add	140
Figure 86 Status > Interface Status Summary	140
Figure 87 Network > Device HA > Synchronize	141
Figure 88 User/Group > User > add	142
Figure 89 User/Group > Group > add	143
Figure 90 Object > AAA Server > RADIUS > Default	143
Figure 91 Object > AAA Server > RADIUS > Default	144
Figure 92 System > WWW > Authentication	144
Figure 93 User/Group > Setting > Add (Force User Authentication Policy)	144
Figure 94 Policy > App Patrol > http > edit	145
Figure 95 Policy > Route > Policy Route	146
Figure 96 Policy > Route > Policy Route > add	146
Figure 97 Object > Schedule > Recurring > add	147
Figure 98 Policy > Firewall > LAN > DMZ > edit	148
Figure 99 Policy > Firewall > LAN > DMZ > add	148
Figure 100 Trunk Example	149
Figure 101 Network > Interface > Ethernet > edit > ge2	149
Figure 102 Network > Interface > Trunk > WAN_TRUNK > edit	150
Figure 103 1-1 NAT Example Network Topology	150
Figure 104 Create Address Objects	151
Figure 105 Address Objects	151
Figure 106 Create a WAN Virtual Interface	151
Figure 107 Virtual WAN Interface	152
Figure 108 Create a Policy Route	152
Figure 109 Status	156
Figure 110 Status > VPN Status	160
Figure 111 Status > DHCP Table	161
Figure 112 Status > Statistics	162
Figure 113 Registration	164
Figure 114 Registration: Registered Device	165
Figure 115 Registration: Service	166
Figure 116 Configuration File / Shell Script: Example	167
Figure 117 File Manager > Configuration File	170
Figure 118 File Manager > Configuration File > Copy	171
Figure 119 File Manager > Configuration File > Rename	171
Figure 120 File Manager > Firmware Package	173
Figure 121 Firmware Upload In Process	173
Figure 122 Network Temporarily Disconnected	174
Figure 123 Firmware Upload Error	174
Figure 124 File Manager > Shell Script	174

Figure 125 File Manager > Shell Script > Copy	175
Figure 126 File Manager > Shell Script > Rename	175
Figure 127 Example: Entry in the Routing Table Derived from Interfaces	179
Figure 128 Network > Interface > Ethernet	184
Figure 129 Network > Interface > Ethernet > Edit	186
Figure 130 Network > Interface > Edit > Add Static DHCP	190
Figure 131 Port Grouping Example: Network	191
Figure 132 Port Grouping Example: Screen	191
Figure 133 Network > Interface > Port Grouping	192
Figure 134 Example: Before VLAN	193
Figure 135 Example: After VLAN	193
Figure 136 Network > Interface > VLAN	195
Figure 137 Network > Interface > VLAN > Edit	196
Figure 138 Network > Interface > Edit > Add Static DHCP	199
Figure 139 Network > Interface > Bridge	202
Figure 140 Network > Interface > Bridge > Edit	203
Figure 141 Network > Interface > Edit > Add Static DHCP	206
Figure 142 Example: PPPoE/PPTP Interfaces	207
Figure 143 Network > Interface > PPPoE/PPTP	208
Figure 144 Network > Interface > PPPoE/PPTP > Edit	209
Figure 145 Network > Interface > Auxiliary	212
Figure 146 Network > Interface > Edit	214
Figure 147 Least Load First Example 1	216
Figure 148 Weighted Round Robin Algorithm Example	217
Figure 149 Spillover Algorithm Example	218
Figure 150 Network > Interface > Trunk	218
Figure 151 Network > Interface > Trunk > Members	219
Figure 152 Network > Interface > Trunk > Members Select	220
Figure 153 VPN: Example	223
Figure 154 VPN: IKE SA and IPSec SA	224
Figure 155 VPN: Transport and Tunnel Mode Encapsulation	225
Figure 156 VPN Example: NAT for Inbound and Outbound Traffic	227
Figure 157 Network > IPSec VPN > VPN Connection	230
Figure 158 Network > IPSec VPN > VPN Connection > Edit (IKE)	231
Figure 159 Network > IPSec VPN > VPN Connection > Manual Key > Edit	235
Figure 160 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal	239
Figure 161 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange	240
Figure 162 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication	241
Figure 163 VPN/NAT Example	243
Figure 164 Network > IPSec VPN > VPN Gateway	245
Figure 165 Network > IPSec VPN > VPN Gateway > Edit	246
Figure 166 VPN Topologies	251
Figure 167 Network > IPSec VPN > Concentrator	252

Figure 168 Network > IPSec VPN > Concentrator > Edit	253
Figure 169 Network > IPSec VPN > Concentrator > Edit > Member	253
Figure 170 Network > IPSec VPN > SA Monitor	254
Figure 171 Network > Routing Protocol > RIP	257
Figure 172 OSPF: Types of Areas	259
Figure 173 OSPF: Types of Routers	260
Figure 174 OSPF: Virtual Link	261
Figure 175 Network > Routing Protocol > OSPF	262
Figure 176 Network > Routing Protocol > OSPF > Edit	264
Figure 177 Example: Zones	267
Figure 178 Network > Zone	268
Figure 179 Configuration > Network > Zone > Edit	269
Figure 180 Network > ISP Account	271
Figure 181 Network > ISP Account > Edit	272
Figure 182 Example: VRRP, Normal Operation	275
Figure 183 Example: VRRP, Master Becomes Unavailable	276
Figure 184 Example: VRRP, No Preempt	276
Figure 185 Network > Device HA > VRRP Group	278
Figure 186 Network > Device HA > VRRP Group > Edit	280
Figure 187 Network > Device HA > Synchronize	283
Figure 188 Network > DDNS	287
Figure 189 Network > DDNS > Edit	288
Figure 190 Trigger Port Forwarding Example	293
Figure 191 Policy Route	293
Figure 192 Policy Route Edit	295
Figure 193 Policy Route Edit: Service	297
Figure 194 Example of Static Routing Topology	298
Figure 195 IP Static Route	299
Figure 196 IP Static Route Edit	300
Figure 197 Default Firewall Action	301
Figure 198 Blocking All LAN to WAN IRC Traffic Example	304
Figure 199 Limited LAN to WAN IRC Traffic Example	305
Figure 200 Triangle Route: Using Virtual Interfaces	307
Figure 201 Firewall: Zone Pairs	308
Figure 202 Firewall: All Rules	310
Figure 203 Firewall: To-ZyWALL Rules	313
Figure 204 Firewall Rule Edit	315
Figure 205 Firewall Example: Object > Service	317
Figure 206 Firewall Example: Create a Service Object	317
Figure 207 Firewall Example: Object > Address	318
Figure 208 Firewall Example: Create an Address Object	318
Figure 209 Firewall Example: Select the Traveling Direction of Traffic	319
Figure 210 Firewall Example: Edit a Firewall Rule	319

Figure 211 Firewall Example: MyService Example Rule Summary	320
Figure 212 Policy > Application Patrol > Configuration	324
Figure 213 Policy > Application Patrol > Configuration > Edit	326
Figure 214 Policy > Application Patrol > Other Protocol	329
Figure 215 Policy > Application Patrol > Other Protocol > Edit	330
Figure 216 Enable IDP Warning	334
Figure 217 IDP > General	335
Figure 218 Base Profiles	336
Figure 219 Policy > IDP > Profile	338
Figure 220 IDP Service Groups	341
Figure 221 Policy > IDP > Profile > Packet Inspection_Group View	342
Figure 222 Policy > IDP > Profile > Packet Inspection_Query View	345
Figure 223 Query Example Search Criteria	347
Figure 224 Query Example Search Results	347
Figure 225 Smurf Attack	350
Figure 226 TCP Three-Way Handshake	350
Figure 227 SYN Flood	351
Figure 228 Profiles: Traffic Anomaly	352
Figure 229 Profiles: Protocol Anomaly	357
Figure 230 IP v4 Packet Headers	359
Figure 231 Policy > IDP > Custom Signatures	361
Figure 232 Policy > IDP > Custom Signatures > Add/Edit	363
Figure 233 Custom Signature Example Pattern 1	367
Figure 234 Custom Signature Example Pattern 2	368
Figure 235 Custom Signature Example Patterns 3 and 4	368
Figure 236 Example Custom Signature	369
Figure 237 Example: Custom Signature in IDP Profile	370
Figure 238 Custom Signature Log	371
Figure 239 IDP Update	373
Figure 240 Downloading IDP Signatures	374
Figure 241 Successful IDP Signature Download	374
Figure 242 Configuration > Policy > Content Filter > General	377
Figure 243 Configuration > Policy > Content Filter > General > Add I	380
Figure 244 Configuration > Policy > Content Filter > Filtering Profile	381
Figure 245 Content Filtering Lookup Procedure	381
Figure 246 Configuration > Policy > Content Filtering > Filtering Profile > Add	383
Figure 247 Configuration > Policy > Content Filtering > Filtering Profiles > Customization	389
Figure 248 Configuration > Policy > Content Filter > Cache	392
Figure 249 myZyXEL.com: Login	395
Figure 250 myZyXEL.com: Welcome	396
Figure 251 myZyXEL.com: Service Management	397
Figure 252 Blue Coat: Login	397
Figure 253 Blue Coat Content Filtering Reports Main Screen	398

Figure 254 Blue Coat: Report Home	398
Figure 255 Global Report Screen Example	399
Figure 256 Requested URLs Example	400
Figure 257 Web Page Review Process Screen	401
Figure 258 Multiple Servers Behind NAT Example	404
Figure 259 Policy > Virtual Server	405
Figure 260 Policy > Virtual Server > Edit	406
Figure 261 HTTP Redirect Example	410
Figure 262 HTTP Redirect	411
Figure 263 HTTP Redirect Edit	412
Figure 264 H.323 ALG Example	415
Figure 265 SIP ALG Example	416
Figure 266 VoIP Calls from the WAN with Multiple Outgoing Calls	417
Figure 267 VoIP with Multiple WAN IP Addresses	417
Figure 268 Policy > VoIP Passthru	418
Figure 269 WAN to LAN H.323 Peer-to-peer Calls Example	419
Figure 270 Policy > Virtual Server > Add	419
Figure 271 Object > Address > Add	420
Figure 272 Policy > Firewall > WAN to LAN	420
Figure 273 Policy > Firewall > WAN > LAN > Add	421
Figure 274 LDAP Example: Keywords for User Attributes	424
Figure 275 RADIUS Example: Keywords for User Attributes	425
Figure 276 User/Group	426
Figure 277 User/Group > User > Edit	427
Figure 278 User/Group > Group	429
Figure 279 User/Group > Group > Edit	430
Figure 280 User/Group > Group > Edit > Member	430
Figure 281 User/Group > Setting	431
Figure 282 User/Group > Setting > Force User Authentication Policy > add/edit	434
Figure 283 Web Configurator for Non-Admin Users	435
Figure 284 Object > Address > Address	438
Figure 285 Object > Address > Address > Edit	439
Figure 286 Object > Address > Address Group	440
Figure 287 Objects > Address > Address Group > Edit	441
Figure 288 Object > Address > Address Group > Member	441
Figure 289 Object > Service > Service	444
Figure 290 Object > Service > Service > Edit	445
Figure 291 Object > Service > Service Group	446
Figure 292 Object > Service > Service Group > Edit	447
Figure 293 Object > Service > Service Group > Member	448
Figure 294 Configuration > Object > Schedule	450
Figure 295 Configuration > Object > Schedule > One Time_1	451
Figure 296 Configuration > Object > Schedule > Recurring_1	452

Figure 297 Example: LDAP Client and Server	456
Figure 298 Basic LDAP Directory Structure	457
Figure 299 Objects: AAA Server: LDAP: Default	458
Figure 300 Objects > AAA Server > LDAP > Group	459
Figure 301 Objects > AAA Server > LDAP > Group > Add	460
Figure 302 RADIUS Server Network Example	461
Figure 303 Objects > AAA Server > RADIUS > Default	462
Figure 304 Objects > AAA Server > RADIUS > Group	463
Figure 305 Objects > AAA Server > RADIUS > Group > Add	464
Figure 306 Objects: Auth. Method	465
Figure 307 Objects > Auth. Method > Add	467
Figure 308 Example: Using Authentication Method in VPN	468
Figure 309 Remote Host Certificates	471
Figure 310 Certificate Details	472
Figure 311 My Certificates Screen	473
Figure 312 My Certificates Add Screen	475
Figure 313 My Certificate Edit Screen	478
Figure 314 My Certificate Import Screen	481
Figure 315 Trusted Certificates Screen	482
Figure 316 Trusted Certificates Edit Screen	484
Figure 317 Trusted Certificates Import Screen	487
Figure 318 System > Host Name	489
Figure 319 System > Date and Time	490
Figure 320 Synchronization in Process	493
Figure 321 System > Console Port Speed	494
Figure 322 System > DNS	495
Figure 323 System > DNS > Address/PTR Record Edit	498
Figure 324 System > DNS > Domain Zone Forwarder Edit	499
Figure 325 System > DNS > MX Record Edit	500
Figure 326 System > DNS > Service Control Rule Edit	500
Figure 327 HTTP/HTTPS Implementation	505
Figure 328 System > WWW	506
Figure 329 System > Service Control Rule Edit	508
Figure 330 Security Alert Dialog Box (Internet Explorer)	510
Figure 331 Security Certificate 1 (Netscape)	510
Figure 332 Security Certificate 2 (Netscape)	511
Figure 333 Login Screen (Internet Explorer)	512
Figure 334 Login Screen (Netscape)	512
Figure 335 SSH Communication Example	513
Figure 336 How SSH v1 Works Example	513
Figure 337 System > SSH	514
Figure 338 SSH Example 1: Store Host Key	516
Figure 339 SSH Example 2: Test	516

Figure 340 SSH Example 2: Log in	517
Figure 341 Telnet Configuration on a TCP/IP Network	517
Figure 342 System > Telnet	518
Figure 343 System > FTP	519
Figure 344 SNMP Management Model	521
Figure 345 System > SNMP	522
Figure 346 Maintenance > Logs > View Log	526
Figure 347 Maintenance > Logs > Log Setting	529
Figure 348 Maintenance > Logs > Log Setting > E-mail > Edit	530
Figure 349 Maintenance > Logs > Log Setting > Remote Server > Edit	533
Figure 350 Active Log Summary	535
Figure 351 Maintenance > Report > Report	538
Figure 352 Maintenance > Report > Session	541
Figure 353 Maintenance > Reboot	543

List of Tables

Table 1 Front Panel LEDs	48
Table 2 Managing the ZyWALL: Console Port	49
Table 3 Starting and Stopping the ZyWALL	50
Table 4 Packet Flow Key	54
Table 5 Title Bar: Web Configurator Icons	61
Table 6 Navigation Panel Summary (Except for Configuration Menu)	62
Table 7 Navigation Panel Summary (Configuration Menu Only)	62
Table 8 Internet Access: Step 1	69
Table 9 Ethernet Encapsulation: Static	71
Table 10 PPPoE Encapsulation: Auto	73
Table 11 PPPoE Encapsulation: Static	75
Table 12 PPTP Encapsulation: Auto	78
Table 13 PPTP Encapsulation: Static	80
Table 14 Registration	84
Table 15 VPN Wizard: Step 1: Wizard Type	89
Table 16 VPN Express Wizard: Step 2	90
Table 17 VPN Express Wizard: Step 3	92
Table 18 VPN Express Wizard: Step 4	93
Table 19 VPN Advanced Wizard: Step 2	95
Table 20 VPN Advanced Wizard: Step 3	97
Table 21 VPN Advanced Wizard: Step 4	99
Table 22 VPN Advanced Wizard: Step 5	101
Table 23 ZyWALL Terminology That is Different Than ZyNOS	106
Table 24 ZyWALL Terminology That Might Be Different Than Other Products	106
Table 25 NAT: Differences Between the ZyWALL and ZyNOS	106
Table 26 Bandwidth Management: Differences Between the ZyWALL and ZyNOS	106
Table 27 Physical Ports, Interfaces, and Zones	107
Table 28 Interfaces and Zones Example	119
Table 29 Ethernet Interfaces Example	121
Table 30 Trunk Example	124
Table 31 Zones Example	128
Table 32 User-Aware Access Control Example	141
Table 33 Status	156
Table 34 Status > VPN Status	160
Table 35 Status > DHCP Table	161
Table 36 Status > Statistics	162
Table 37 Registration	164
Table 38 Service	166

Table 39 Configuration Files and Shell Scripts in the ZyWALL	168
Table 40 File Manager > Configuration File	171
Table 41 File Manager > Firmware Package	173
Table 42 File Manager > Shell Script	175
Table 43 Ethernet, VLAN, Bridge, PPPoE/PPTP, and Virtual Interfaces Characteristics	178
Table 44 Example: Routing Table Entries for Interfaces	179
Table 45 Example: Routing Table Entry for a Gateway	179
Table 46 Example: Assigning IP Addresses from a Pool	181
Table 47 Relationships Between Different Types of Interfaces	182
Table 48 Network > Interface > Ethernet	184
Table 49 Network > Interface > Ethernet > Edit	187
Table 50 Network > Interface > Port Grouping	192
Table 51 Network > Interface > VLAN	195
Table 52 Network > Interface > VLAN > Edit	196
Table 53 Example: Bridge Table After Computer A Sends a Packet to Computer B	200
Table 54 Example: Bridge Table After Computer B Responds to Computer A	201
Table 55 Example: Routing Table Before and After Bridge Interface br0 Is Created	201
Table 56 Network > Interface > Bridge	202
Table 57 Network > Interface > Bridge > Edit	204
Table 58 Network > Interface > PPPoE/PPTP	208
Table 59 Network > Interface > PPPoE/PPTP > Edit	209
Table 60 Network > Interface > Auxiliary	212
Table 61 Network > Interface > Edit	214
Table 62 Least Load First: Example 1	217
Table 63 Network > Interface > Trunk	219
Table 64 Network > Interface > Trunk > Members	220
Table 65 Network > IPSec VPN > VPN Connection	230
Table 66 Network > IPSec VPN > VPN Connection > Edit	231
Table 67 Network > IPSec VPN > VPN Connection > Manual Key > Edit	235
Table 68 VPN Example: Matching ID Type and Content	242
Table 69 VPN Example: Mismatching ID Type and Content	242
Table 70 Network > IPSec VPN > VPN Gateway	245
Table 71 Network > IPSec VPN > VPN Gateway > Edit	246
Table 72 Network > IPSec VPN > Concentrator	252
Table 73 Network > IPSec VPN > Concentrator > Edit	253
Table 74 Network > IPSec VPN > SA Monitor	254
Table 75 OSPF vs. RIP	255
Table 76 Network > Routing Protocol > RIP	257
Table 77 OSPF: Redistribution from Other Sources to Each Type of Area	260
Table 78 Network > Routing Protocol > OSPF	262
Table 79 Network > Routing Protocol > OSPF > Edit	264
Table 80 Network > Zone	268
Table 81 Configuration > Network > Zone > Edit	269

Table 82 Network > ISP Account	271
Table 83 Network > ISP Account > Edit	272
Table 84 Network > Device HA > VRRP Group	278
Table 85 Network > Device HA > VRRP Group > Edit	280
Table 86 Network > Device HA > Synchronize	283
Table 87 Network > DDNS	287
Table 88 Network > DDNS > Edit	288
Table 89 Policy Route	293
Table 90 Policy Route Edit	295
Table 91 Policy Route Edit: Service	298
Table 92 IP Static Route	299
Table 93 IP Static Route Edit	300
Table 94 Default Through-ZyWALL Firewall Rules	302
Table 95 Blocking All LAN to WAN IRC Traffic Example	304
Table 96 Limited LAN to WAN IRC Traffic Example 1	305
Table 97 Limited LAN to WAN IRC Traffic Example 2	306
Table 98 Firewall: Zone Pairs	308
Table 99 Firewall: All Rules	311
Table 100 Firewall: To-ZyWALL Rules	313
Table 101 Firewall Rule Edit	316
Table 102 Policy > Application Patrol > Configuration	324
Table 103 Policy > Application Patrol > Configuration > Edit	326
Table 104 Policy > Application Patrol > Other Protocol	329
Table 105 Policy > Application Patrol > Other Protocol > Edit	330
Table 106 IDP > General	335
Table 107 Base Profiles	337
Table 108 Policy > IDP > Profile	338
Table 109 Policy Types	339
Table 110 IDP Service Groups	340
Table 111 Policy > IDP > Profile > Packet Inspection_Group View	343
Table 112 Policy > IDP > Profile > Packet Inspection_Query View	345
Table 113 IDP > Profile > Traffic Anomaly	353
Table 114 HTTP Inspection and TCP/UDP/ICMP Decoders	354
Table 115 IDP > Profile > Protocol Anomaly	358
Table 116 IP v4 Packet Headers	359
Table 117 Policy > IDP > Custom Signatures	361
Table 118 Policy > IDP > Custom Signatures > Add/Edit	364
Table 119 ZyWALL - Snort Equivalent Terms	371
Table 120 IDP Update	373
Table 121 Configuration > Policy > Content Filter > General	377
Table 122 Configuration > Policy > Content Filter > General > Add	380
Table 123 Configuration > Policy > Content Filter > Filtering Profile	381
Table 124 Configuration > Policy > Content Filtering > Filtering Profile > Add	383

Table 125 Configuration > Policy > Content Filtering > Filtering Profiles > Customization	389
Table 126 Configuration > Policy > Content Filter > Cache	392
Table 127 Policy > Virtual Server	405
Table 128 Policy > Virtual Server > Edit	406
Table 129 HTTP Redirect	411
Table 130 HTTP Redirect Edit	412
Table 131 Policy > VoIP Passthru	418
Table 132 Types of User Accounts	423
Table 133 LDAP/RADIUS: Keywords for User Attributes	424
Table 134 User/Group	426
Table 135 User/Group > User > Edit	427
Table 136 Reserved User Names	428
Table 137 User/Group > Group	429
Table 138 User/Group > Group > Edit	430
Table 139 User/Group > Setting	431
Table 140 User/Group > Setting > Force User Authentication Policy > add/edit	434
Table 141 Web Configurator for Non-Admin Users	435
Table 142 Object > Address > Address	438
Table 143 Object > Address > Address > Edit	439
Table 144 Object > Address > Address Group	440
Table 145 Object > Address > Address Group > Edit	441
Table 146 Object > Service > Service	444
Table 147 Object > Service > Service > Edit	445
Table 148 Object > Service > Service Group	446
Table 149 Object > Service > Service Group > Edit	447
Table 150 Configuration > Object > Schedule	450
Table 151 Configuration > Object > Schedule > One Time_1	451
Table 152 Configuration > Object > Schedule > Recurring_1	452
Table 153 Objects: AAA Server: LDAP: Default	458
Table 154 Objects > AAA Server > LDAP > Group	459
Table 155 Objects > AAA Server > LDAP > Group > Add	460
Table 156 Objects > AAA Server > RADIUS > Default	462
Table 157 Objects > AAA Server > RADIUS > Group	463
Table 158 Objects > AAA Server > RADIUS > Group > Add	464
Table 159 Objects > Auth. Method	465
Table 160 Objects > Auth. Method > Add	467
Table 161 My Certificates Screen	473
Table 162 My Certificates Add Screen	475
Table 163 My Certificate Edit Screen	479
Table 164 My Certificate Import Screen	481
Table 165 Trusted Certificates Screen	482
Table 166 Trusted Certificates Edit Screen	485
Table 167 Trusted Certificates Import Screen	487

Table 168 System > Host Name	489
Table 169 System > Date and Time	490
Table 170 Default Time Servers	492
Table 171 System > Console Port Speed	494
Table 172 System > DNS	495
Table 173 System > DNS > Address/PTR Record Edit	498
Table 174 System > DNS > Domain Zone Forwarder Edit	499
Table 175 System > DNS > MX Record Edit	500
Table 176 System > DNS > Service Control Rule Edit	501
Table 177 System > WWW	506
Table 178 Edit Service Control Rule	509
Table 179 System > SSH	515
Table 180 System > Telnet	518
Table 181 System > FTP	519
Table 182 SNMP Traps	522
Table 183 System > SNMP	523
Table 184 Specifications: Logs	525
Table 185 Maintenance > Logs > View Log	526
Table 186 Maintenance > Logs > Log Setting	529
Table 187 Maintenance > Logs > Log Setting > E-mail > Edit	531
Table 188 Maintenance > Logs > Log Setting > Remote Server > Edit	533
Table 189 Maintenance > Logs > Log Setting > Active Log Summary	536
Table 190 Maintenance > Report > Report	538
Table 191 Maximum Values for Reports	540
Table 192 Maintenance > Report > Session	541
Table 193 Device Specifications	545
Table 194 Hardware Specifications	545
Table 195 Commonly Used Services	547

About This User's Guide

This manual is designed to guide you through the configuration of your ZyWALL for its various applications. Generally, it is organized as follows.

- Introduction (ZyWALL, web configurator)
- Features (by menu item in the web configurator)
 - Overview, including background
 - Web Configurator screens
- Appendices

Intended Audience

This manual is intended for network administrators, or people who have a good knowledge of TCP/IP networking concepts and topology, who want to want to configure the ZyWALL using the web configurator.

- 1 Read [Chapter 1 on page 47](#) chapter for an overview of features available on the ZyWALL.
- 2 Read [Chapter 3 on page 59](#) for web browser requirements and an introduction to the main components, icons and menus in the ZyWALL web configurator.
- 3 Read [Chapter 4 on page 67](#) if you're using the wizards for first time setup and you want more detailed information than what the real time online help provides.
- 4 It is highly recommended you read [Chapter 5 on page 105](#) for detailed information on essential terms used in the ZyWALL, what prerequisites are needed to configure a feature and how to use that feature.
- 5 It is highly recommended you read [Chapter 6 on page 119](#) for multiple ZyWALL application examples.
- 6 Subsequent chapters are arranged by menu item as defined in the web configurator. Read each chapter carefully for detailed information on that menu item.

Related Technical Documentation

- Quick Start Guide

The Quick Start Guide is designed to show you how to make the ZyWALL hardware connections, rack mounting and access the web configurator wizards. (See the wizard real time help for information on configuring each screen.) It contains a connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- Configuration Reference Card

See this handy reference card to see what prerequisites are needed to configure a feature and how to use this feature in the ZyWALL.

- Command Reference Guide

The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the ZyWALL.

Note: It is recommended you use the web configurator to configure the ZyWALL.

- Web Configurator Online Help

Click the help icon in any screen for help in configuring that screen and supplementary information.

- Supporting Disk

Refer to the included CD for support documents.

- ZyXEL Web Site

Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!










The Technical Writing Team
ZyXEL Communications Corp.
6 Innovation Road II
Science-Based Industrial Park
Hsinchu, 30099, Taiwan.

E-mail: techwriters@zyxel.com.tw

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one of the predefined choices.
- 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

<p>ZyWALL</p> 	<p>Computer</p> 	<p>Notebook computer</p> 
<p>Server</p> 	<p>DSLAM</p> 	<p>Firewall</p> 
<p>Telephone</p> 	<p>Switch</p> 	<p>Router</p> 

CHAPTER 1

Introducing the ZyWALL

This chapter gives an overview of the ZyWALL. It explains the front panel ports, LEDs, introduces the management methods, different ways to start or stop the ZyWALL and shows you how to reset the ZyWALL to its factory default settings.

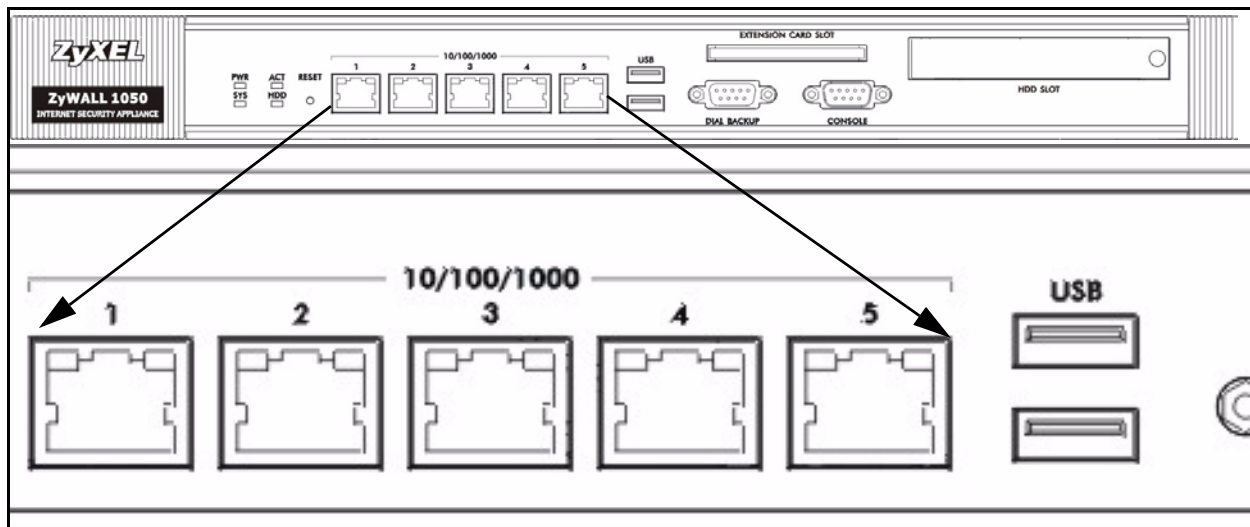
1.1 Overview and Key Default Settings

The ZyWALL is an Internet Security Gateway designed for Small and Medium Businesses (SMB). Its flexible configuration helps network administrators set up the network and enforce security policies efficiently. In addition, the ZyWALL provides excellent throughput, making it an ideal solution for reliable, secure service.

The physical ports on the front panel of the ZyWALL are called “ge1”, “ge2”, “ge3”, “ge4”, “ge5” where “ge” stands for Gigabit Ethernet. By default “ge1” is mapped to port 1, “ge2” to port 2 and so on.

Also, by default “ge1” is the LAN interface, “ge2” and “ge3” are combined as the WAN_TRUNK.

Figure 1 Front Panel Ports



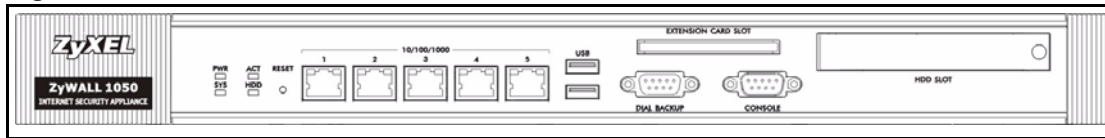
The Ethernet management interface can only be accessed from LAN side by default. The default management IP address is 192.168.1.1; the default login user name and password are “admin” and “1234” respectively.

To enable management access from the WAN, log into the web configurator, go to **System > WWW**, and change the default **Deny** to **Accept** in the rule in the **Admin Service Control** section.

You should configure the **Network > Interface** screens first to establish network connectivity before configuring security features such as firewall, VPN, content filtering, IDP and so on.

1.2 Front Panel LEDs

Figure 2 Front Panel



The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The ZyWALL is turned off.
	Green	On	The ZyWALL is turned on.
	Red	On	There is a hardware component failure. Shut down the device, wait for a few minutes and then restart the device. If the LED turns red again, then please contact your vendor.
SYS	Green	Off	The ZyWALL is not ready or has failed.
		On	The ZyWALL is ready and running.
		Flashing	The ZyWALL is restarting.
ACT	Green	Off	The DIAL BACKUP port is not connected.
		Flashing	The DIAL BACKUP port is sending or receiving packets.
		On	The DIAL BACKUP port is connected.
HDD	Green	Off	No hard disk is present. The ZyWALL can run without the hard disk.
		On	The hard disk is present.
		Flashing	The ZyWALL is accessing the hard disk.
Ports 1 - 5	Green	Off	There is no traffic on this port.
		Flashing	The ZyWALL is sending or receiving packets on this port.
	Orange	Off	There is no connection on this port.
		On	This port has a successful link.

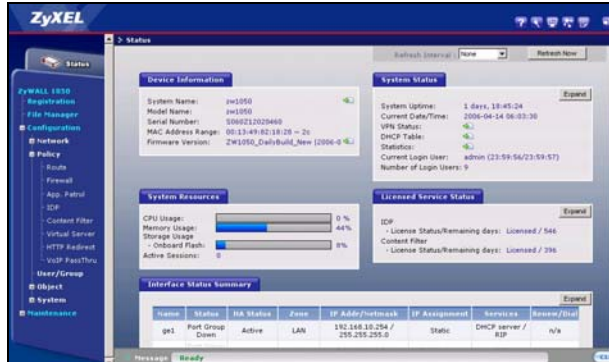
1.3 Management Overview

You can use the following ways to manage the ZyWALL.

Web Configurator

The web configurator allows easy ZyWALL setup and management using an Internet browser. This User's Guide provides information about the web configurator.

Figure 3 Managing the ZyWALL: Web Configurator



Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the ZyWALL. You can access it using remote management (for example, SSH or Telnet) or via the console port. The Command Reference Guide provides more information about the CLI.

Figure 4 Managing the ZyWALL: Command-Line Interface

```
Welcome to ZyWALL 1050

Username: admin
Password:

> enable
> configure terminal
Router(config)#
```

Console Port

You can use the console port to manage the ZyWALL. You have to use CLI commands, which are explained in the Command Reference Guide.

The default settings for the console port are as follows.

Table 2 Managing the ZyWALL: Console Port

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None

Table 2 Managing the ZyWALL: Console Port

SETTING	VALUE
Stop Bit	1
Flow Control	Off

1.4 Starting and Stopping the ZyWALL

This section explains some of the ways to start and stop the ZyWALL. These are summarized below.

Table 3 Starting and Stopping the ZyWALL

METHOD	DESCRIPTION
Turning on the power button	A cold start occurs when you turn on the power to the ZyWALL. The ZyWALL powers up, checks the hardware, and starts the system processes.
Rebooting the ZyWALL	A warm start (without powering down and powering up again) occurs when you use the Reboot button in the Reboot screen or when you use the <code>reboot</code> command. The ZyWALL writes all cached data to disk, stops the system processes, and then does a warm start.
Using the RESET button	If you press the RESET button, the ZyWALL sets the configuration to its default values and then reboots.
Using the <code>shutdown</code> command	The <code>shutdown</code> command writes all cached data to disk and stops the system processes. It does not turn off the power. You have to turn the power off and on manually to start the ZyWALL again. You should use this command before you turn off the ZyWALL.
Turning off the power button	Power off occurs when you turn off the power to the ZyWALL. The ZyWALL simply turns off. It does not stop the system processes or write cached data to disk.

Note: It is recommended you use the `shutdown` command before turning off the ZyWALL.

When you apply configuration files or running shell scripts, the ZyWALL does not stop or start the system processes. However, you might lose access to network resources temporarily while the ZyWALL is applying configuration files or running shell scripts.

1.5 Resetting the ZyWALL

If you forget the administrator password(s) or cannot access the ZyWALL by any method, you can reset the ZyWALL to its factory-default settings. Any configuration files or shell scripts that you saved on the ZyWALL should still be available afterwards.

use the procedure to reset the ZyWALL to its factory-default settings.

Note: This procedure removes the current configuration. If you want to reboot the device without changing the current configuration, see [Chapter 38 on page 543](#).

- 1** Make sure the **SYS** LED is on and not blinking.
- 2** Press the **RESET** button and hold it until the **SYS** LED begins to blink. (This usually takes about five seconds.)
- 3** Release the **RESET** button, and wait for the ZyWALL to restart.

You should be able to access the ZyWALL using the default settings.

CHAPTER 2

Features and Applications

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

2.1 Features

The ZyWALL's security features include VPN, firewall, content filtering, IDP (Intrusion Detection and Prevention), and certificates. It also provides bandwidth management, NAT, port forwarding, policy routing, DHCP server and many other powerful features.

The rest of this section provides more information about the features of the ZyWALL.

High Availability

To ensure the ZyWALL provides reliable, secure Internet access, set up one or more of the following:

- Multiple WAN ports and configure load balancing between these ports
- A backup Internet connection
- A backup ZyWALL in the event the master ZyWALL fails (device HA).

Virtual Private Networks (VPN)

Use IPSec VPN to provide secure communication between two sites over the Internet or any insecure network that uses TCP/IP for communication. The ZyWALL also offers hub-and-spoke VPN.

Flexible Security Zones

Many security settings are made by zone, not by interface, port, or network. As a result, it is much simpler to set up and to change security settings in the ZyWALL. You can create or remove zones, and you can assign each network, VLAN, or interface to any zone.

Firewall

The ZyWALL's firewall is a stateful inspection firewall. The ZyWALL restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

Intrusion Detection and Prevention (IDP)

IDP (Intrusion Detection and Protection) on the ZyWALL is designed to protect against network-based intrusions. See [Section 21.7.1 on page 339](#) for a list of attacks that the ZyWALL can protect against. You can also create your own custom IDP rules.

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 applications such as Internet access, e-mail, Voice-over-IP (VoIP), video conferencing and other business-critical applications.

Content Filtering

Content filtering allows schools and businesses to create and enforce Internet access policies tailored to the needs of the organization.

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

2.2 Packet Flow

The following is the key used to describe the packet flow in the ZyWALL.

Table 4 Packet Flow Key

Ethernet	The interface on which the packet is received or sent
VLAN	Virtual LAN
Encap	The PPPoE or PPTP encapsulation used
ALG	Application Layer Gateway
AC	Application Classifier is the Application Protocol (AP) layer-7 classifier.
DNAT	Destination NAT
Routing	Routing includes policy routes, interface routing, static routes and load balancing for example.
FW	Firewall (Through ZyWALL)
zFW	Firewall (To ZyWALL)
IDP	Intrusion Detection & Protection
AP	Application Patrol

Table 4 Packet Flow Key

CF	Content Filtering
SNAT	Source NAT
IPSec D/E	VPN Decryption/Encryption
BWM	Bandwidth Management
RM	Remote Management (System)

2.2.1 Interface to Interface (Through ZyWALL)

Ethernet -> VLAN -> Encap -> ALG -> AC -> DNAT-> Routing -> FW -> AC -> IDP -> AP
-> CF -> SNAT -> BWM -> Encap -> VLAN -> Ethernet

2.2.2 Interface to Interface (To/From ZyWALL)

To: Ethernet -> VLAN -> Encap -> ALG -> AC -> DNAT -> Routing -> zFW -> RM
From: RM -> Routing -> BWM -> Encap -> VLAN -> Ethernet

2.2.3 Interface to Interface (From VPN Tunnel)

This example shows the flow from a VPN tunnel through the ZyWALL, not to the ZyWALL or to another VPN tunnel (VPN concentrator).

Ethernet -> VLAN -> Encap -> ALG -> AC -> DNAT-> Routing -> zFW -> IPSec D -> ALG
-> AC -> DNAT-> Routing -> FW -> AC -> IDP -> AP -> CF -> -> SNAT -> BWM -> Encap
-> VLAN -> Ethernet

2.2.4 Interface to Interface (To VPN Tunnel)

This example shows the flow to a VPN tunnel from a source other than the ZyWALL or another VPN tunnel (VPN concentrator).

Ethernet -> VLAN -> Encap -> ALG -> AC -> DNAT-> Routing -> FW -> AC -> IDP -> AP
-> CF -> SNAT -> IPSec E -> Routing -> BWM -> Encap -> VLAN -> Ethernet

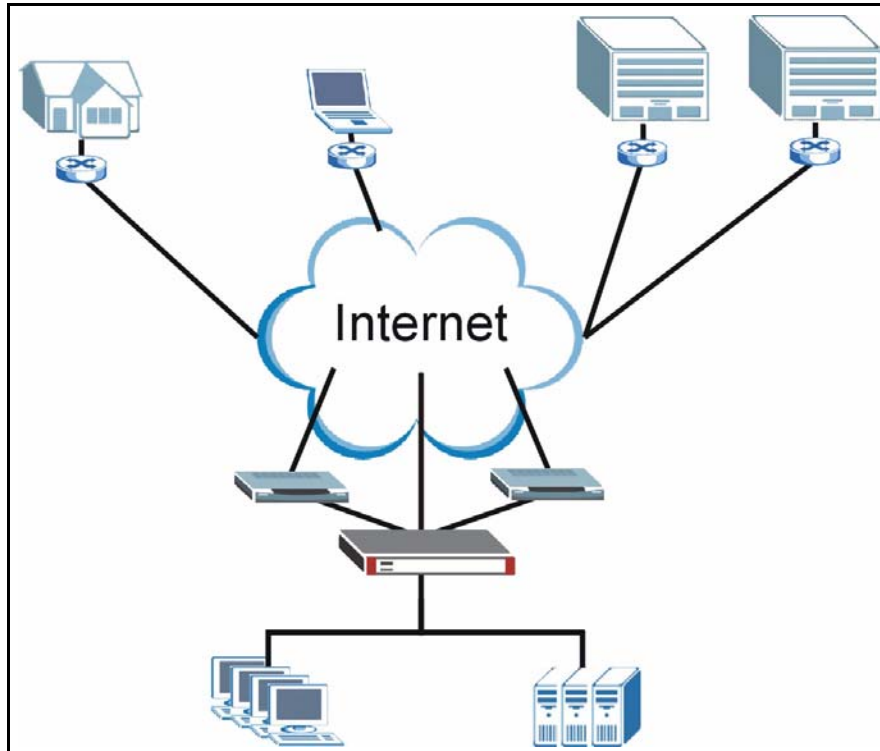
2.3 Applications

These are some example applications for your ZyWALL. See also [Chapter 6 on page 119](#) for configuration tutorial examples.

2.3.1 VPN Connectivity

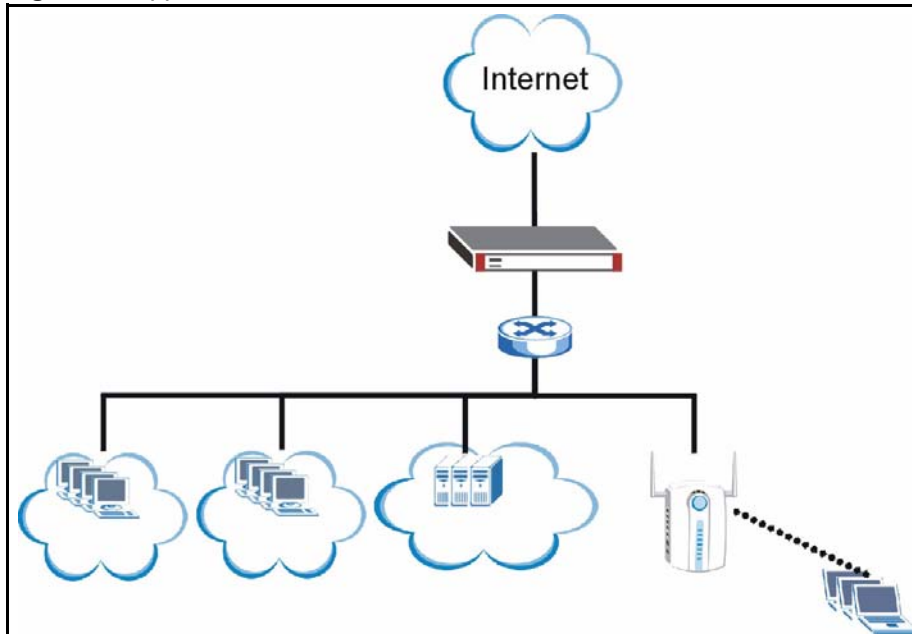
Set up VPN tunnels with other companies, branch offices, telecommuters, and business travelers to provide secure access to your network. You can also set up additional connections to the Internet to provide better service.

Figure 5 Applications: VPN Connectivity



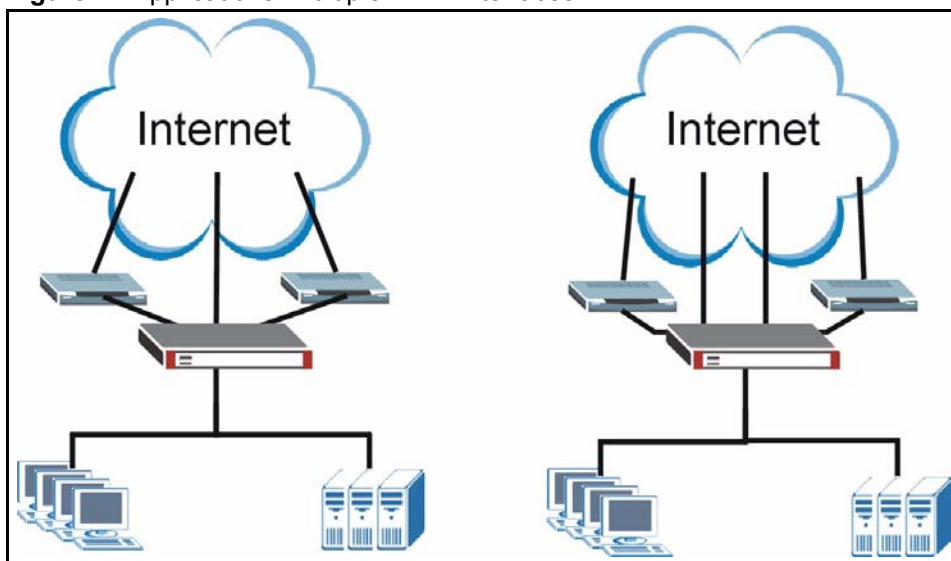
2.3.2 User-Aware Access Control

Set up security policies that restrict access to sensitive information and shared resources based on the user who is trying to access it.

Figure 6 Applications: User-Aware Access Control

2.3.3 Multiple WAN Interfaces

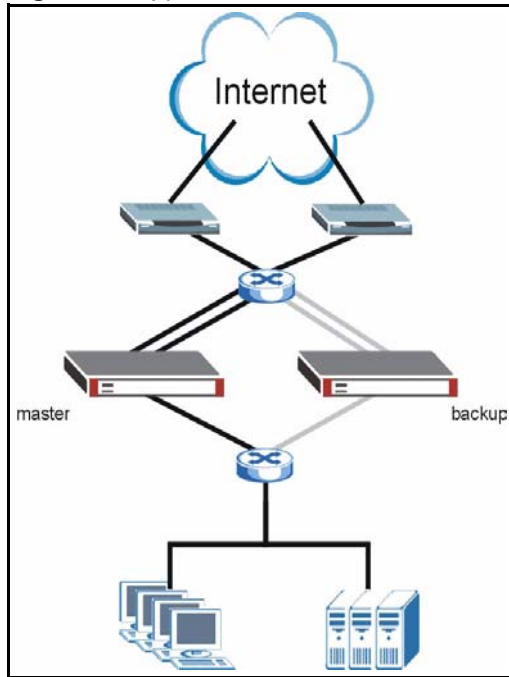
Set up multiple connections to the Internet on the same port, or set up multiple connections on different ports. In either case, you can balance the loads between them.

Figure 7 Applications: Multiple WAN Interfaces

2.3.4 Device HA

Set up an additional ZyWALL as a backup gateway to ensure the default gateway is always available for the network.

Figure 8 Applications: Device HA



CHAPTER 3

Web Configurator

The ZyWALL web configurator allows easy ZyWALL setup and management using an Internet browser.

3.1 Web Configurator Requirements

In order to use the web configurator, you must

- Use Internet Explorer 6.0 or later, Netscape Navigator 7.2 or later, or Firefox 1.0.7 or later
- Allow pop-up windows (blocked by default in Windows XP Service Pack 2)
- Enable JavaScripts (enabled by default)
- Enable Java permissions (enabled by default)
- Enable cookies

The recommended screen resolution is 1024 x 768 pixels.

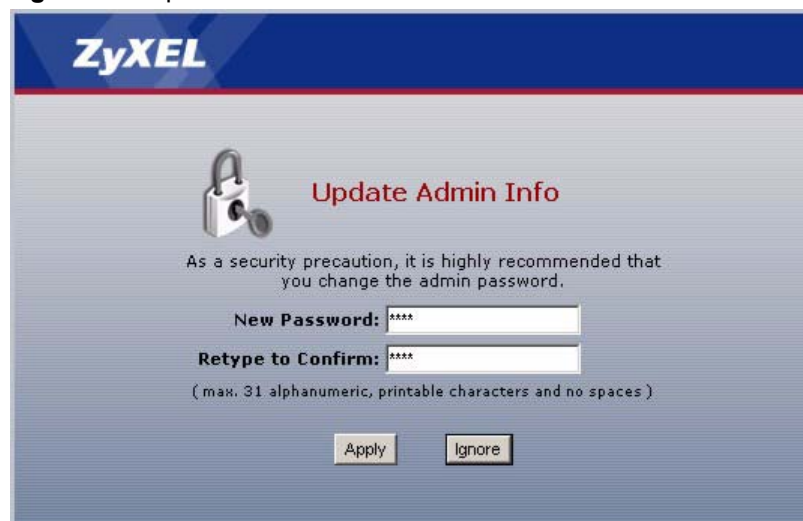
3.2 Web Configurator Access

- 1 Make sure your ZyWALL hardware is properly connected. See the Quick Start Guide.
- 2 Open your web browser, and go to <http://192.168.1.1>. By default, the ZyWALL automatically routes this request to its HTTPS server, and it is recommended to keep this setting. The **Login** screen appears.

Figure 9 Login Screen

The screenshot shows the ZyWALL 1050 login interface. At the top is the ZyXEL logo. Below it, the text "ZyWALL 1050" is centered. A prompt says "Enter User Name/password and click to login." There are two input fields: "User Name:" and "Password:". Below the password field, a note in parentheses states "(max. 31 alphanumeric, printable characters and no spaces)". A yellow note icon is followed by the text "Note:" and two numbered instructions: "1. Turn on Javascript and Cookie setting in your web browser." and "2. Turn off Popup Window Blocking in your web browser." At the bottom, there are two buttons: "Login" and "Reset".

- 3** Type the user name (default: “admin”) and password (default: “1234”), and click **Login**. If you logged in using the default user name and password, the **Update Admin Info** screen ([Figure 10 on page 60](#)) appears. Otherwise, the main screen ([Figure 11 on page 61](#)) appears.

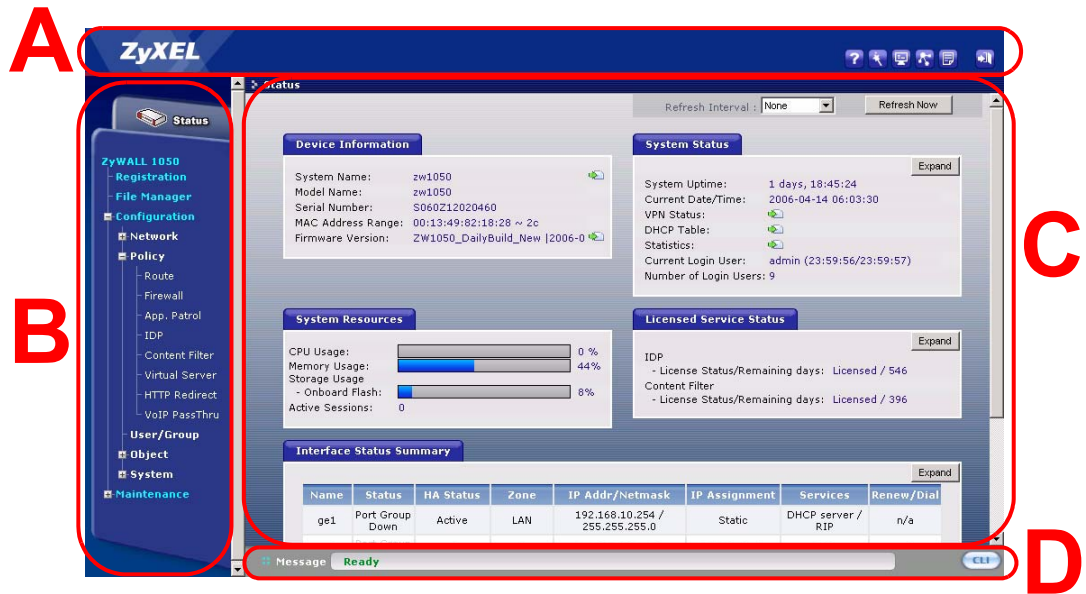
Figure 10 Update Admin Info Screen

The screenshot shows the "Update Admin Info" screen. At the top is the ZyXEL logo. Below it, a padlock icon is shown next to the title "Update Admin Info". A message reads: "As a security precaution, it is highly recommended that you change the admin password." There are two input fields: "New Password:" and "Retype to Confirm:". Below the second field, a note in parentheses states "(max. 31 alphanumeric, printable characters and no spaces)". At the bottom, there are two buttons: "Apply" and "Ignore".

- 4** The screen above appears every time you log in using the default user name and default password. If you change the password for the default user account, this screen does not appear anymore.

Follow the directions in this screen. If you change the default password, the **Login** screen ([Figure 9 on page 60](#)) appears after you click **Apply**. If you click **Ignore**, the main screen appears.

Figure 11 Main Screen



3.3 Web Configurator Main Screen

As illustrated in [Figure 11 on page 61](#), the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

3.3.1 Title Bar

The title bar provides some icons in the upper right corner.



The icons provide the following functions.

Table 5 Title Bar: Web Configurator Icons







ICON	DESCRIPTION
	Help: Click this icon to open the help page for the current screen.
	Wizards: Click this icon to open one of the web configurator wizards. See Chapter 4 on page 67 for more information.
	Console: Click this icon to open the console in which you can use the command line interface (CLI).

Table 5 Title Bar: Web Configurator Icons (continued)

ICON	DESCRIPTION
	Site Map: Click this icon to display the site map for the web configurator. You can use the site map to go directly to any menu item or any tab in the web configurator.
	About: Click this icon to display basic information about the ZyWALL.
	Logout: Click this icon to log out of the web configurator.

3.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyWALL features. The following tables describe each menu item.

Table 6 Navigation Panel Summary (Except for Configuration Menu)

LINK	TAB	FUNCTION
Status		Use this screen to look at the ZyWALL's general device information, system status, system resource usage, licensed service status, and interface status.
Registration	Registration	Use this screen to register the device and activate trial services.
	Service	Use this screen to look at the licensed service status and to upgrade licensed services.
File Manager	Configuration File	Use this screen to manage and upload configuration files for the ZyWALL.
	Firmware Package	Use this screen to look at the current firmware version and to upload firmware.
	Shell Script	Use this screen to manage and run shell script files for the ZyWALL.
Maintenance		
Log	View Log	Use this screen to look at log entries.
	Log Setting	Use this screen to configure the system log, e-mail logs, and remote syslog servers.
Report	Report	Use this screen to collect traffic information and display basic reports about it.
	Session	Use this screen to display the status of all current sessions.
Reboot		Use this screen to restart the ZyWALL.

Table 7 Navigation Panel Summary (Configuration Menu Only)

LINK	TAB	FUNCTION
Network		

Table 7 Navigation Panel Summary (Configuration Menu Only) (continued)

LINK	TAB	FUNCTION
Interface	Ethernet	Use this screen to manage Ethernet interfaces and virtual Ethernet interfaces.
	Port Grouping	Use this screen to configure physical port groups.
	VLAN	Use this screen to create and manage VLAN interfaces and virtual VLAN interfaces.
	Bridge	Use this screen to create and manage bridges and virtual bridge interfaces.
	PPPoE/PPTP	Use this screen to create and manage PPPoE/PPTP interfaces.
	Auxiliary	Use this screen to manage the DIAL BACKUP port.
	Trunk	Use this screen to create and manage trunks for load balancing and link HA.
IPSec VPN	VPN Connection	Use this screen to configure IPSec tunnels.
	VPN Gateway	Use this screen to configure IKE tunnels.
	Concentrator	Use this screen to configure VPN concentrators (hub-and-spoke VPN).
	SA Monitor	Use this screen to monitor current VPN tunnels.
Routing Protocol	RIP	Use this screen to configure device-level RIP settings.
	OSPF	Use this screen to configure device-level OSPF settings, including areas and virtual links.
Zone		Use this screen to configure zones used to define various policies.
Device HA	VRRP Group	Use this screen to define and configure virtual groups of redundant routers.
	Synchronize	Use this screen to manage synchronization of ZyWALL configuration between master routers and backup routers in virtual groups of redundant routers.
ISP Account		Use this screen to create and manage ISP account information for PPPoE/PPTP interfaces.
DDNS		Use this screen to define and manage domain names and DDNS servers.
Policy		
Route	Policy Route	Use this screen to create and manage routing policies.
	Static Route	Use this screen to create and manage IP static routing information.
Firewall		Use this screen to create and manage level-3 traffic rules.
App Patrol	Configuration	Use this screen to manage traffic for instant messenger, peer-to-peer, streaming, and general protocols.
	Other Protocol	Use this screen to manage other kinds of traffic.
IDP	General	Use this screen to look at and manage IDP bindings.
	Profile	Use this screen to create and manage IDP profiles.
	Custom Signatures	Use this screen to create, import, or export custom signatures.
	Update	Use this screen to schedule signature updates and to update signature information immediately.
Content Filter	General	Use this screen to create and manage content filter policies.
	Filtering Profile	Use this screen to create and manage the detailed filtering rules for content filtering policies.
	Cache	Use this screen to manage the URL cache in the ZyWALL.
Virtual Server		Use this screen to set up and manage port forwarding rules.

Table 7 Navigation Panel Summary (Configuration Menu Only) (continued)

LINK	TAB	FUNCTION
HTTP Redirect		Use this screen to set up and manage HTTP redirection rules.
VoIP passThru		Use this screen to configure SIP and H.323 pass-through settings.
User/Group	User	Use this screen to create and manage users.
	Group	Use this screen to create and manage groups of users.
	Setting	Use this screen to manage default settings for all users, general settings for user sessions, and rules to force user authentication.
Object		
Address	Address	Use this screen to create and manage host, range, and network (subnet) addresses.
	Address Group	Use this screen to create and manage groups of addresses.
Service	Service	Use this screen to create and manage TCP and UDP services.
	Service Group	Use this screen to create and manage groups of services.
Schedule		Use this screen to create one-time and recurring schedules.
AAA Server	LDAP-Default	Use this screen to configure the default LDAP settings.
	LDAP-Group	Use this screen to create and manage groups of LDAP servers.
	RADIUS-Default	Use this screen to configure the default RADIUS settings.
	RADIUS-Group	Use this screen to create and manage groups of RADIUS servers.
Auth. Method		Use this screen to create and manage ways of authenticating users.
Certificate	My Certificates	Use this screen to create and manage the ZyWALL's certificates.
	Trusted Certificates	Use this screen to import and manage certificates from trusted sources.
System		
Host Name		Use this screen to configure the system and domain name for the ZyWALL.
Date/Time		Use this screen to configure the current date, time, and time zone in the ZyWALL.
Console Speed		Use this screen to set the console speed.
DNS		Use this screen to configure the DNS server and address records for the ZyWALL.
WWW		Use this screen to configure HTTP, HTTPS, and general authentication.
SSH		Use this screen to configure the SSH server and SSH service settings for the ZyWALL.
TELNET		Use this screen to configure the telnet server settings for the ZyWALL.
FTP		Use this screen to configure the FTP server settings for the ZyWALL.
SNMP		Use this screen to configure SNMP communities and services.

3.3.3 Main Window

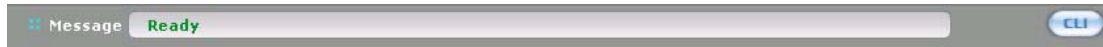
The main window shows the screen you select in the menu. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See [Chapter 3 on page 59](#) for more information about the **Status** screen.

3.3.4 Status Bar

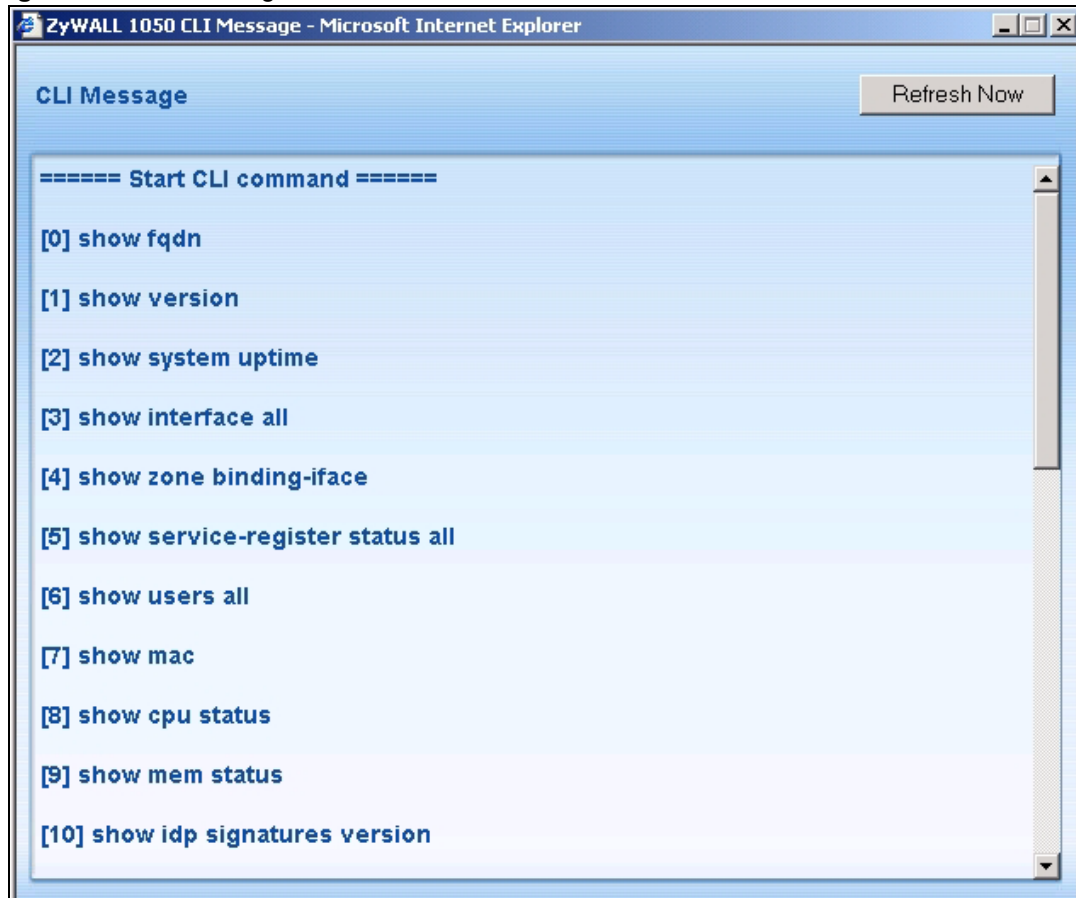
Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

Figure 12 Message Bar



Click **CLI** to look at the CLI commands sent by the web configurator. These commands appear in a popup window, such as the following.

Figure 13 CLI Messages



Click **Refresh Now** to update the screen. For example, if you just enabled a particular feature, you can look at the commands the web configurator generated to enable it. Close the popup window when you are done with it.

See the Command Reference Guide for information about each command.

CHAPTER 4

Wizard Setup


This chapter provides information on configuring the Wizard setup screens in the web configurator. See the feature-specific chapters in this User's Guide for background information.

4.1 Wizard Setup Overview

The web configurator's setup wizards help you configure Internet and VPN connection settings.

Note: Use the wizards only for initial configuration starting from the default configuration.

Changes you make in an installation or VPN wizard may not be applied if you have already changed the ZyWALL's configuration.

In the ZyWALL web configurator, click the **Wizard** icon  to open the **Wizard Setup Welcome** screen. The following summarizes the wizards you can select:

- **INSTALLATION SETUP, ONE ISP**

Click this link to open a wizard to set up a single Internet connection for Gigabit Ethernet port **2**. This wizard creates matching ISP account settings in the ZyWALL if you use PPPoE or PPTP. See [Section 4.2 on page 68](#).

- **INSTALLATION SETUP, TWO ISP**

Click this link to open a wizard to set up Internet connections for Gigabit Ethernet (ge) interfaces **2** and **3**. See [Section 4.5 on page 86](#). You can connect one interface to one ISP (or network) and connect the other to a second ISP (or network). You can use the second WAN connection for load balancing to increase overall network throughput or as a backup to enhance network reliability (see [Section 11.3 on page 215](#) for more on load balancing).

This wizard creates matching ISP account settings in the ZyWALL if you use PPPoE or PPTP. This wizard also creates a WAN trunk.

- **VPN SETUP**

Use **VPN SETUP** to configure a VPN connection. See [Section 4.6 on page 88](#).

Figure 14 Wizard Setup Welcome

4.2 Installation Setup, One ISP

The wizard screens vary 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.

Note: Enter the Internet access information exactly as your ISP gave it to you.

Figure 15 Internet Access: Step 1

The following table describes the labels in this screen.

Table 8 Internet Access: Step 1

LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	Choose the Ethernet option when the WAN port is used as a regular Ethernet. Otherwise, choose PPPoE or PPTP for a dial-up connection according to the information from your ISP.
WAN IP Address Assignments	
WAN Interface	This is the interface you are configuring for Internet access.
Zone	Select the security zone to which you want this interface and Internet connection to belong.
IP Address Assignment	Select Auto If your ISP did not assign you a fixed IP address. Select Static If the ISP assigned a fixed IP address.
Next	Click Next to continue.

4.3 Step 1 Internet Access

Encapsulation: Choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection according to the information from your ISP.

WAN Interface: This is the interface you are configuring for Internet access.

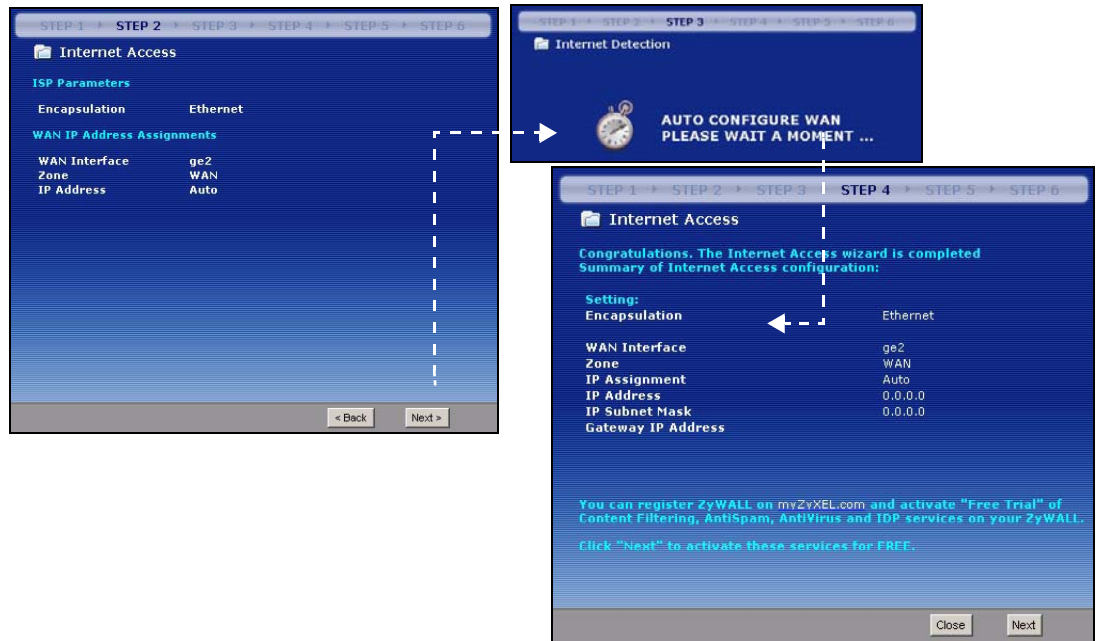
Zone: Select the security zone to which you want this interface and Internet connection to belong.

IP Address Assignment: Select **Auto** if your ISP did not assign you a fixed IP address. Select **Static** if the ISP assigned a fixed IP address.

4.3.1 Ethernet: Auto IP Address Assignment

If you select **Auto** as the **IP Address Assignment** in the previous screen, the following screen displays. Click **Next** to apply the configuration settings.

Figure 16 Ethernet Encapsulation: Auto: Finish



You have set up your ZyWALL to access the Internet.

Note: If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP. You can click **Next** and use the following screen to perform a basic registration (see [Section 4.4 on page 83](#)). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.3.2 Ethernet: Static IP Address Assignment

If you select **Static** as the **IP Address Assignment**, the following screen displays.

Figure 17 Ethernet Encapsulation: Static

The following table describes the labels in this screen.

Table 9 Ethernet Encapsulation: Static

LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	This displays the type of Internet connection you are configuring.
WAN IP Address Assignments	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	Enter the IP address that your ISP gave you. This should be a static, public IP address.
IP Subnet Mask	Enter the subnet mask for the IP address.
Gateway IP Address	Enter the IP address of the router through which this WAN connection will send traffic (the default gateway).
First DNS Server Second 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 computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Enter the DNS server IP addresses.
Next	Click Next to continue.

The ZyWALL applies the configuration settings.

4.3.3 Step 2 Internet Access Ethernet

You do not configure this screen if you selected **Auto** as the **IP Address Assignment** in the previous screen.

Note: Enter the Internet access information exactly as given to you by your ISP.

WAN Interface: This is the number of the interface that will connect with your ISP.

Zone: This is the security zone to which this interface and Internet connection will belong.

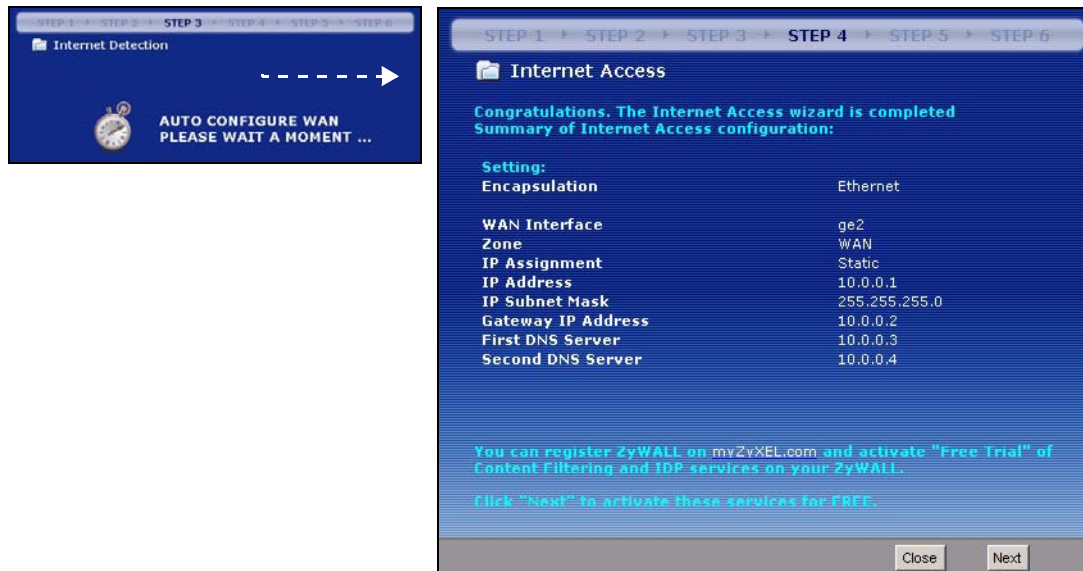
IP Address: Enter your (static) public IP address.

IP Subnet Mask: Enter the subnet mask for this WAN connection's IP address.

Gateway IP Address: Enter the IP address of the router through which this WAN connection will send traffic (the default gateway).

DNS Server: The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The ZyWALL uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.

Figure 18 Ethernet Encapsulation: Static: Finish



You have set up your ZyWALL to access the Internet.

Note: If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP. You can click **Next** and use the following screen to perform a basic registration (see [Section 4.4 on page 83](#)). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.3.4 PPPoE: Auto IP Address Assignment

If you select **Auto** as the **IP Address Assignment** in the previous screen, the following screen displays after you click **Next**.

Figure 19 PPPoE Encapsulation: Auto

The following table describes the labels in this screen.

Table 10 PPPoE Encapsulation: Auto

LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	This displays the type of Internet connection you are configuring.
Service Name	Type the PPPoE service name given to you by your ISP. PPPoE uses a service name to identify and reach the PPPoE server. You can use alphanumeric and -_@\$. / characters, and it can be up to 64 characters long.
User Name	Type the user name given to you by your ISP. You can use alphanumeric and -_@\$. / characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select Nailed-Up if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is 100 seconds.
WAN IP Address Assignments	

Table 10 PPPoE Encapsulation: Auto (continued)

LABEL	DESCRIPTION
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	The ISP will assign your WAN IP address automatically
Next	Click Next to continue.

The ZyWALL applies the configuration settings.

Figure 20 PPPoE Encapsulation: Auto: Finish



You have set up your ZyWALL to access the Internet.

Note: If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP. You can click **Next** and use the following screen to perform a basic registration (see [Section 4.4 on page 83](#)). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.3.5 PPPoE: Static IP Address Assignment

If you select **Static** as the **IP Address Assignment**, the following screen displays.

Figure 21 PPPoE Encapsulation: Static

STEP 1 > STEP 2 > STEP 3 > STEP 4 > STEP 5 > STEP 6

Internet Access

ISP Parameters

Encapsulation: PPPoE

Service Name: test (Optional)

User Name: test

Password: ****

Retype to Confirm: ****

Nailed-Up

Idle Timeout: 100 (Seconds)

WAN IP Address Assignments

WAN Interface: ppp0

Zone: WAN

IP Address: 10.0.0.2

First DNS Server: 10.0.0.7

Second DNS Server: 10.0.0.8

< Back Next >

The following table describes the labels in this screen.

Table 11 PPPoE Encapsulation: Static

LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	This displays the type of Internet connection you are configuring.
Service Name	Type the PPPoE service name given to you by your ISP. PPPoE uses a service name to identify and reach the PPPoE server. You can use alphanumeric and - _@\$. / characters, and it can be up to 64 characters long.
User Name	Type the user name given to you by your ISP. You can use alphanumeric and - _@\$. / characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select Nailed-Up if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is 100 seconds.
WAN IP Address Assignments	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	Enter your WAN IP address in this field.

Table 11 PPPoE Encapsulation: Static (continued)

LABEL	DESCRIPTION
	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 computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
First DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right.
Second DNS Server	Leave the field as 0.0.0.0 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.
Next	Click Next to continue.

4.3.6 Step 2 Internet Access PPPoE

Note: Enter the Internet access information exactly as given to you by your ISP.

4.3.6.1 ISP Parameters

Type the PPPoE **Service Name** from your service provider.

Type the **User Name** given to you by your ISP.

Type the **Password** associated with the user name.

Select **Nailed-Up** if you do not want the connection to time out. Otherwise, type the **Idle Timeout** in seconds that elapses before the router automatically disconnects from the PPPoE server.

4.3.6.2 WAN IP Address Assignments

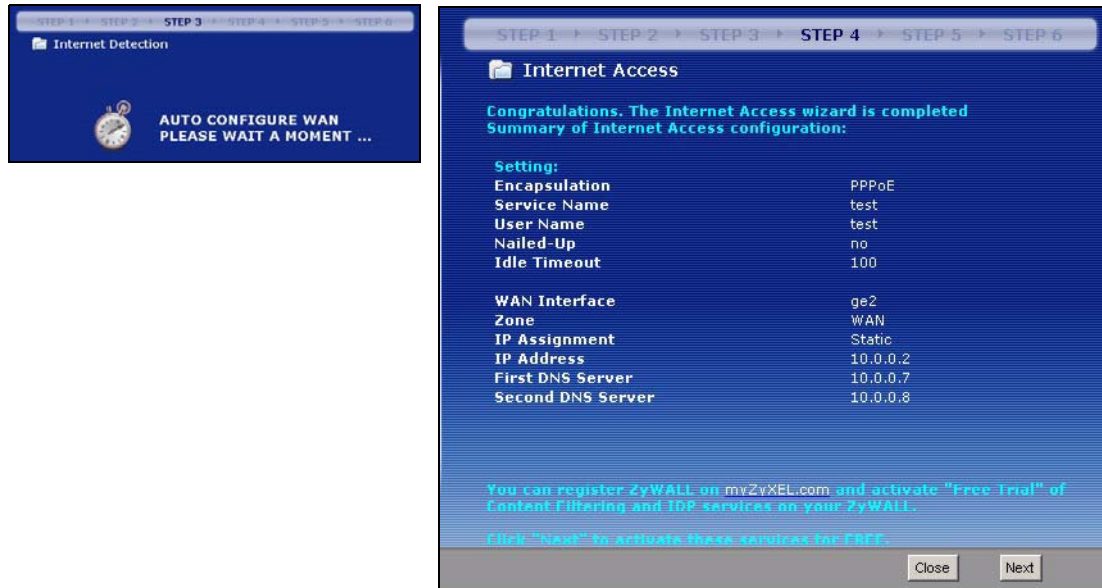
You do not configure this section if you selected **Auto** as the **IP Address Assignment** in the previous screen.

WAN Interface: This is the number of the interface that will connect with your ISP.

Zone: This is the security zone to which this interface and Internet connection will belong.

IP Address: Enter your (static) public IP address.

DNS Server: The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The ZyWALL uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.

Figure 22 PPPoE Encapsulation: Static: Finish

You have set up your ZyWALL to access the Internet.

Note: If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP. You can click **Next** and use the following screen to perform a basic registration (see [Section 4.4 on page 83](#)). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.3.7 PPTP: Auto IP Address Assignment

If you select **Auto** as the **IP Address Assignment** in the previous screen, the following screen displays.

Figure 23 PPTP Encapsulation: Auto



The following table describes the labels in this screen.

Table 12 PPTP Encapsulation: Auto

LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	This displays the type of Internet connection you are configuring.
User Name	Type the user name given to you by your ISP. You can use alphanumeric and - _@\$. / characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select Nailed-Up if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server.
PPTP Configuration	
Base Interface	This displays the identity of the Ethernet interface you configure to connect with a modem or router.
Base IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP	Type the IP address of the PPTP server.

Table 12 PPTP Encapsulation: Auto (continued)

LABEL	DESCRIPTION
Connection ID	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 DSL modem. You can use alphanumeric and -_ : characters, and it can be up to 31 characters long.
WAN IP Address Assignments	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	Enter your WAN IP address in this field.
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 computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	
First DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right.
Second DNS Server	Leave the field as 0.0.0.0 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.
Next	Click Next to continue.

The ZyWALL applies the configuration settings.

Figure 24 PPTP Encapsulation: Auto: Finish

You have set up your ZyWALL to access the Internet.

Note: If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP. You can click **Next** and use the following screen to perform a basic registration (see [Section 4.4 on page 83](#)). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.3.8 PPTP: Static IP Address Assignment

If you select **Static** as the **IP Address Assignment**, the following screen displays.

Figure 25 PPTP Encapsulation: Static

The screenshot shows a configuration wizard for PPTP Encapsulation. At the top, there is a progress bar with steps 1 through 6, where STEP 2 is highlighted. Below the progress bar, the title 'Internet Access' is displayed. The configuration is divided into three sections: 'ISP Parameters', 'PPTP Configuration', and 'WAN IP Address Assignments'. In the 'ISP Parameters' section, 'Encapsulation' is set to 'PPTP', 'User Name' is 'test', 'Password' and 'Retype to Confirm' are masked with '****', and 'Idle Timeout' is set to 100 seconds. In the 'PPTP Configuration' section, 'Base Interface' is 'ge2', 'Base IP Address' is '10.0.0.5', 'IP Subnet Mask' is '255.255.255.0', 'Server IP' is '10.0.0.1', and 'Connection ID' is an empty field. In the 'WAN IP Address Assignments' section, 'WAN Interface' is 'ppp0', 'Zone' is 'WAN', 'IP Address' is '10.0.0.3', 'First DNS Server' is '10.0.0.7', and 'Second DNS Server' is '10.0.0.8'. At the bottom of the screen, there are two buttons: '< Back' and 'Next >'.

The following table describes the labels in this screen.

Table 13 PPTP Encapsulation: Static

LABEL	DESCRIPTION
ISP Parameters	
Encapsulation	This displays the type of Internet connection you are configuring.

Table 13 PPTP Encapsulation: Static (continued)

LABEL	DESCRIPTION
User Name	Type the user name given to you by your ISP. You can use alphanumeric and -_@\$./ characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select Nailed-Up if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server.
PPTP Configuration	
Base Interface	This displays the identity of the Ethernet interface you configure to connect with a modem or router.
Base IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP	Type the IP address of the PPTP server.
Connection ID	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 DSL modem. You can use alphanumeric and -_ : characters, and it can be up to 31 characters long. This field can be blank.
WAN IP Address Assignments	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	Enter your WAN IP address in this field.
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 computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	
First DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right.
Second DNS Server	Leave the field as 0.0.0.0 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.
Next	Click Next to continue.

4.3.9 Step 2 Internet Access PPTP

Note: Enter the Internet access information exactly as given to you by your ISP.

4.3.9.1 ISP Parameters

Type the **User Name** given to you by your ISP.

Type the **Password** associated with the user name.

Select **Nailed-Up** if you do not want the connection to time out. Otherwise, type the **Idle Timeout** in seconds that elapses before the router automatically disconnects from the PPTP server.

4.3.9.2 PPTP Configuration

Base Interface: This is the identity of the Ethernet interface you configure to connect with a modem or router.

Type a **Base IP Address** (static) assigned to you by your ISP.

Type the **IP Subnet Mask** assigned to you by your ISP (if given).

Server IP: Type the IP address of the PPTP server.

Type a **Connection ID** or connection name. 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 broadband modem or router.

4.3.9.3 WAN IP Address Assignments

You do not configure this section if you selected **Auto** as the **IP Address Assignment** in the previous screen.

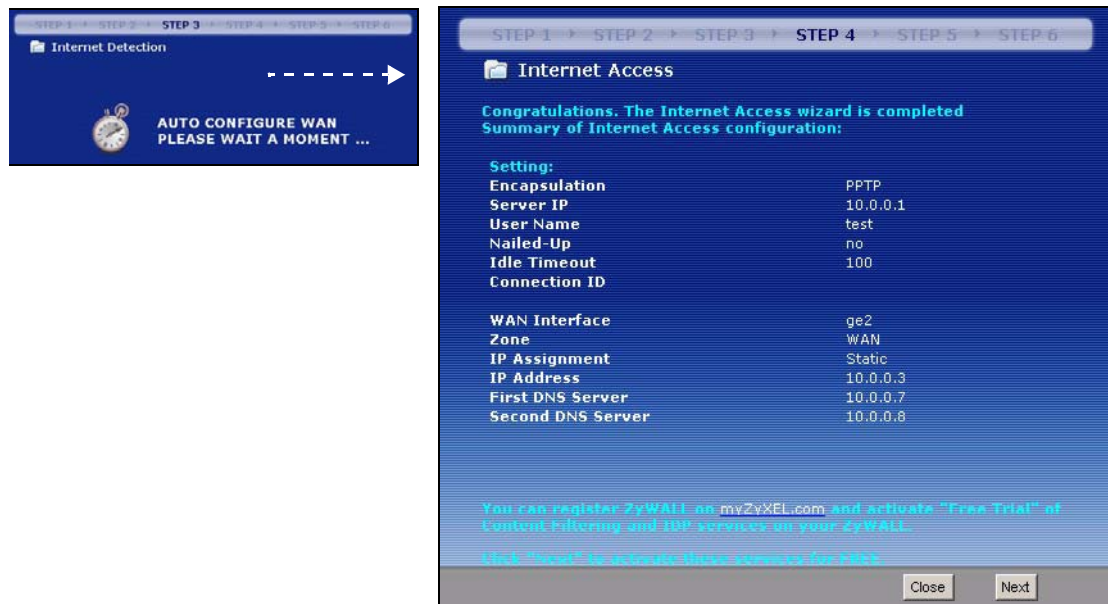
WAN Interface: This is the connection type on the interface you are configuring to connect with your ISP.

Zone: This is the security zone to which this interface and Internet connection will belong.

IP Address: Enter your (static) public IP address.

DNS Server: The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The ZyWALL uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.

The ZyWALL applies the configuration settings.

Figure 26 PPTP Encapsulation: Static: Finish

4.3.10 Step 4 Internet Access - Finish

You have set up your ZyWALL to access the Internet.

Note: If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP. You can click **Next** and use the following screen to perform a basic registration (see [Section 4.4 on page 83](#)). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

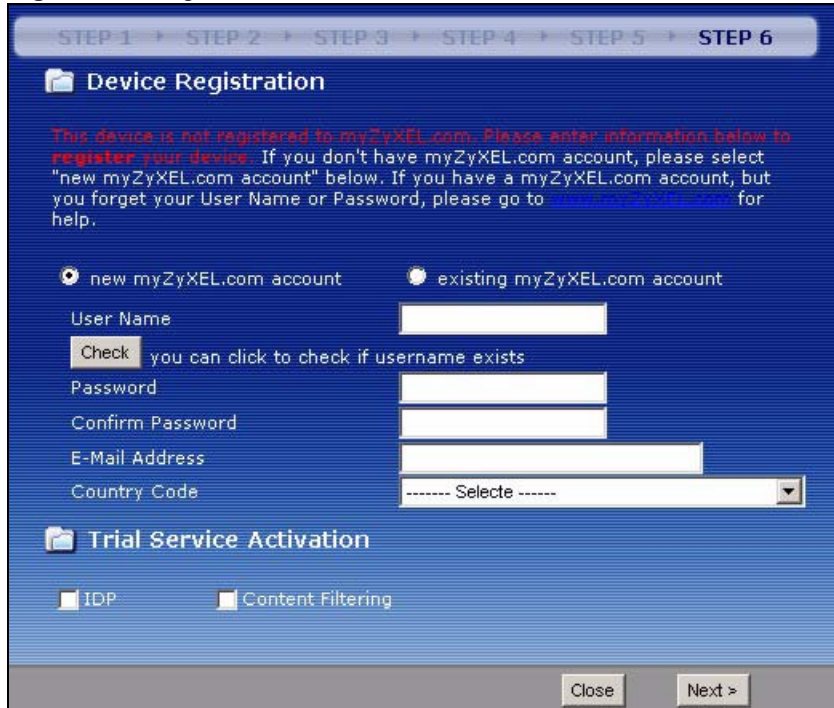
4.4 Device Registration

Use this screen to register your ZyWALL with myZXEL.com and activate trial periods of subscription security features if you have not already done so.

Note: You must be connected to the Internet to register.

This screen displays a read-only user name and password if the ZyWALL is already registered. It also shows which trial services are activated (if any). You can still select the unchecked trial service(s) to activate it after registration. Use the **Registration > Service** screen to update your service subscription status.

Figure 27 Registration



The following table describes the labels in this screen.

Table 14 Registration

LABEL	DESCRIPTION
Device Registration	If you select existing myZyXEL.com account , only the User Name and Password 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.
UserName	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 Code	Select your country from the drop-down box list.
Trial Service Activation	You can try a trial service subscription. After the trial expires, you can buy an iCard and enter the license key in the Registration Service screen to extend the service.
IDP Content Filtering	Select the check box to activate a trial. The trial period starts the day you activate the trial.

Table 14 Registration (continued)

LABEL	DESCRIPTION
Close	Click Close to exit the wizard.
Next	Click Next to save your changes back to the ZyWALL and activate the selected services.

Select **existing myZyXEL.com account** if you already have an account at myZyXEL.com and enter your user name and password in the fields below to register your ZyWALL.

Enter a **User Name** for your myZyXEL.com account. Use from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed. Click **Check** to verify that it is available.

Password: Use six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.

E-Mail Address: Use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.

Country Code: Select your country from the drop-down box list.

Trial Service Activation: You can try a trial service subscription. The trial period starts the day you activate the trial. After the trial expires, you can buy an iCard and enter the license key in the **Registration > Service** screen to extend the service.

Figure 28 Registration: Registered Device

The screenshot displays the 'Device Registration' wizard at Step 6. At the top, a progress bar shows steps 1 through 6, with Step 6 being the active step. The main area is titled 'Device Registration' and contains two input fields: 'User Name' with the value 'johngall' and 'Password' with masked characters '*****'. Below this is the 'Trial Service Activation' section, which includes two checked checkboxes: 'IDP' and 'Content Filtering'. A 'Close' button is located in the bottom right corner of the window.

4.5 Installation Setup, Two Internet Service Providers

This wizard allows you to configure two interfaces for Internet access through either two different Internet Service Providers (ISPs) or two different accounts with the same ISP.

The configuration of the following screens is explained in [Section 4.2 on page 68](#) section. Configure the **First WAN Interface** and click **Next**.

Figure 29 Internet Access: Step 1: First WAN Interface

STEP 1 STEP 2 STEP 3 STEP 4 STEP 5 STEP 6 STEP 7 STEP 8

Internet Access, First WAN Interface

ISP Parameters

Encapsulation: Ethernet

WAN IP Address Assignments

WAN Interface: ge2
Zone: WAN
IP Address Assignment: Auto

< Back Next >

After you configure the **First WAN Interface**, you can configure the **Second WAN Interface**. Click **Next** to continue.

Figure 30 Internet Access: Step 3: Second WAN Interface

The screenshot displays the configuration wizard for the second WAN interface. At the top, a progress bar shows steps 1 through 8, with 'STEP 3' highlighted. Below the progress bar, the title 'Internet Access, Second WAN Interface' is shown. The configuration is divided into two sections: 'ISP Parameters' and 'WAN IP Address Assignments'. Under 'ISP Parameters', the 'Encapsulation' is set to 'Ethernet'. Under 'WAN IP Address Assignments', the 'WAN Interface' is set to 'ge3', the 'Zone' is set to 'WAN', and the 'IP Address Assignment' is set to 'Static'. At the bottom right, there are '< Back' and 'Next >' buttons.

After you configure the **Second WAN Interface**, a summary of configuration settings display for both WAN interfaces.

Figure 31 Internet Access: Finish

Note: You can register your ZyWALL with myZyXEL.com and activate trials of services like IDP. Use the myZyXEL.com link if you do already have a myZyXEL.com account. If you already have a myZyXEL.com account, you can click **Next** and use the following screen to register your ZyWALL and activate service trials (see [Section 4.4 on page 83](#)).

Alternatively, click **Close** to exit the wizard.

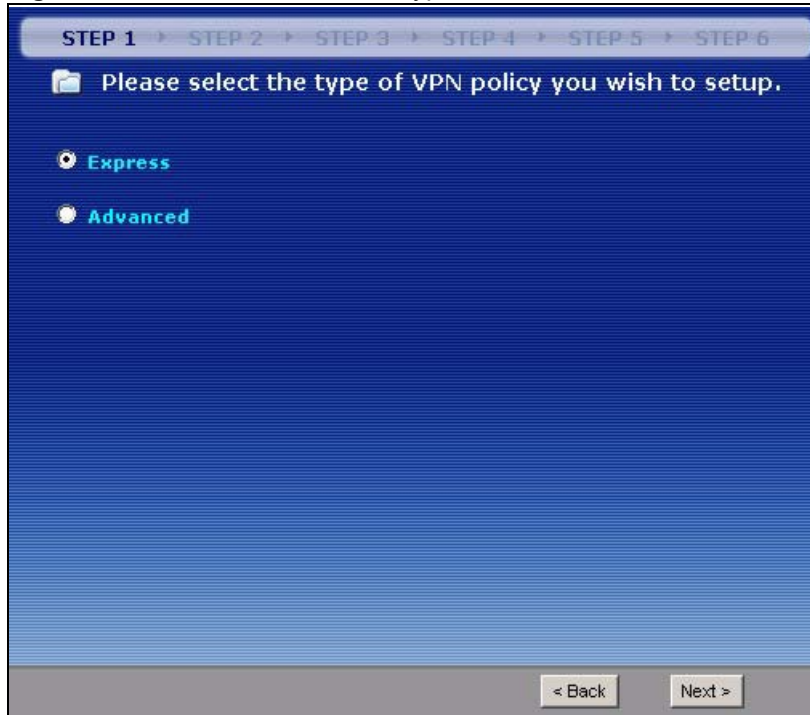
4.5.1 Internet Access Wizard Setup Complete

Well done! You have successfully set up your ZyWALL to access the Internet.

4.6 VPN Setup

The VPN wizard creates corresponding VPN connection and VPN gateway settings, a policy route and address objects that you can use later in configuring more VPN connections or other features.

Click **VPN SETUP** in the Wizard Setup Welcome screen ([Figure 14 on page 68](#)) to open the following screen. Use it to select which type of VPN settings you want to configure.

Figure 32 VPN Wizard: Wizard Type

The following table describes the labels in this screen.

Table 15 VPN Wizard: Step 1: Wizard Type

LABEL	DESCRIPTION
Express	Use this wizard to create a VPN connection with another ZyWALL 1050 using a pre-shared key and default security settings.
Advanced	Use this wizard to configure detailed VPN security settings such as using certificates. The VPN connection can be to a ZyWALL 1050 or other IPsec device.
Next	Click Next to continue.

4.7 VPN Wizards

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

Use the **Express** wizard to create a VPN connection with another ZyWALL 1050 using a pre-shared key and default security settings.

Use the **Advanced** wizard to configure detailed VPN security settings such as using certificates. The VPN connection can be to a ZyWALL 1050 or other IPsec devices.

4.7.1 VPN Express Wizard

Click the **Express** radio button as shown in [Figure 32 on page 89](#) to display the following screen.

Figure 33 VPN Express Wizard: Step 2

The following table describes the labels in this screen.

Table 16 VPN Express Wizard: Step 2

LABEL	DESCRIPTION
Name	Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Secure Gateway	Enter the WAN IP address or domain name of the remote IPSec router (secure gateway) to identify the remote IPSec router by its IP address or a domain name. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address.
Pre-Shared Key	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. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. Precede hexadecimal characters with "0x". 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.
Next	Click Next to continue.

4.8 VPN Express Wizard - Remote Gateway

The **Remote Gateway** policy identifies the IPSec devices at either end of a VPN tunnel.

Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Secure Gateway: Enter the WAN IP address or domain name of the remote IPSec router (secure gateway). Use 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address and no domain name.

Pre-Shared Key: Type the password. Both ends of the VPN tunnel must use the same password. Use 8 to 31 case-sensitive ASCII characters or 16 to 62 hexadecimal ("0-9", "A-F") characters. Proceed hexadecimal characters with "0x".

Figure 34 VPN Express Wizard: Step 3

Policy Type	IP Address	Mask
Local Policy (IP/Mask)	192.168.1.2	255.255.255.0
Remote Policy (IP/Mask)	10.10.10.10	255.255.255.0

The following table describes the labels in this screen.

Table 17 VPN Express Wizard: Step 3

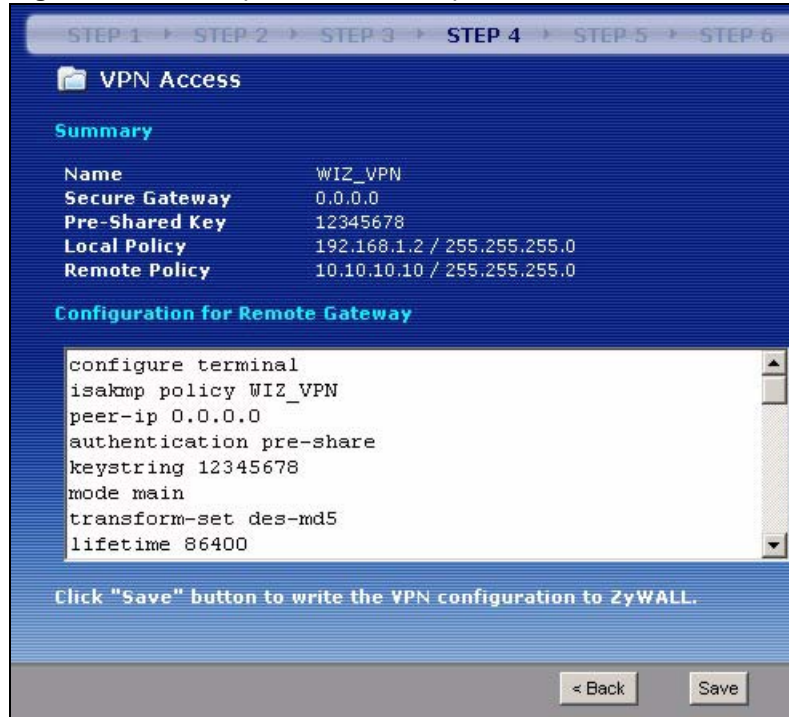
LABEL	DESCRIPTION
Local Policy (IP/ Mask)	Type a static local IP address that corresponds to the remote IPSec router's configured remote IP address (the remote IP address of the other ZyWALL 1050). To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind your ZyWALL.
Remote Policy (IP/Mask)	Type a static local IP address that corresponds to the remote IPSec router's configured local IP address (the local IP address of the ZyWALL 70 or other ZyWALL 1050). To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind the remote gateway.
Next	Click Next to continue.

4.8.1 VPN Express Wizard - Policy Setting

The **Policy Setting** specifies which devices can use the VPN tunnel. Local and remote IP addresses must be static.

Local Policy (IP/Mask): Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the peer IPSec device.

Remote Policy (IP/Mask): Type the IP address of a computer behind the peer IPSec device. You can also specify a subnet. This must match the local IP address configured on the peer IPSec device.

Figure 35 VPN Express Wizard: Step 4

The following table describes the labels in this screen.

Table 18 VPN Express Wizard: Step 4

LABEL	DESCRIPTION
Summary	
Name	This is the name of the VPN connection (and VPN gateway).
Secure Gateway	This is the WAN IP address or domain name of the remote IPSec router. If this field displays 0.0.0.0 , only the remote IPSec router can initiate the VPN connection.
Pre-Shared Key	This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation.
Local Policy	This is a (static) IP address and Subnet Mask on the LAN behind your ZyWALL.
Remote Policy	This is a (static) IP address and Subnet Mask on the network behind the remote IPSec router.
Configuration for Remote Gateway	These commands set the matching VPN connection settings for the remote gateway. If the remote gateway is a ZyWALL 1050, you can copy and paste this list into its command line interface in order to configure it for the VPN tunnel. You can also use a text editor to save these commands as a shell script file with a ".zysh" filename extension. Then you can use the file manager to run the script in order to configure the VPN connection. See the commands reference guide for details on the commands displayed in this list.
Save	Click Save to store the VPN settings on your ZyWALL.

4.8.2 VPN Express Wizard - Summary

This summary of VPN tunnel settings is read-only.

Name: Identifies the VPN gateway policy.

Secure Gateway: IP address or domain name of the peer IPsec device.

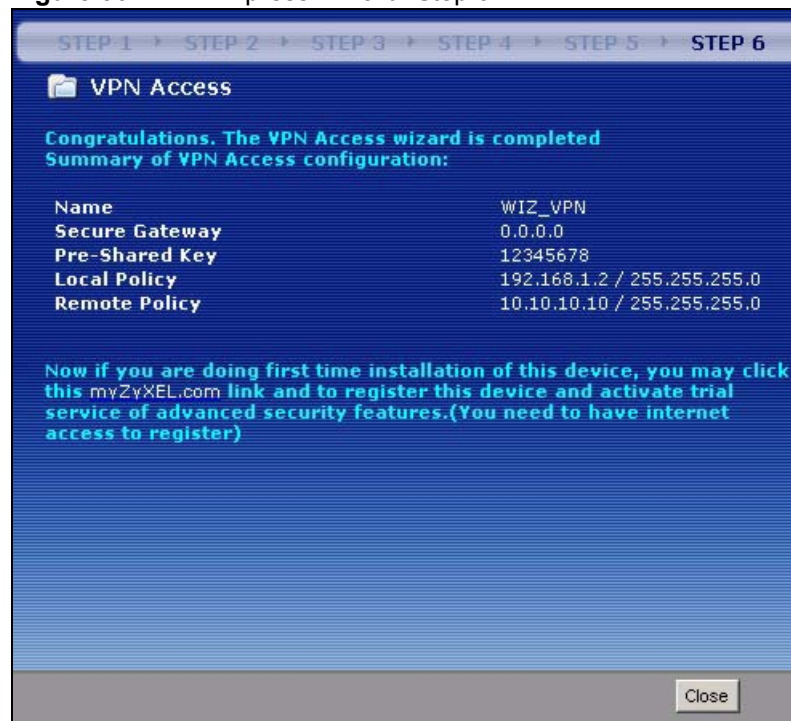
Pre-Shared Key: VPN tunnel password.

Local Policy: IP address and subnet mask of the computers on the network behind your ZyWALL that can use the tunnel.

Remote Policy: IP address and subnet mask of the computers on the network behind the peer IPsec device that can use the tunnel.

You can copy and paste the **Configuration for Remote Gateway** commands into a peer ZyWALL 1050's command line interface.

Figure 36 VPN Express Wizard: Step 6



Note: If you have not already done so, use the myZyXEL.com link and register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

Alternatively, click **Close** to exit the wizard.

4.8.3 VPN Express Wizard - Finish

Now you can use the VPN tunnel.

Note: If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP. You can click **Next** and use the following screen to perform a basic registration (see [Section 4.4 on page 83](#)). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

4.8.4 VPN Advanced Wizard

Click the **Advanced** radio button as shown in [Figure 32 on page 89](#) to display the following screen.

Figure 37 VPN Advanced Wizard: Step 2

The following table describes the labels in this screen.

Table 19 VPN Advanced Wizard: Step 2

LABEL	DESCRIPTION
Remote Gateway	
Name	Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Secure Gateway	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 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address.

Table 19 VPN Advanced Wizard: Step 2 (continued)

LABEL	DESCRIPTION
My Address (interface)	Select an interface from the drop-down list box to use on your ZyWALL.
Authentication Method	
Pre-Shared Key	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. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. Precede hexadecimal characters with "0x". 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.
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 My Certificates screen. Click Certificate under the Object menu to go to the My Certificates screen where you can view the ZyWALL's list of certificates.
Next	Click Next to continue.

4.8.5 VPN Advanced Wizard - Remote Gateway

The **Remote Gateway** policy identifies the IPSec devices at either end of a VPN tunnel.

Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Secure Gateway: Enter the WAN IP address or domain name of the remote IPSec router (secure gateway). Use 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address and no domain name.

Select an interface to use on your ZyWALL.

Select **Pre-Shared Key** to use a password for authentication. Both ends of the VPN tunnel must use the same pre-shared key. Use 8 to 31 case-sensitive ASCII characters or 16 to 62 hexadecimal ("0-9", "A-F") characters. Precede hexadecimal characters with "0x".

Select **Certificate** to use a digital certificate for authentication. default uses the ZyWALL's default certificate. Click **Object > Certificate** to configure other certificates in the **My Certificates** screen.

4.8.5.1 Phase 1 Setting

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).

Figure 38 VPN Advanced Wizard: Step 3

STEP 1 → STEP 2 → **STEP 3** → STEP 4 → STEP 5 → STEP 6

VPN Advanced Access

Phase 1 Setting

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

Key Group: DH1

SA Life Time (Seconds): 86400 <180 - 3000000>

NAT Traversal

Dead Peer Detection (DPD)

< Back Next >

The following table describes the labels in this screen.

Table 20 VPN Advanced Wizard: Step 3

LABEL	DESCRIPTION
Negotiation Mode	Select Main for identity protection. Select Aggressive to allow more incoming connections from dynamic IP addresses to use separate passwords. Note: Multiple SAs (security associations) connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES . It also requires more processing power, resulting in increased latency and decreased throughput. AES128 uses a 128-bit key and is faster than 3DES . AES192 uses a 192-bit key and AES256 uses a 256-bit key. Select Null to have no encryption.
Authentication Algorithm	MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5 , but is slower. Select MD5 for minimal security and SHA1 for maximum security.
Key Group	You must choose a key group for phase 1 IKE setup. DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number.

Table 20 VPN Advanced Wizard: Step 3 (continued)

LABEL	DESCRIPTION
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 60 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.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. Note: The remote IPSec router must also have NAT traversal enabled. See Section 12.4.2.2 on page 243 for more information.
Dead Peer Detection (DPD)	Select this check box if you want the ZyWALL to make sure the remote IPSec router is there before it transmits data through the IKE SA. If there has been no traffic for at least 15 seconds, the ZyWALL sends a message to the remote IPSec server. If the remote IPSec server responds, the ZyWALL transmits the data. If the remote IPSec server does not respond, the ZyWALL shuts down the IKE SA.
Next	Click Next to continue.

4.8.6 VPN Advanced Wizard - Phase 1

Phases: IKE (Internet Key Exchange) negotiation has two phases. A phase 1 exchange establishes an IKE SA (Security Association) and phase 2 (Key Exchange) uses the SA to negotiate SAs for IPSec.

Note: Multiple SAs connecting through a secure gateway must have the same negotiation mode.

Negotiation Mode: Select **Main** for identity protection. Select **Aggressive** to allow more incoming connections from dynamic IP addresses to use separate passwords.

Proposal: **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** uses no encryption.

Authentication Algorithm: **MD5** gives minimal security. **SHA-1** gives higher security.

Key Group: **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput).

SA Life Time: Set how often the ZyWALL renegotiates the IKE SA. A short SA Life Time increases security, but renegotiation temporarily disconnects the VPN tunnel.

NAT Traversal: Select this if the VPN tunnel must pass through NAT (there is a NAT router between the IPSec devices).

Use **Dead Peer Detection (DPD)** to have the ZyWALL make sure the remote IPsec router is there before transmitting data through the IKE SA. If the remote IPsec server does not respond, the ZyWALL shuts down the IKE SA.

4.8.6.1 Phase 2 Setting

Phase 2 in an IKE uses the SA that was established in phase 1 to negotiate SAs for IPsec.

Figure 39 VPN Advanced Wizard: Step 4

The following table describes the labels in this screen.

Table 21 VPN Advanced Wizard: Step 4

LABEL	DESCRIPTION
Phase 2 Setting	
Active Protocol	Select the security protocols used for an SA. Both AH and ESP increase ZyWALL processing requirements and communications latency (delay).
Encapsulation	Tunnel is compatible with NAT, Transport is not. Tunnel mode encapsulates the entire IP packet to transmit it securely. 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).

Table 21 VPN Advanced Wizard: Step 4 (continued)

LABEL	DESCRIPTION
Encryption Algorithm	When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES . It also requires more processing power, resulting in increased latency and decreased throughput. AES128 uses a 128-bit key and is faster than 3DES . AES192 uses a 192-bit key and AES256 uses a 256-bit key. Select Null to have no encryption.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 60 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 (None) by default in phase 2 IPsec SA setup. This allows faster IPsec setup, but is not so secure. Select DH1 , DH2 or DH5 to enable PFS. DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number (more secure, yet slower).
Policy Setting	
Local Policy (IP/ Mask)	Type a static local IP address that corresponds to the remote IPsec router's configured remote IP address. To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind your ZyWALL.
Incoming Interface	Select an interface from the drop-down list box to have packets encrypted by the remote IPsec router to enter the ZyWALL via this interface.
Remote Policy (IP/ Mask)	Type a static local IP address that corresponds to the remote IPsec router's configured local IP address. To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind the remote gateway.
Property	
Nail Up	Select this if you want the ZyWALL to automatically renegotiate the IPsec SA when the SA life time expires.
Next	Click Next to continue.

4.8.7 VPN Advanced Wizard - Phase 2

Active Protocol: **ESP** is compatible with NAT, **AH** is not.

Encapsulation: **Tunnel** is compatible with NAT, **Transport** is not.

Proposal: **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** uses no encryption.

Local Policy (IP/Mask): Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the peer IPsec device.

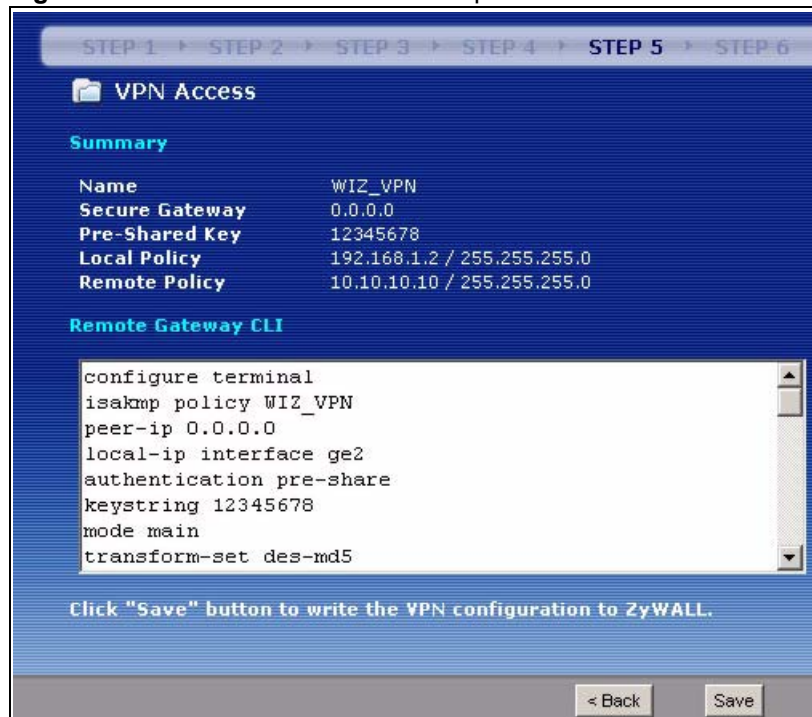
Incoming Interface: The peer IPSec device connects to the ZyWALL via this interface.

Remote Policy (IP/Mask): Type the IP address of a computer behind the peer IPSec device. You can also specify a subnet. This must match the local IP address configured on the peer IPSec device.

Nail Up: Select this to have the ZyWALL automatically renegotiate the IPSec SA when the SA life time expires.

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 40 VPN Advanced Wizard: Step 5



The following table describes the labels in this screen.

Table 22 VPN Advanced Wizard: Step 5

LABEL	DESCRIPTION
Summary	
Name	This is the name of the VPN connection (and VPN gateway).
Secure Gateway	This is the WAN IP address or domain name of the remote IPSec router. If this field displays 0.0.0.0 , only the remote IPSec router can initiate the VPN connection.
Pre-Shared Key	This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation.
Local Policy	This is a (static) IP address and Subnet Mask on the LAN behind your ZyWALL.
Remote Policy	This is a (static) IP address and Subnet Mask on the network behind the remote IPSec router.

Table 22 VPN Advanced Wizard: Step 5 (continued)

LABEL	DESCRIPTION
Remote Gateway CLI	These commands set the matching VPN connection settings for the remote gateway. If the remote gateway is a ZyWALL 1050, you can copy and paste this list into its command line interface in order to configure it for the VPN tunnel. You can also use a text editor to save these commands as a shell script file with a ".zysh" filename extension. Then you can use the file manager to run the script in order to configure the VPN connection. See the commands reference guide for details on the commands displayed in this list.
Save	Click Save to store the VPN settings on your ZyWALL.

4.8.8 VPN Advanced Wizard - Summary

This summary of VPN tunnel settings is read-only.

Name: Identifies the VPN connection (and the VPN gateway).

Secure Gateway: IP address or domain name of the peer IPsec device.

Pre-Shared Key: VPN tunnel password.

Local Policy: IP address and subnet mask of the computers on the network behind your ZyWALL that can use the tunnel.

Remote Policy: IP address and subnet mask of the computers on the network behind the peer IPsec device that can use the tunnel.

Copy and paste the **Remote Gateway CLI** commands into a peer ZyWALL 1050's command line interface.

Click **Save** to save the VPN rule.

4.8.9 VPN Advanced Wizard - Finish

Now you can use the VPN tunnel.

Figure 41 VPN Wizard: Step 6: Advanced



Note: If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP. You can click **Next** and use the following screen to perform a basic registration (see [Section 4.4 on page 83](#)). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

CHAPTER 5

Configuration Basics

This section provides a lot of information to help you configure the ZyWALL effectively. Some of it is helpful when you are just getting started. Some of it is provided for your reference when you try configuring various features in the ZyWALL.

- [Section 5.1 on page 105](#) introduces (very briefly) how granular the configuration is in the ZyWALL.
- [Section 5.2 on page 106](#) introduces some differences in terminology and organization between the ZyWALL and other routers, particularly ZyNOS routers.
- [Section 5.3 on page 107](#) explains the differences between physical ports, interfaces, and zones in the ZyWALL.
- [Section 5.4 on page 108](#) identifies the features you should configure before and after you configure the main screens for each feature. For example, if you want to configure a trunk for load-balancing, you should configure the member interfaces before you configure the trunk. After you configure the trunk, you should configure a policy route for it as well. (You might also have to configure criteria for the policy route.)
- [Section 5.5 on page 116](#) identifies the features (such as the criteria in a policy route, mentioned above) that are primarily used to store information used by other features.
- [Section 5.6 on page 117](#) introduces some of the tools available for system management.

5.1 Granular Configuration

ZyWALL configuration is granular. When you configure a feature, you may have to configure other screens first before you can finish configuring the feature. When you configure these other screens, you are configuring objects.

For example, when you set up a policy route, each criterion is an object. You should configure each criterion in a different screen before you configure the policy route itself. A policy route can have up to six criteria, so you might have to configure several screens before you finish the policy route.

Fortunately, when you finish, you can reuse the objects--without configuring them again--in other policy routes or in other features such as firewall rules or remote management.

For a list of common objects, see [Section 5.5 on page 116](#).

5.2 Terminology in the ZyWALL

This section highlights some differences in terminology or organization between the ZyWALL and other routers, particularly ZyNOS routers.

Table 23 ZyWALL Terminology That is Different Than ZyNOS

ZYNOS FEATURE / TERM	ZYWALL FEATURE / TERM
Port forwarding	Virtual server
IP alias	Virtual interface
Gateway policy	VPN gateway
Network policy (IPSec SA)	VPN connection

Table 24 ZyWALL Terminology That Might Be Different Than Other Products

FEATURE / TERM	ZYWALL FEATURE / TERM
Hub-and-spoke VPN	(VPN) concentrator

Table 25 NAT: Differences Between the ZyWALL and ZyNOS

ZYNOS FEATURE / SCREEN	ZYWALL FEATURE / SCREEN
Port forwarding	Virtual server
Trigger port, port triggering	Policy route
Address mapping	Policy route
Address mapping (VPN)	IPSec VPN

Table 26 Bandwidth Management: Differences Between the ZyWALL and ZyNOS

ZYNOS FEATURE / SCREEN	ZYWALL FEATURE / SCREEN
Interface bandwidth (outbound)	Interface
OSI level-7 bandwidth	Application patrol
General bandwidth	Policy route

5.3 Physical Ports, Interfaces, and Zones

If you want to configure the ZyWALL effectively, you should understand the differences between physical ports, interfaces, and zones. The following illustration provides an overview of the relationship between physical ports, interfaces, and zones in the ZyWALL. It also identifies the types of features you can configure with each one.

Table 27 Physical Ports, Interfaces, and Zones

Zones (LAN, DMZ, WAN, ...)	Used in firewall, IDP, and remote management
Interfaces (Ethernet, VLAN,...)	Used in VPN, device HA, DDNS, policy routes, static routes, HTTP redirect, and virtual server
Physical Ports (1, 2, 3, 4, 5)	Used in port groups.

A physical port is the place to which you connect the cable. As shown above, you do not usually configure physical ports to use various features. You configure interfaces and zones. The ZyWALL supports 1:1, 1:M, M:1, and M:N relationships between physical ports and interfaces.

There are many types of interfaces in the ZyWALL. In addition to being used in various features, interfaces also describe the network that is directly connected to the ZyWALL.

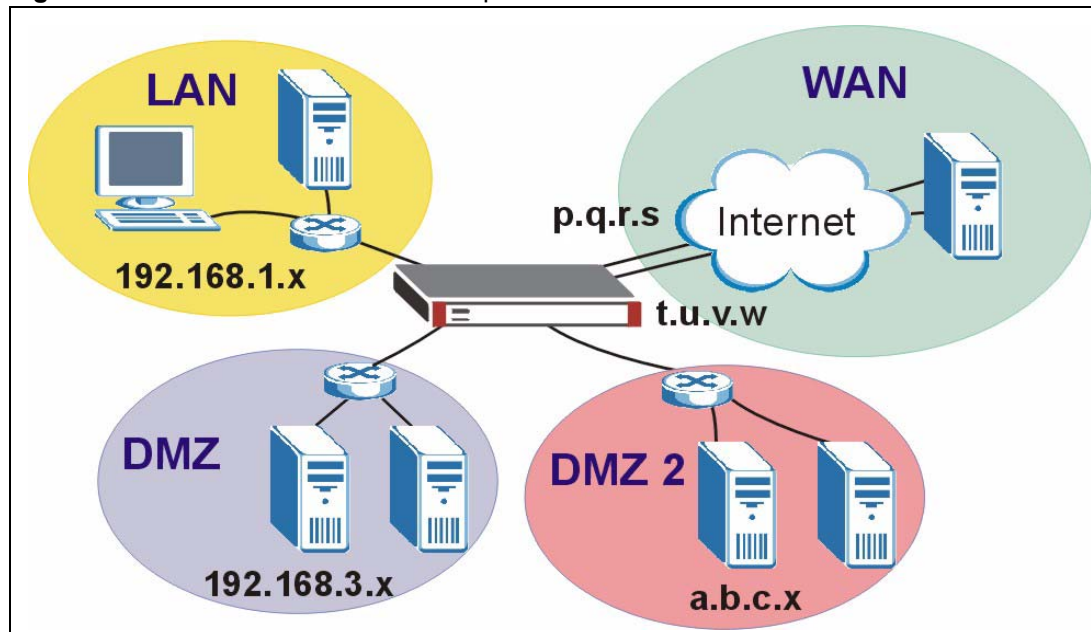
- **Port groups** create a hardware connection between physical ports at the layer-2 (MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. You also configure RIP and OSPF in these interfaces.
- **VLAN interfaces** recognize tagged frames. The ZyWALL automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Then, you can configure the IP address and subnet mask of the bridge. It is also possible to configure zone-level security between the member interfaces in the bridge.
- **PPPoE/PPTP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Virtual interfaces** increase the amount of routing information in the ZyWALL. There are three types: **virtual Ethernet interfaces** (also known as IP alias), **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- The **auxiliary interface**, along with an external modem, provides an interface the ZyWALL can use to dial out. This interface can be used as a backup WAN interface, for example. The auxiliary interface controls the **DIAL BACKUP** port.

Zones are used for security policies. A zone is simply a group of interfaces and/or VPN tunnels; by default, the ZyWALL has LAN, WAN and DMZ zones. Each interface and VPN tunnel can be assigned to one and only one zone. You can add, change, or remove the interfaces and VPN tunnels in each zone without affecting the settings that are based on zones.

5.3.1 Network Topology Example

The following example is used to further explain the differences between interfaces and zones.

Figure 42 Interfaces and Zones: Example



- The LAN zone contains the **ge1** (Gigabit Ethernet 1) interface. This is a protected zone and uses private IP addresses. **ge1** uses 192.168.1.1 and the connected devices use IP addresses in the 192.168.1.2 to 192.168.1.254 range.
- The WAN zone contains interfaces **ge2** and **ge3**. They use public IP addresses to connect to the Internet.
- The DMZ zone contains interface **ge4**. The DMZ zone has servers that are available to the public. **ge4** uses private IP address 192.168.3.1 and the connected devices use private IP addresses in the 192.168.3.2 to 192.168.3.254 range.
- The DMZ-2 zone contains interface **ge5** and has servers that are available to the public. **ge5** and the connected servers use public IP addresses.

This example is also used in several examples in [Section 5.4 on page 108](#).

5.4 Feature Configuration Overview

This section provides information about configuring the main features in the ZyWALL. The features are listed in the same sequence as the menu item(s) in the web configurator. Each feature is organized as shown below.

Feature

This provides a brief description. See the appropriate chapter(s) in this User's Guide for more information about any feature.

MENU ITEM(S)	This shows you the sequence of menu items and tabs you should click to find the main screen(s) for this feature. See the User's Guide for information about each screen.
PREREQUISITES	These are other features you should configure before you configure the main screen(s) for this feature. In most cases, if you forget to configure one of the prerequisites first, you can still save your changes in the main screen. Then, you can configure the prerequisite and return to the main screen to finish configuring the feature. You may not have to configure everything in the list of prerequisites. For example, you do not have to create a schedule for a policy route unless time is one of the criterion.
WHERE USED	There are two uses for this. These are other features you should usually configure or check right after you configure the main screen(s) for this feature. For example, you should usually create a policy route for a VPN tunnel. You have to delete the references to this feature before you can delete any settings. For example, you have to delete (or modify) all the policy routes that refer to a VPN tunnel before you can delete the VPN tunnel.

Example: This provides a simple example to show you how to configure this feature. The example is usually based on the network topology in [Figure 42 on page 108](#).

Note: If there are no prerequisites or if there are no references in other features to this one, then the entry has been removed. For example, there are no references to DDNS entries, so there is no **Where Used** entry.

Interface

See [Section 5.3 on page 107](#) for background information.

Note: You have to assign interfaces to zones manually after you create an interface.

Most of the features that use interfaces support Ethernet, VLAN, bridge, and PPPoE/PPTP interfaces. You can only use virtual interfaces in IPSec VPN and device HA.

MENU ITEM(S)	Network > Interface (except Network > Interface > Trunk)
PREREQUISITES	OSPF (Ethernet interfaces), ISP accounts (PPPoE/PPTP interfaces)
WHERE USED	Zones, trunks, IPSec VPN, device HA, DDNS, policy routes, static routes, HTTP redirect, virtual server

Example: The **ge5** interface is in the DMZ-2 zone and uses a public IP address. To configure **ge5**'s settings, click **Configuration > Network > Interface > Ethernet** and then **ge5**'s **Edit** icon.

Trunks

Use trunks to set up load balancing using two or more interfaces.

MENU ITEM(S)	Network > Interface > Trunk
PREREQUISITES	Interfaces
WHERE USED	Policy routes

Example: See [Chapter 6 on page 119](#).

IPSec VPN

Use VPN to provide secure communication between two sites over the Internet or any insecure network that uses TCP/IP for communication. The ZyWALL also offers hub-and-spoke VPN.

MENU ITEM(S)	Network > IPSec VPN ; you can also use the VPN Setup Wizard , which handles most of the prerequisites for you.
PREREQUISITES	Interfaces, certificates (authentication), authentication methods (extended authentication), addresses (local network, remote network, NAT), to-ZyWALL firewall, firewall
WHERE USED	Policy routes, zones

Example: See [Chapter 6 on page 119](#).

Zones

See [Section 5.3 on page 107](#) for background information. A zone is a group of interfaces and VPN tunnels. The ZyWALL uses zones, not interfaces, in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each interface and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

When you create a zone, the ZyWALL does not create any firewall rules, assign an IDP profile, or configure remote management for the new zone.

MENU ITEM(S)	Network > Zone
PREREQUISITES	Interfaces, IPSec VPN
WHERE USED	Firewall, IDP, remote management

Example: For example, to create the DMZ-2 zone and add **ge5** as in the network topology example, click **Configuration > Network > Zone** and then the **Add** icon.

Device HA

Use device HA to create redundant backup gateways. The ZyWALL 1050 runs VRRP v2. You can only set up device HA with other ZyWALL 1050s running the same firmware version.

MENU ITEM(S)	Network > Device HA
PREREQUISITES	Interfaces (with a static IP address), to-ZyWALL firewall

Example: See [Chapter 6 on page 119](#).

DDNS

Dynamic DNS maps a domain name to a dynamic IP address. The ZyWALL helps maintain this mapping.

MENU ITEM(S)	Network > DDNS
PREREQUISITES	Interfaces

Policy Routes

Use policy routes to control the routing of packets through the ZyWALL's interfaces, trunks, and VPN connections. You also use policy routes for bandwidth management (out of the ZyWALL), port triggering, and general NAT on the source address. You have to set up the criteria, next-hops, and NAT settings in other screens first.

MENU ITEM(S)	Policy > Route > Policy Route
PREREQUISITES	Criteria: users, user groups, interfaces (incoming), IPSec VPN (incoming), addresses (source, destination), address groups (source, destination), schedules, services, service groups Next-hop: addresses (HOST gateway), IPSec VPN, trunks, interfaces NAT: addresses (translated address), services and service groups (port triggering)

Example: You have an FTP server connected to **ge 4** (in the DMZ zone). You want to limit the amount of FTP traffic that goes out from the FTP server through your WAN connection.

- 1 Create an address object for the FTP server (**Objects > Address**).
- 2 Click **Policy > Route** to go to the policy route configuration screen. Add a policy route.
- 3 Name the policy route.
- 4 Select the interface that the traffic comes in through (**ge4** in this example).
- 5 Select the FTP server's address as the source address.
- 6 You don't need to specify the destination address or the schedule.
- 7 For the service, select **FTP**.

- 8** For the **Next Hop** fields, select **Interface** as the **Type** if you have a single WAN connection or **Trunk** if you have multiple WAN connections.
- 9** Select the interface that you are using for your WAN connection (**ge2** and **ge3** are **WAN** interfaces by default). If you have multiple WAN connections, select the trunk.
- 10** Specify the amount of bandwidth FTP traffic can use. You may also want to set a low priority for FTP traffic.

Note: The ZyWALL checks the policy routes in the order that they are listed. So make sure that your custom policy route comes before any other routes that would also match the FTP traffic.

Static Routes

Use static routes to tell the ZyWALL about networks not directly connected to the ZyWALL.

MENU ITEM(S)	Policy > Route > Static Route
PREREQUISITES	Interfaces

Firewall

The firewall allows you to control traffic between or within zones. You might also configure the firewall to control traffic for virtual server (port forwarding) and policy routes (NAT). You can configure firewall rules based on schedules, specific users (or user groups), source or destination addresses (or address groups) and services (or service groups). Each of these must be configured in a different screen first.

To-ZyWALL firewall rules control access to the ZyWALL. By default, the firewall allows any computer from the LAN zone to access or manage the ZyWALL. The ZyWALL drops packets from the WAN or DMZ zone to the ZyWALL itself, except for Device HA and VPN traffic. Configure to-ZyWALL firewall rules for remote management..

MENU ITEM(S)	Policy > Firewall
PREREQUISITES	Zones, schedules, users, user groups, addresses (source, destination), address groups (source, destination), services, service groups

Example: Suppose you have a SIP proxy server connected to the DMZ-2 zone for VoIP calls. You could configure a firewall rule to allow VoIP sessions from the SIP proxy server on DMZ-2 to the LAN so VoIP users on the LAN can receive calls.

- 1** Create a VoIP service object for UDP port 5060 traffic (**Objects > Service**).
- 2** Create an address object for the VoIP server (**Objects > Address**).
- 3** Click **Policy > Firewall** to go to the firewall configuration.
- 4** Select from the **DMZ-2** zone to the **LAN** zone, and add a firewall rule using the items you have configured.
 - You don't need to specify the schedule or the user.

- In the **Source** field, select the address object of the VoIP server.
- You don't need to specify the destination address.
- Leave the **Access** field set to **Allow** and the **Log** field set to **No**.

Note: The ZyWALL checks the firewall rules in order. Make sure this rule is in the correct place in the sequence.

Application Patrol

Use application patrol to control which individuals can use which services through the ZyWALL (and when they can do so). You can also specify allowed amounts of bandwidth.

MENU ITEM(S)	Policy > Application Patrol
PREREQUISITES	Schedules, users, user groups, addresses (source, destination), address groups (source, destination). These are only used as criteria in exceptions and conditions.

Example: Suppose you want to allow vice president Bob to use BitTorrent and block everyone else from using it.

- 1 Create a user account for Bob (**User/Group**).
- 2 Click **Policy > App. Patrol** to go to the application patrol configuration screen. Click the BitTorrent application patrol entry's **Edit** icon.
 - Set the default policy for access to **Drop**.
 - Add an exception policy.
 - Select the user account that you created for Bob.
 - You can leave the source, destination and log settings at the default.

Note: With this example, Bob would have to log in using his account. If you do not want him to have to log in, you might create an exception policy with Bob's computer IP address as the source.

IDP

Use IDP to detect and take action on malicious or suspicious packets and traffic flows. You must subscribe to use IDP. You can subscribe using the menu item or using one of the wizards.

MENU ITEM(S)	Policy > IDP
PREREQUISITES	Registration, zones

Content Filter

Use content filtering to block or allow access to specific categories of web site content, individual web sites and web features (such as cookies). You can define which user accounts (or groups) can access what content and at what times. You must have a subscription in order to use the category-based content filtering. You can subscribe using the menu item or using one of the wizards.

MENU ITEM(S)	Policy > Content Filter
PREREQUISITES	Registration, addresses (source), schedules, users, user groups

Example: You can configure a policy that blocks Bill's access to arts and entertainment web pages during the workday.

- 1 Create a user account for Bill if you have not done so already (**User/Group**).
- 2 Create a schedule for the work day (**Objects > Schedule**).
- 3 Click **Policy > Content Filter > Filtering Profile > Categories** to go to the screen where you can configure a category-based profile.
- 4 Name the profile and enable it.
- 5 You also need to decide what to do for matched web sites (**Block** in this example), unrated web sites and what to do when the category-based content filtering service is not available.
- 6 Select the **Arts/Entertainment** category (you need to click **Advanced** to display it).
- 7 Click **Policy > Content Filter** to go to the content filter general configuration screen.
- 8 Enable the content filter.
- 9 Add a policy that uses the schedule, the filtering profile and the user that you created.

Virtual Server (Port Forwarding)

Use this to change the address and/or port number of packets coming in from a specified interface. This is also known as port forwarding.

The ZyWALL does not check to-ZyWALL firewall rules for packets that are redirected by virtual server. It does check regular (through-ZyWALL) firewall rules.

MENU ITEM(S)	Policy > Virtual Server
PREREQUISITES	Interfaces, addresses (HOST)

Example: Suppose you have an FTP server with a private IP address connected to a DMZ port. You could configure a virtual server rule to forwards FTP sessions from the WAN to the DMZ.

- 1 Click **Policy > Virtual Server** to configure the virtual server. Add an entry.

- 2 Name the entry.
- 3 Select the WAN interface that the FTP traffic is to come in through (in this example, **ge2** or **ge3**.)
- 4 Specify the public WAN IP address where the ZyWALL will receive the FTP packets.
- 5 In the **Mapped IP field**, list the IP address of the FTP server. The ZyWALL will forward the packets received for the original IP address.
- 6 In **Mapping Type**, select **Port**.
- 7 Enter 21 in both the **Original** and the **Mapped Port** fields.

HTTP Redirect

Configure this feature to have the ZyWALL transparently forward HTTP (web) traffic to a proxy server. This can speed up web browsing because the proxy server keeps copies of the web pages that have been accessed so they are readily available the next time one of your users needs to access that page.

The ZyWALL does not check to-ZyWALL firewall rules for packets that are redirected by HTTP redirect. It does check regular (through-ZyWALL) firewall rules.

MENU ITEM(S)	Policy > HTTP Redirect
PREREQUISITES	Interfaces

Example: Suppose you want HTTP requests from your LAN to go to a HTTP proxy server at IP address 192.168.3.80.

- 1 Click **Policy > HTTP Redirect**.
- 2 Add an entry.
- 3 Name the entry.
- 4 Select the interface from which you want to redirect incoming HTTP requests (**ge1** is a LAN interface by default).
- 5 Specify the IP address of the HTTP proxy server.
- 6 Specify the port number to use for the HTTP traffic that you forward to the proxy server.

VoIP PassThru

The ZyWALL's Application Layer Gateway (ALG) allows VoIP applications to go through NAT on the ZyWALL.

MENU ITEM(S)	Policy > VoIP PassThru
---------------------	----------------------------------

User/Group

Use these screens to configure the ZyWALL's administrator and user accounts. The ZyWALL provides the following user types.

TYPE	ABILITIES
Admin	Change ZyWALL configuration (web, CLI)
Limited-Admin	Look at ZyWALL configuration (web)
User	Access network services, browse user-mode commands (CLI)
Guest	Access network services
Ext-User	The same as a User or a Guest. The ZyWALL looks for the specific type in an external authentication server. If the type is not available, the ZyWALL applies default settings.

If you want to force users to log in to the ZyWALL before the ZyWALL routes traffic for them, you might have to configure prerequisites first.

User accounts and user groups can also be used in a lot of features. See section 5.5 for more information.

MENU ITEM(S)	User/Group
PREREQUISITES	Addresses, address groups, schedules. The prerequisites are only used in policies to force user authentication
Where Used	Policy routes, firewall, application patrol, content filter, user groups

5.5 Objects

Objects store information and are referenced by other features. If you update this information in response to changes, the ZyWALL automatically propagates the change through the features that use the object.

The following table introduces the objects. You can find most of these objects in the **Object** menu. There are a couple menu items from **Network (ISP Account, Routing Protocol)** and **User/Group** as well. You can also use this table when you want to delete an object because you have to delete references to the object first.

OBJECT	WHERE USED
addresses	VPN connections (local / remote network, NAT), policy routes (criteria, next-hop [HOST], NAT), firewall, application patrol (source, destination), content filter, virtual server (HOST), user settings (force user authentication), address groups, remote management (System)
address groups	Policy routes (criteria), firewall, application patrol (source, destination), content filter, user settings (force user authentication), address groups, remote management (System)
services, service groups	Policy routes (criteria, port triggering), firewall, service groups, log (criteria)

OBJECT	WHERE USED
schedules	Policy routes (criteria), firewall, application patrol, content filter, user settings (force user authentication)
AAA server	Authentication methods
authentication methods	VPN gateways (extended authentication), WWW (client authentication)
certificates	VPN gateways, WWW, SSH, FTP

5.6 System Management

This section introduces some of the management and maintenance features in the ZyWALL. Use **Host Name** to configure the system and domain name for the ZyWALL. Use **Date/Time** to configure the current date, time, and time zone in the ZyWALL. Use **Console Speed** to set the console speed.

DNS, WWW, SSH, TELNET, FTP, SNMP

Use these screens to set which services or protocols can be used to access the ZyWALL through which zone and from which addresses (address objects) the access can come.

MENU ITEM(S)	System > DNS, WWW, SSH, TELNET, FTP, SNMP
PREREQUISITES	To-ZyWALL firewall, zones, addresses, address groups, certificates (WWW, SSH, FTP), authentication methods (WWW)

Example: Suppose you want to allow an administrator to use HTTPS to manage the ZyWALL from the WAN.

- 1** Create an administrator account (**User/Group**).
- 2** Create an address object for the administrator's computer (**Objects > Address**).
- 3** Click **System > WWW** to configure the HTTP management access. Enable HTTPS and add an administrator service control entry.
 - Select the address object for the administrator's computer.
 - Select the **WAN** zone.
 - Set the action to **Accept**.

File Manager

Use these screens to upload, download, delete, or run scripts of CLI commands. You can manage

- Configuration files. Use configuration files to back up and restore the complete configuration of the ZyWALL. You can store multiple configuration files in the ZyWALL and switch between them without restarting.

- Shell scripts. Use shell scripts to run a series of CLI commands. These are useful for large, repetitive configuration changes (for example, creating a lot of VPN tunnels) and for troubleshooting.

You can edit configuration files and shell scripts in any text editor.

MENU ITEM(S)	File Manager
---------------------	---------------------

Registration

Use these screens to register your ZyWALL or to subscribe to the IDP or content filtering services. You must have Internet access to myZyXEL.com.

MENU ITEM(S)	Registration
PREREQUISITES	Internet access to myZyXEL.com

Logs and Reports

The ZyWALL provides a system log, offers two e-mail profiles to which to send log messages, and sends information to four syslog servers. It also provides three types of statistical reports to track user activity and web site hits.

MENU ITEM(S)	Maintenance > Logs, Reports
---------------------	---------------------------------------

CHAPTER 6

Tutorials

This chapter provides some examples of using the web configurator to set up features in the ZyWALL.

6.1 Interfaces and Zones

The following example shows how to use port grouping, Ethernet interfaces, trunks, and zones to set up the following configuration.

Table 28 Interfaces and Zones Example

PHYSICAL PORT	ETHERNET INTERFACE	SETTINGS	TRUNK	ZONE
1	ge1	192.168.1.1/24, DHCP server	---	LAN
2	ge1	---	---	---
3	ge3	172.23.19.244/24	WAN_TRUNK	WAN
4	ge4	DHCP client	WAN_TRUNK	WAN
5	ge5	192.168.10.10/24, DHCP server	---	DMZ

In this example, ge2 does not have any physical ports assigned to it. The example begins with the following interface configuration.

Figure 43 Status > Interface Status Summary, Initial

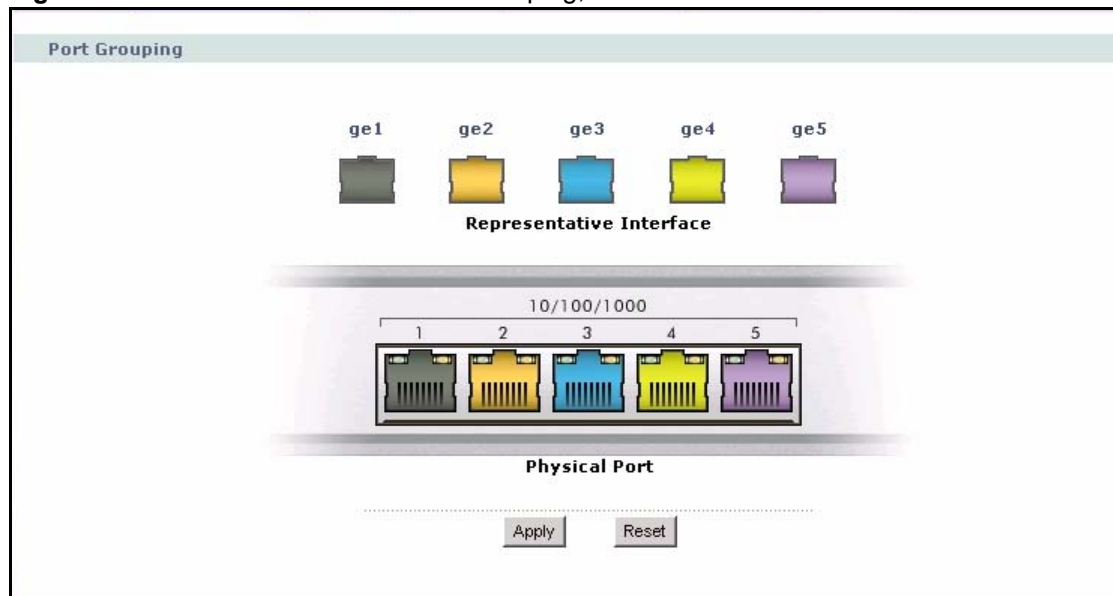
Interface Status Summary								Expand
Name	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Renew/Dial	
ge1	100M/Full	n/a	LAN	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a	
ge2	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew	
ge3	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew	
ge4	Down	n/a	DMZ	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew	
ge5	Down	n/a	DMZ	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew	
aux	Disconnected	n/a	n/a	10.64.64.76 / 255.255.255.255	Dynamic	n/a	<HD>	

6.1.1 Set up Port Grouping

This example creates a port group in ge1 by adding physical port 2 to representative interface ge1. There are no existing port groups.

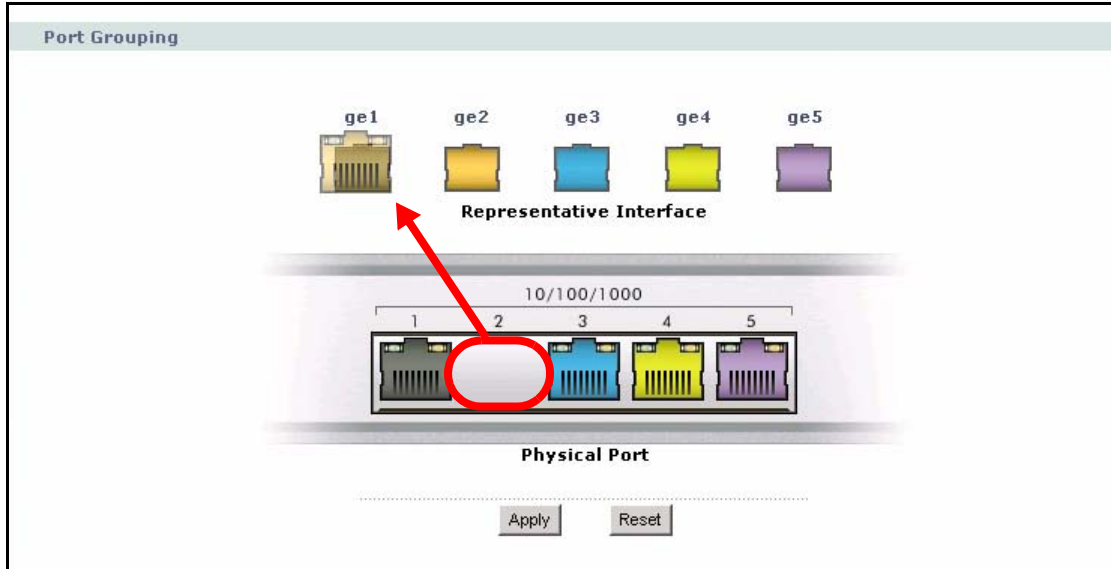
- 1 Click **Network > Interface > Port Grouping**. The following screen appears.

Figure 44 Network > Interface > Port Grouping, Initial



- 2 Drag physical port 2 onto representative interface **ge1**, as shown below.

Figure 45 Network > Interface > Port Grouping, Drag-and-Drop



3 Click **Apply**.

4 Click **Status**, and scroll down to the **Interface Status Summary**, shown below. Ethernet interface ge1 has a status of **Port Group Up**, and Ethernet interface ge2 is disabled and has a **Status** of **Port Group Inactive**.

Figure 46 Status > Interface Status Summary, After Port Grouping

Interface Status Summary								Expand
Name	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Renew/Dial	
ge1	Port Group Up	n/a	LAN	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a	
ge2	Port Group Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	n/a	
ge3	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew	
ge4	Down	n/a	DMZ	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew	
ge5	Down	n/a	DMZ	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew	
aux	Disconnected	n/a	n/a	10.64.64.76 / 255.255.255.255	Dynamic	n/a	<HD>	

6.1.2 Set up Ethernet Interfaces

This example sets up the Ethernet interfaces as shown below.

Table 29 Ethernet Interfaces Example

ETHERNET INTERFACE	SETTINGS
ge1	192.168.1.1/24, DHCP server
ge3	172.23.19.244/24

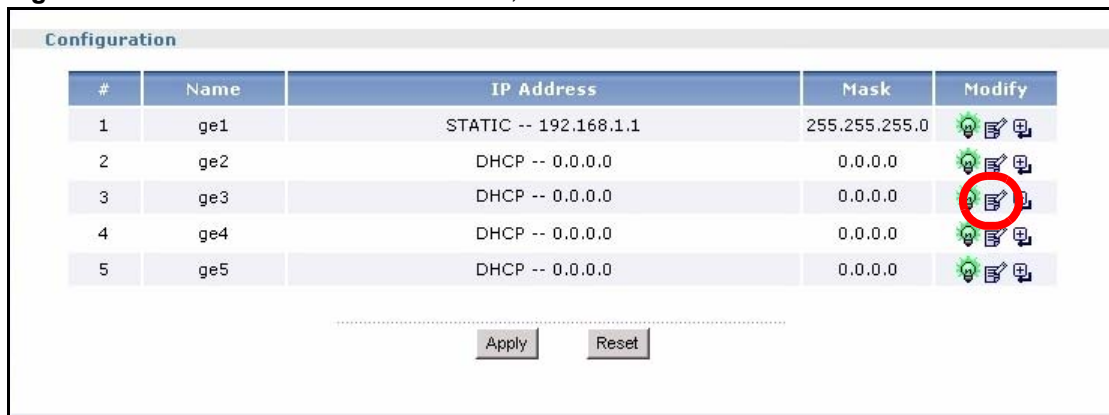
Table 29 Ethernet Interfaces Example (continued)

ETHERNET INTERFACE	SETTINGS
ge4	DHCP client
ge5	192.168.10.10/24, DHCP server

You have decided to use the default settings for ge1 and ge4, so it is not necessary to edit these interfaces. You can also skip ge2 because there are no physical ports associated with it anymore. Therefore, the following steps set up ge3 and ge5.

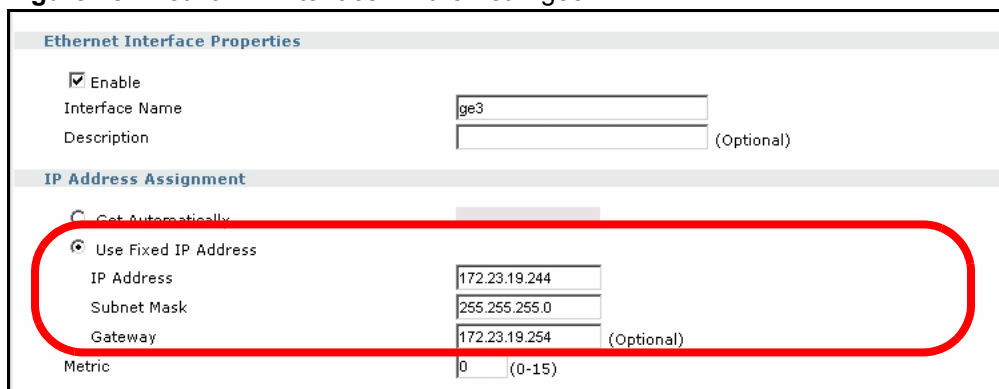
- 1 Click **Network > Interface > Ethernet**. The following screen appears.

Figure 47 Network > Interface > Ethernet, Initial



- 2 Click the **Edit** icon for ge3, as shown above, and set up the IP address as shown below.

Figure 48 Network > Interface > Ethernet > ge3



- 3 Use the default values for the rest of the settings. Click **Apply** to save these changes and return to the previous screen. Click the **Edit** icon for ge5, and set up the IP address as shown below.

Figure 49 Network > Interface > Ethernet > ge5 > IP Address Assignment

Ethernet Interface Properties	
<input checked="" type="checkbox"/> Enable	
Interface Name	ge5
Description	<input type="text"/> (Optional)
IP Address Assignment	
<input type="radio"/> Get Automatically	<input type="text"/>
<input checked="" type="radio"/> Use Fixed IP Address	
IP Address	192.168.10.10
Subnet Mask	255.255.255.0
Gateway	<input type="text"/> (Optional)
Metric	0 (0-15)

- 4 Scroll down to the **DHCP Setting** section, and set up the DHCP server for ge5, as shown below.

Figure 50 Network > Interface > Ethernet > ge5 > DHCP Setting

DHCP Setting	
DHCP	<input type="checkbox"/> DHCP Server
IP Pool Start Address (Optional)	192.168.10.33
Pool Size	32
First DNS Server (Optional)	Custom Defined
Second DNS server (Optional)	Custom Defined
Third DNS Server (Optional)	Custom Defined
Lease time	<input type="radio"/> infinite
	<input checked="" type="radio"/> 3 days 0 hours (Optional) 0 minutes
Static DHCP Table	<input type="button" value="Add Static DHCP"/>

- 5 Use the default values for the rest of the settings. Click **Apply** to save these changes and return to the previous screen. Click **Status**, and scroll down to the **Interface Status Summary**, shown below. In this example, you have already connected ge3 to the Internet as well.

Figure 51 Status > Interface Status Summary, After Ethernet Interfaces

Interface Status Summary								Expand
Name	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Renew/Dial	
ge1	Port Group Up	n/a	LAN	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a	
ge2	Port Group Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	n/a	
ge3	100M/Full	n/a	WAN	172.23.19.244 / 255.255.255.0	Static	n/a	n/a	
ge4	Down	n/a	DMZ	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew	
ge5	Down	n/a	DMZ	192.168.10.10 / 255.255.255.0	Static	DHCP server	n/a	
aux	Disconnected	n/a	n/a	10.04.04.70 / 255.255.255.255	Dynamic	n/a	<D>	

6.1.3 WAN Trunk

This example sets up trunk WAN_TRUNK with ge3 and ge4. This example uses the default settings for the trunk and shows how to add the interfaces to it.

Table 30 Trunk Example

ETHERNET INTERFACE	TRUNK
ge1	---
ge3	WAN_TRUNK
ge4	WAN_TRUNK
ge5	---

There are no existing trunks at the beginning of this example.

- 1 Click **Network > Interface > Trunk**. The following screen appears.

Figure 52 Network > Interface > Trunk, Initial

Name	Algorithm	

- 2 Click the **Add** icon. The following screen appears.

Figure 53 Network > Interface > Trunk > add, Initial

Group Members

Name

Load Balancing Algorithm Least Load First

#	Member	Mode	Downstream Bandwidth	Upstream Bandwidth	

OK Cancel

- 3** Enter the name **WAN_TRUNK**, select **Least Load First** for the load balancing algorithm (used in this example), and click the **Add** icon, as shown above. A new member appears, as shown below.

Figure 54 Network > Interface > Trunk > add, Add Member

Group Members

Name

Load Balancing Algorithm Least Load First

#	Member	Mode	Downstream Bandwidth	Upstream Bandwidth	
1	ge1	Active	1048576 Kbps	1048576 Kbps	

OK Cancel

- 4** Click the **Popup** icon next to **ge1**, as shown above. The **Popup** window appears, as shown below.

Figure 55 Network > Interface > Trunk > add, Edit Member

Group Members

Name

Load Balancing Algorithm Least Load First

#	Member	Mode	Downstream Bandwidth	Upstream Bandwidth	
1	ge1	Active	1048576 Kbps	1048576 Kbps	

GoTo: 1 Page 1/1

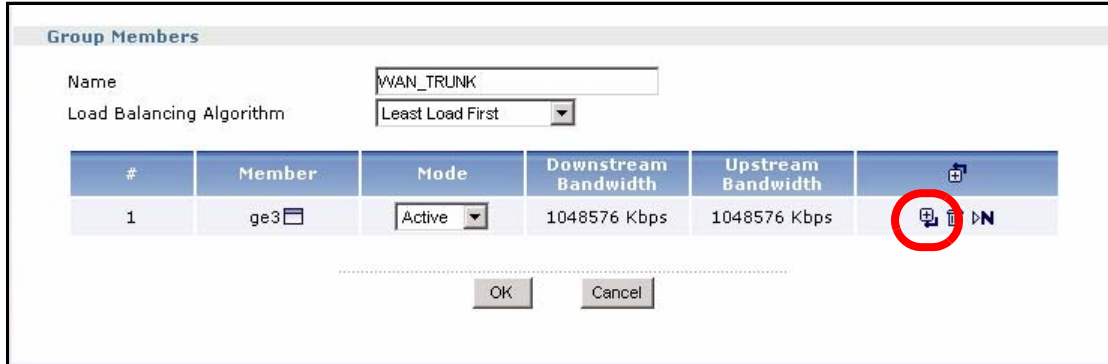
Please select one Member.

aux	hwt	ge1
ge2	ge3	ge4
ge5	ppp0	vlan1

OK Cancel

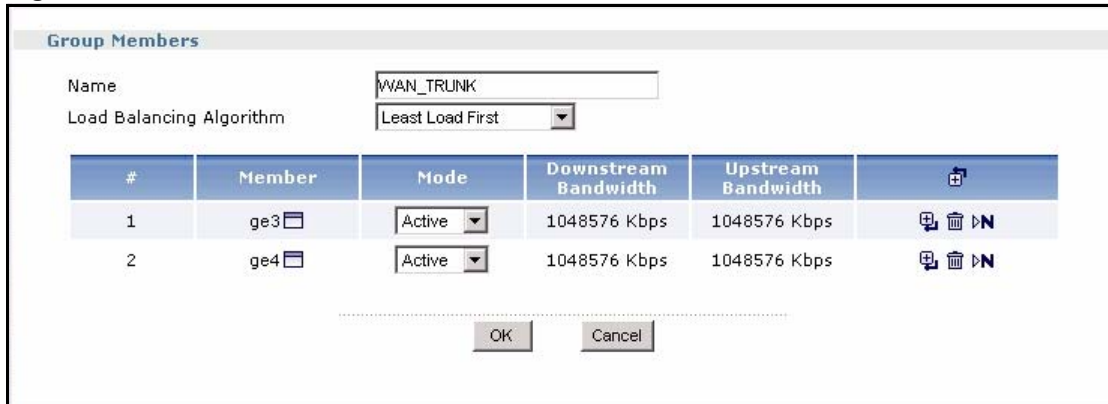
- 5** Select **ge3**, and click **OK**, as shown above.

Figure 56 Network > Interface > Trunk > add, Member ge3



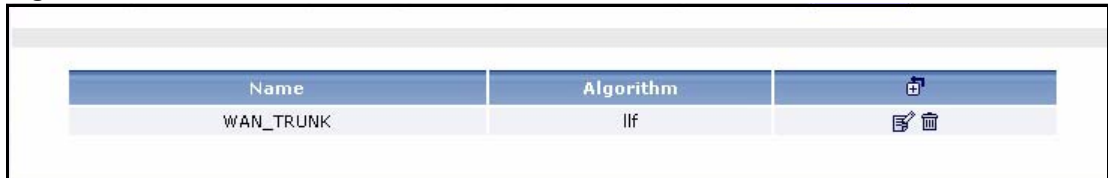
6 Click the **Add** icon for **ge3**, as shown above, and repeat steps 4-5 to add ge4. The screen then appears as shown below.

Figure 57 Network > Interface > Trunk > add, Final



7 Use the default values for the rest of the settings. Click **OK** to save these changes and return to the previous screen.

Figure 58 Network > Interface > Trunk, Final



8 Next, set up a policy route for the trunk. Click **Policy > Route > Policy Route**, and click the **Add** icon.

9 Change the **Incoming** field to ge1. By default, there is an address object called LAN_SUBNET with the same settings as ge1 (192.168.1.0/24). Select it in the **Source Address** field. In the **Next-Hop** section, select **Trunk**, and then select WAN_TRUNK. Finally, select **outgoing-interface** in the **Source Network Address Translation** field to set up NAT, and click **OK**.

Figure 59 Policy > Route > Policy Route

Configuration									
<input checked="" type="checkbox"/> Enable									
Description	<input type="text"/> (Optional)								
Criteria									
User	any								
Incoming	Interface / ge1 <input type="button" value="Change..."/>								
Source Address	LAN_SUBNET								
Destination Address	any								
Schedule	none								
Service	any <input type="button" value="New..."/>								
Next-Hop									
Type	Trunk								
Gateway									
Interface	ge1								
VPN Tunnel									
Trunk	WAN_TRUNK								
Address Translation									
Source Network Address Translation	outgoing-interface								
Port Triggering	<table border="1"> <thead> <tr> <th>#</th> <th>Incoming Service</th> <th>Trigger Service</th> <th><input type="button" value="Add"/></th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>	#	Incoming Service	Trigger Service	<input type="button" value="Add"/>				
#	Incoming Service	Trigger Service	<input type="button" value="Add"/>						

10 Click **Status**, and scroll down to the **Interface Status Summary**, shown below. There should be no change.

Figure 60 Status > Interface Status Summary, After Trunks

Interface Status Summary								Expand
Name	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Renew/Dial	
ge1	Port Group Up	n/a	LAN	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a	
ge2	Port Group Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	n/a	
ge3	100M/Full	n/a	WAN	172.23.19.244 / 255.255.255.0	Static	n/a	n/a	
ge4	Down	n/a	DMZ	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew	
ge5	Down	n/a	DMZ	192.168.10.10 / 255.255.255.0	Static	DHCP server	n/a	
aux	Disconnected	n/a	n/a	10.64.64.76 / 255.255.255.255	Dynamic	n/a	<D>	

6.1.4 Zones

This example sets up the LAN, WAN, and DMZ zones as shown below.






Table 31 Zones Example

ETHERNET INTERFACE	DEFAULT ZONE	FINAL ZONE
ge1	LAN	LAN
ge2	WAN	---
ge3	WAN	WAN
ge4	DMZ	WAN
ge5	DMZ	DMZ

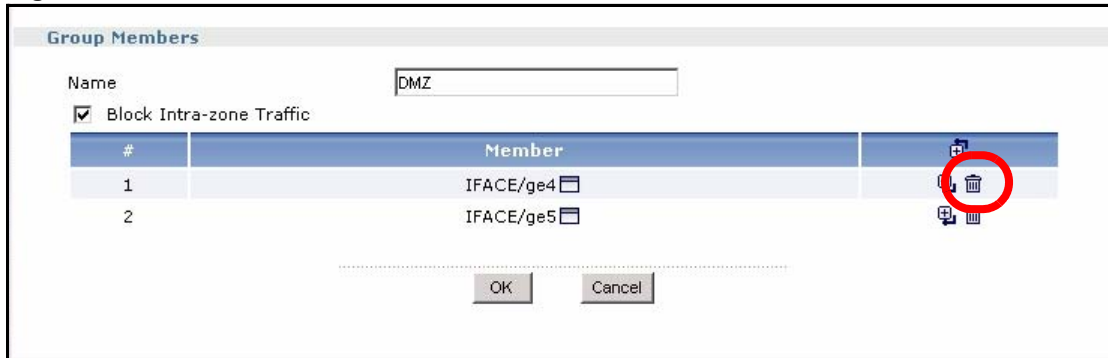
Ethernet interface ge2 does not have any physical ports associated with it, so it does not matter to which zone it is assigned or if it is assigned to any zone at all. The only change you must make is to remove ge4 from the DMZ zone and add it to the WAN zone. The following steps accomplish this by removing ge4 from the DMZ zone and changing WAN member ge2 into ge4, leaving ge2 unassigned to any zone.

- 1 Click **Network > Zone**. The following screen appears.

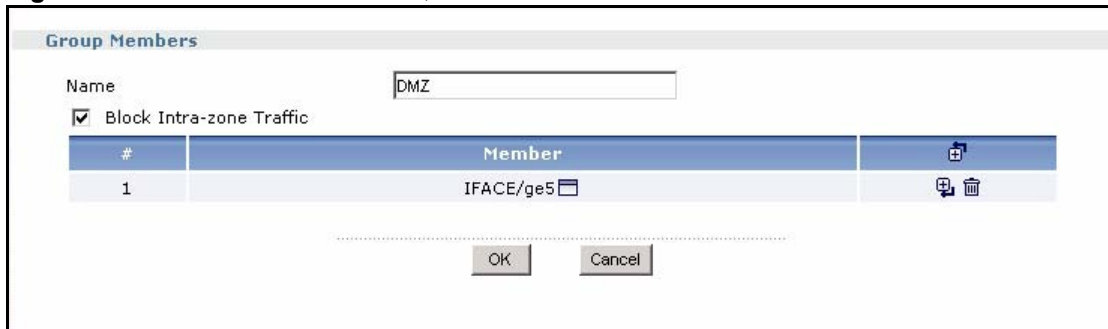
Figure 61 Network > Zone, Initial

Configuration		
Name	Block Intra-zone Traffic	
LAN	No	
WAN	Yes	 
DMZ	Yes	 

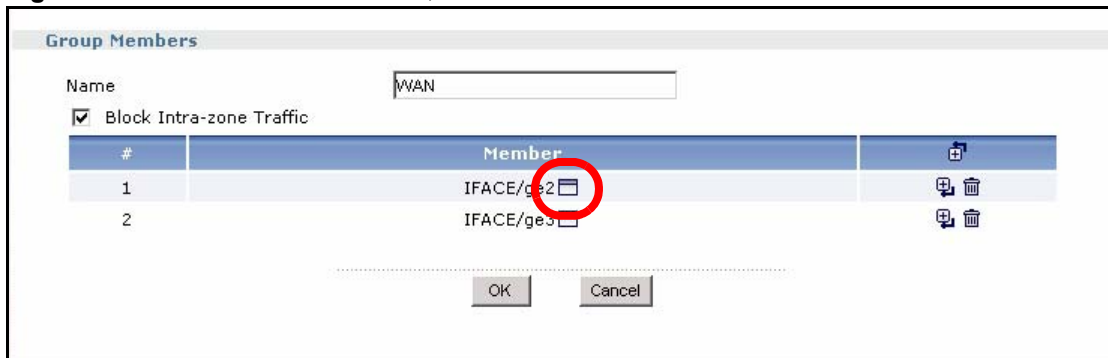
- 2 Click the **Edit** icon for **DMZ**, as shown above, because you have to remove ge4 from the DMZ before you can add it to the WAN.

Figure 62 Network > Zone > DMZ, Initial

- 3** Click the **Remove** icon for **ge4**, as shown above. A message box appears, confirming that you want to remove ge4. Click **OK** in this message box. The screen is updated, as shown below.

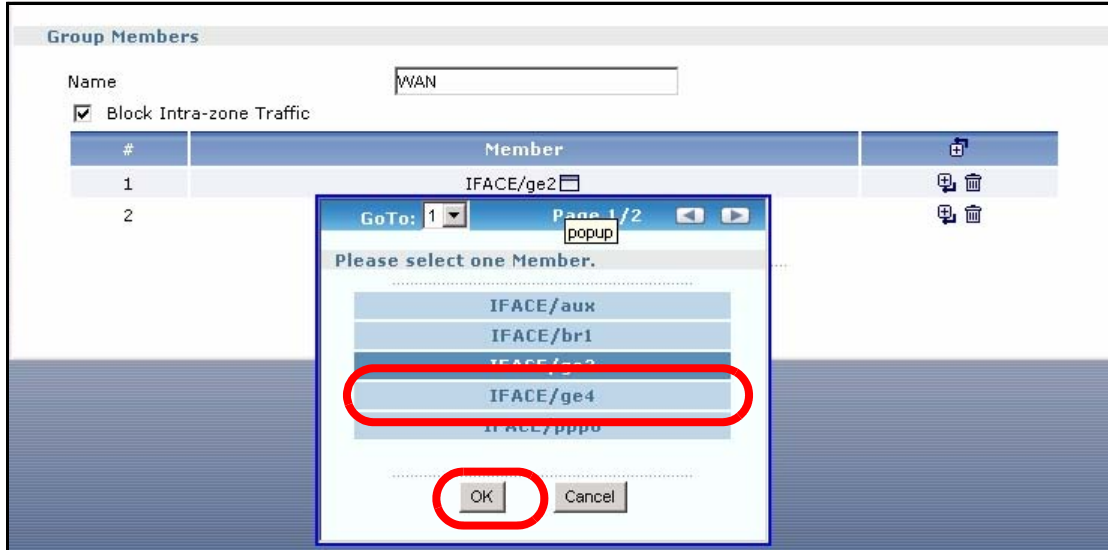
Figure 63 Network > Zone > DMZ, Final

- 4** Keep the default value for **Block Intra-Zone Traffic**, and click **OK** to save these changes and return to the previous screen. Click the **Edit** icon for **WAN**. The following screen appears.

Figure 64 Network > Zone > WAN, Initial

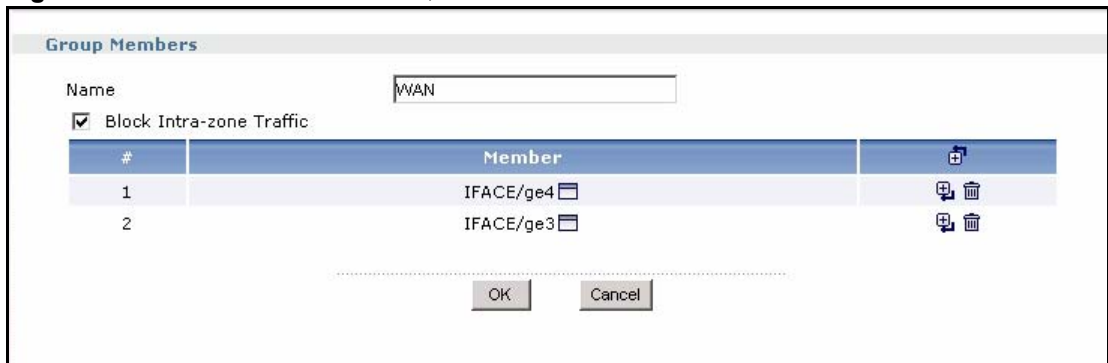
- 5** Click the **Popup** icon next to ge2, as shown above.

Figure 65 Network > Zone > WAN, Edit Member



6 Select **ge4**, and click **OK**, as shown above.

Figure 66 Network > Zone > WAN, Final



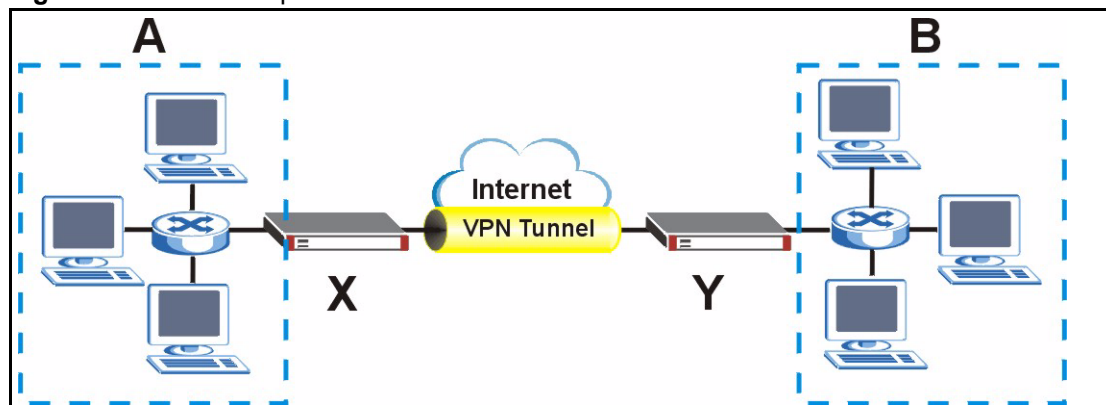
7 Keep the default value for **Block Intra-Zone Traffic**, and click **OK** to save these changes and return to the previous screen. Click **Status**, and scroll down to the **Interface Status Summary**, shown below.

Figure 67 Status > Interface Status Summary, After Zones

Interface Status Summary								Expand
Name	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Renew/Dial	
ge1	Port Group Up	n/a	LAN	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a	
ge2	Port Group Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	DHCP client	n/a	n/a	
ge3	100M/Full	n/a	WAN	172.23.19.244 / 255.255.255.0	Static	n/a	n/a	
ge4	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew	
ge5	Down	n/a	DMZ	192.168.10.10 / 255.255.255.0	Static	DHCP server	n/a	
aux	Disconnected	n/a	n/a	10.64.64.76 / 255.255.255.255	Dynamic	n/a	<D>	

6.2 VPN

This example is going to show you how to create the VPN tunnel illustrated below.

Figure 68 VPN Example

In this example, the ZyWALL is router X (220.123.123.2/24), and the remote IPsec router is router Y (220.123.143.10/24). Create the VPN tunnel between our local network A (192.168.10.0/24) and the remote network B (192.168.1.0/24).

The ZyWALL has its default settings.

6.2.1 Set up the Ethernet Interfaces

ge1 is connected to the local network, and ge3 is connected to the Internet. You have to configure both of them because the default settings are different. The other interfaces are not connected, so you can ignore them. Configure ge3 first. Then, after you configure ge1, you have to log in again.

- 1 Click **Network > Interface > Ethernet**. Click the **Edit** icon for ge3.
- 2 Change the IP address to a static IP address, and set up the static IP address (220.123.123.2/24) using the information provided by the ISP. Click **OK**.

Figure 69 Network > Interface > Ethernet > ge3 > IP Address

The screenshot shows the 'Ethernet Interface Properties' and 'IP Address Assignment' sections for interface 'ge3'. The 'Enable' checkbox is checked. The 'Interface Name' is 'ge3'. Under 'IP Address Assignment', 'Use Fixed IP Address' is selected. The 'IP Address' field contains '220.123.123.2', which is circled in red. The 'Subnet Mask' is '255.255.255.0' and the 'Gateway' is '220.123.123.254' (Optional). The 'Metric' is '0' (0-15).

- 3 In **Network > Interface > Ethernet**, click the **Edit** icon for ge1.
- 4 Change the static IP address to 192.168.10.1.

Figure 70 Network > Interface > Ethernet > ge1 > IP Address

The screenshot shows the 'Ethernet Interface Properties' and 'IP Address Assignment' sections for interface 'ge1'. The 'Enable' checkbox is checked. The 'Interface Name' is 'ge1'. Under 'IP Address Assignment', 'Use Fixed IP Address' is selected. The 'IP Address' field contains '192.168.10.1', which is circled in red. The 'Subnet Mask' is '255.255.255.0' and the 'Gateway' is empty (Optional). The 'Metric' is '0' (0-15).

- 5 The DHCP server is active, and you have to keep the **IP Pool Start Address** in the same subnet as the interface. Change it to 192.168.10.33. Click **OK**.

Figure 71 Network > Interface > Ethernet > ge1 > DHCP Settings

The screenshot shows the 'DHCP Setting' section for interface 'ge1'. The 'DHCP Server' dropdown is set to 'DHCP Server'. The 'IP Pool Start Address (Optional)' field contains '192.168.10.33', which is circled in red. The 'Pool Size' is '200'. The 'First DNS Server (Optional)' and 'Second DNS server (Optional)' are both set to 'From ISP'. The 'Third DNS Server (Optional)' is set to 'Custom Defined'. The 'Lease time' is set to '2' days, '0' hours, and '0' minutes. There is an 'Add Static DHCP' button at the bottom.

Release the old IP address the ZyWALL assigned to your computer (192.168.1.0/24), and renew the IP address again so that the ZyWALL assigns you an IP address in the new subnet (192.168.10.0/24). Go to <http://192.168.10.1> to log in to the ZyWALL again.

By default, there is an address object called LAN_SUBNET, whose subnet is the same as that of ge1 (192.168.1.0/24). It is used by a policy route for the default trunk WAN_TRUNK. Normally, you should either delete these objects or change LAN_SUBNET to 192.168.10.0/24. In this example, ignore all these objects.

6.2.2 Set up the Zones for the Ethernet Interfaces

Use the default zone settings for this example. ge1 is in the LAN zone, and ge3 is in the WAN zone.

6.2.3 Set up the VPN Gateway

The VPN gateway manages the IKE SA. You do not have to set up any other objects before you configure the VPN gateway because this VPN tunnel does not use any certificates or extended authentication.

- 1 Click **Network > IPSec VPN > VPN Gateway**, and then click the **Add** icon.
- 2 Give the VPN gateway a name (“VPN_GW_143”). Use the default proposal settings in this example--DES encryption, MD5 authentication, and DH1 key group. In the **Property** section, select ge3 in the **Interface** field, and enter 220.123.143.10 in the first **Secure Gateway Address** field. In the **Authentication Method** section, the pre-shared key is 12345678, and the routers are using each other's IP addresses for authentication. Click **OK**.

Figure 72 Network > IPSec VPN > VPN Gateway > add

The screenshot shows the configuration page for a new VPN Gateway. The 'Property' section has 'Interface' set to 'ge3' and 'Secure Gateway Address' with '1. 220.123.143.10' entered. The 'Authentication Method' section has 'Pre-Shared Key' selected with '12345678' entered, and 'Local ID Type' set to 'IP' with '220.123.123.2' entered. The 'Peer ID Type' is also set to 'IP' with '220.123.143.10' entered. Red circles highlight the 'ge3' dropdown, the '220.123.143.10' input, and the 'Pre-Shared Key' and 'Local ID Type' fields.

6.2.4 Set up the VPN Connection

The VPN connection manages the IPSec SA. You have to set up the address objects for the local network and remote network before you can set up the VPN connection.

- 1 Click **Object > Address > Address**. Click the **Add** icon.
- 2 Give the new address object a name (“VPN_LOCAL_SUBNET”), change the **Address Type** to **SUBNET**, and set up the rest of the fields to 192.168.10.0/24. Click **OK**.

Figure 73 Object > Address > Address > add

- 3** Repeat the process to create a new address object for the remote network (“VPN_REMOTE_SUBNET”, 192.168.1.0/24).
- 4** Click **Network > IPSec VPN > VPN Connection**. Click the **Add** icon.
- 5** Give the VPN connection a name (“VPN_CONN_143”), and select the VPN gateway (Section 6.2.3 on page 133) in the **VPN Gateway** section. Use the default proposal settings in this example--ESP, Tunnel encapsulation, DES encryption, and SHA1 authentication--so do not change these settings. In the **Policy** section, select the address objects for the local and remote networks. Click **OK**.

Figure 74 Network > IPSec VPN > VPN Connection > add

#	Encryption	Authentication	
1	DES	SHA1	

6.2.5 Set up the Policy Route for the VPN Tunnel

You should create a new policy route to use the VPN tunnel. This policy route will only use the existing address objects, so you do not have to create any additional objects first.

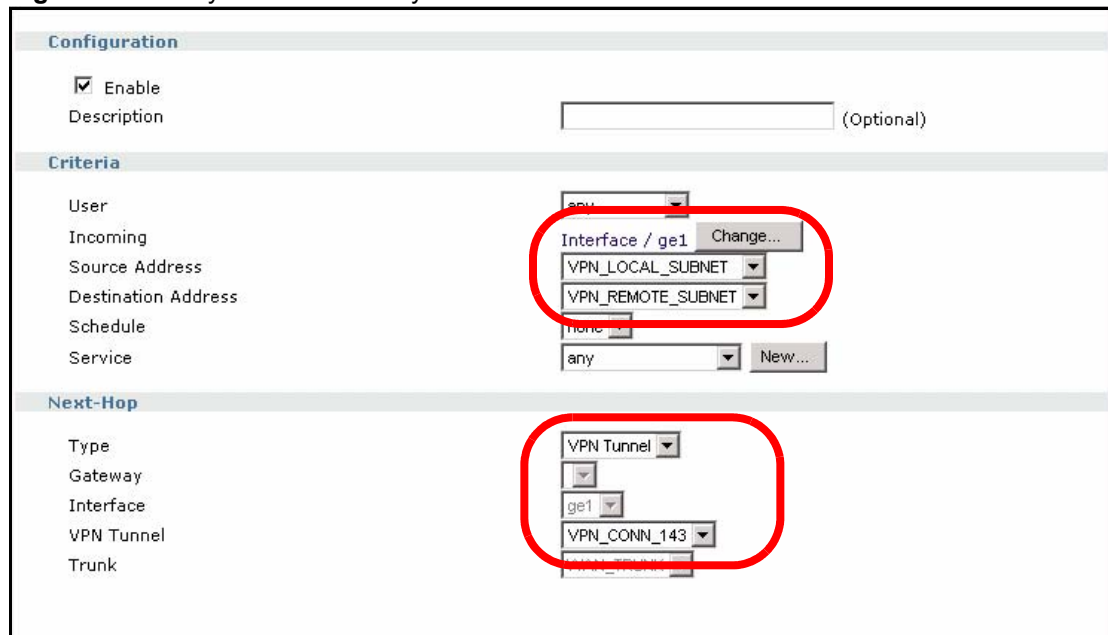
- 1 Click **Policy > Route > Policy Route**. You want this policy route to have higher priority than the default policy route for the trunk, so click the **Add** icon at the top of the column, not the one next to the existing policy route.

Figure 75 Policy > Route > Policy Route



- 2 This policy route applies to traffic from ge1. The source address and destination address must be the same ones represented by the address objects that you used in the VPN connection. The next-hop is the VPN connection that you created. Click **OK**.

Figure 76 Policy > Route > Policy Route > add



Because the new VPN connection has not been assigned to a zone yet, there are no restrictions (for example, firewall) on traffic to or from this VPN connection. You should set up the VPN settings on the remote IPSec router and try to establish the VPN tunnel before continuing.

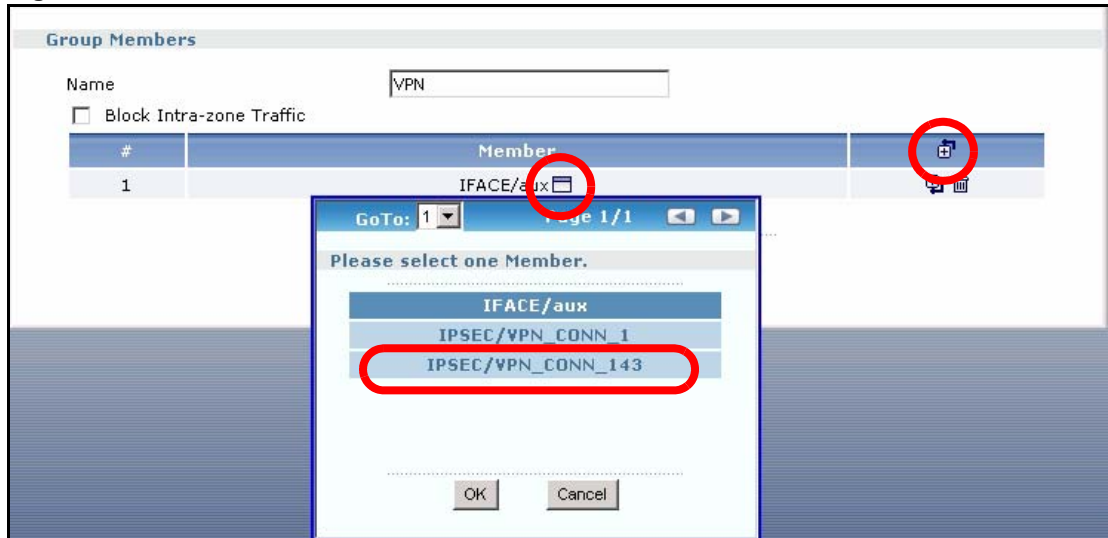
6.2.6 Set up the Zone for the VPN Tunnel

The new VPN connection has not been assigned to a zone yet. In this example, you want to set up different security policies for VPN tunnels than you do for the default LAN, DMZ, and WAN zones, so create a new zone called VPN.

- 1 Click **Network > Zone**. Click the **Add** icon.

- 2 Give the zone a name (“VPN”), and add the VPN tunnel to it. To add the VPN tunnel, click the **Add** icon, and then click the **Popup** icon next to the new member that appears. In the popup window, select the VPN connection. Click **OK**.

Figure 77 Network > Zone > add

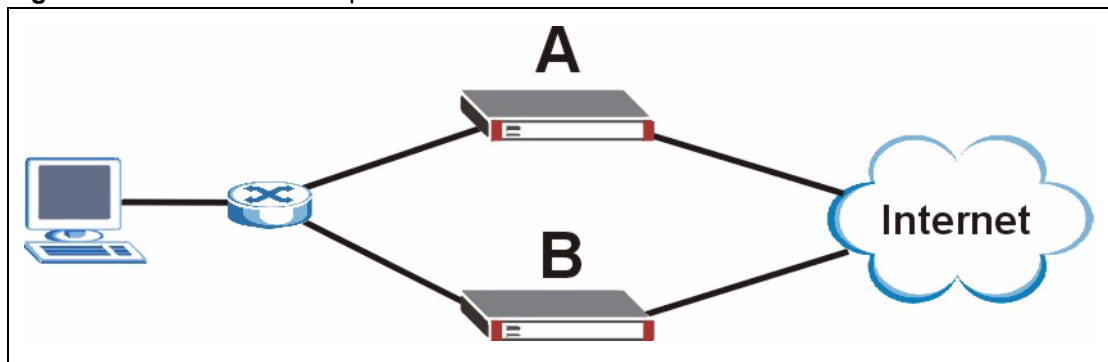


By default, there are no security restrictions on the new zone, so, next, you should set up security policies (firewall rules, IDP, and so on) accordingly. Make sure all the firewalls between the ZyWALL and remote IPsec router allow UDP port 500 (IKE) and IP protocol 50 (AH) or 51 (ESP). You did not enable NAT traversal, so you do not have to configure the firewalls to allow UDP port 4500.

6.3 Device HA

This example is going to show you how to set up device HA as illustrated below.

Figure 78 Device HA Example



In this example, the default gateway for the network is 192.168.10.254, and there are two ZyWALL routers to ensure this gateway is available. Router A is the master; router B is the backup.

The ZyWALL has its default settings. Configure the master first because you can synchronize the backup with the master later.

6.3.1 Set up the Ethernet Interfaces on the Master

You should configure at least two interfaces, ge1 and the interface that is connected to the Internet (ge2 or ge3). Ignore the other interfaces. Configure the interface that is connected to the Internet first because you are using ge1 to access the ZyWALL now. This way, you do not have to log in again until you finish configuring both interfaces.

- 1 Click **Network > Interface > Ethernet**. Click the **Edit** icon for the interface that is connected to the Internet. Configure it, and click **OK**.
- 2 In **Network > Interface > Ethernet**, click the **Edit** icon for ge1.
- 3 Change the static IP address to 192.168.10.254.

Figure 79 Network > Interface > Ethernet > ge1 > IP Address

The screenshot shows the configuration page for the Ethernet interface ge1. The 'Ethernet Interface Properties' section has 'Enable' checked, 'Interface Name' set to 'ge1', and an empty 'Description' field. The 'IP Address Assignment' section has 'Use Fixed IP Address' selected. The 'IP Address' field is highlighted with a red circle and contains the value '192.168.10.254'. The 'Subnet Mask' is '255.255.255.0' and the 'Gateway' is empty. The 'Metric' is '0'.

- 4 The DHCP server is active, and you have to keep the **IP Pool Start Address** in the same subnet as the interface. Change it to 192.168.10.33. Click **OK**.

Figure 80 Network > Interface > Ethernet > ge1 > DHCP Settings

The screenshot shows the DHCP settings page. The 'DHCP Server' dropdown is set to 'From ISP'. The 'IP Pool Start Address (Optional)' field is highlighted with a red circle and contains the value '192.168.10.33'. The 'Pool Size' is '200'. The 'First DNS Server (Optional)' is 'From ISP', the 'Second DNS server (Optional)' is 'From ISP', and the 'Third DNS Server (Optional)' is 'Custom Defined'. The 'Lease time' is set to '2 days 0 hours (Optional) 0 minutes'. There is an 'Add Static DHCP' button at the bottom.

Release the old IP address the ZyWALL assigned to your computer (192.168.1.0/24), and renew the IP address again so that the ZyWALL assigns you an IP address in the new subnet (192.168.10.0/24). Go to <http://192.168.10.254> to log in to the ZyWALL again.

By default, there is an address object called LAN_SUBNET, whose subnet is the same as that of ge1 (192.168.1.0/24). It is used by a policy route for the default trunk WAN_TRUNK. Normally, you should either delete these objects or change LAN_SUBNET to 192.168.10.0/24. In this example, ignore all these objects.

6.3.2 Set up DNS for the Virtual Router

You can use a fully-qualified domain name, instead of an IP address, for the virtual router. If you want to do this, you should set up DNS before you configure the VRRP groups and synchronization. In this example, you are going to use the IP address.

6.3.3 Set up the VRRP Groups on the Master

You have to set up one VRRP group for each interface with a static IP address on which you want to set up device HA. In this example, create two VRRP groups, one for ge1 and one for ge3.

- 1 Click **Network > Device HA > VRRP Group**, and then click the **Add** icon.
- 2 Give the VRRP group a name and virtual router ID, and select the interface ge1. This is the master router, and you are not going to use authentication. Click **OK**.

Figure 81 Network > Device HA > VRRP Group > add

The screenshot shows the configuration page for a VRRP Group. It is divided into two main sections: 'Basic Setting' and 'Authentication'.

Basic Setting:

- Enable
- Name:
- VRID: (1-254)
- Description: (Optional)
- VRRP Interface: (dropdown menu)
- Role: Master Backup
- Priority: (range check for backup: 1-254)
- Preempt
- Manage IP:
- Manage IP Subnet Mask:

Authentication:

- None
- Text:
- IP AH(MD5): (Authentication key)

- 3 Click **Status**, and scroll down to the **Interface Status Summary**. The **H/A Status** field is **Active**, and the IP address is 192.168.10.254.

Figure 82 Status > Interface Status Summary

Interface Status Summary								Expand
Name	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Renew/Dial	
ge1	Down	Active	LAN	192.168.10.254 / 255.255.255.0	Static	DHCP server / RIP	n/a	

- Repeat these steps for the interface that is connected to the Internet. The second VRRP group should have a different VR ID. Part of an example using ge3 is shown below.

Figure 83 Network > Device HA > VRRP Group > add

Basic Setting	
<input checked="" type="checkbox"/> Enable	
Name	id30_master_ge3
VRID	30 (1-254)
Description	(Optional)
VRRP Interface	ge3
Role	<input checked="" type="radio"/> Master <input type="radio"/> Backup
Priority	255 (range check for backup: 1-254)
<input type="checkbox"/> Preempt	
Manage IP	
Manage IP Subnet Mask	

Note: Once you configure an interface in a VRRP group, you should not configure the interface to have a dynamic IP address.

6.3.4 Set up the Password for Synchronization

- Click **Network > Device HA > Synchronize**.
- Type the password for synchronization in the **Password** field. This password does not have to be the same as the password for the **admin** account, but you have to set the same password in the master and backup. Click **Apply**.

Figure 84 Network > Device HA > Synchronize

VRRP Group		Synchronize
Authentication		
Password	****	
Synchronize from	(IP or FQDN)	on port 21 <input type="button" value="Sync. Now"/>
<input type="checkbox"/> Auto Synchronize		
Interval	5 minutes (1-1440)	
<input type="button" value="Apply"/> <input type="button" value="Reset"/>		

6.3.5 Finish Configuring the Master

Finish configuring the master. The backup router will get these updates later, when it synchronizes with the master.

6.3.6 Set up the Ethernet Interfaces on the Backup

On the backup ZyWALL, ge1 should be configured exactly the same way it is configured on the master, including the same IP address. Therefore, you should not configure the backup while it is connected to the same network as the master, or there will be an IP address conflict.

You do not have to configure any other interfaces, including the one that is connected to the Internet, because the backup will get this configuration when it synchronizes with the master.

6.3.7 Set up the VRRP Groups on the Backup

You should set up the same VRRP groups on the backup that you set up on the master. The only difference is the role. In each VRRP group, select **Backup**, instead of **Master**, in the **Role** field. Therefore, you will also set up the management IP address for the backup. The VRRP group for ge1 is shown below.

Figure 85 Network > Device HA > VRRP Group > add

The screenshot shows the configuration page for a VRRP group. The 'Basic Setting' section includes the following fields:

- Enable
- Name: id10_master_ge1
- VRID: 10 (1-254)
- Description: (Optional)
- VRRP Interface: ge1
- Role: Master Backup
- Priority: 1 (range check for backup: 1-254)
- Preempt
- Manage IP: 192.168.10.101
- Manage IP Subnet Mask: 255.255.255.0

The 'Authentication' section includes:

- None
- Text
- IP AH(MD5) (Authentication key)

The **Interface Status Summary**. The **H/A Status** field is **Stand-By**, and the IP address is the management IP address 192.168.10.101.

Figure 86 Status > Interface Status Summary

Interface Status Summary								Expand
Name	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Renew/Dial	
ge1	Down	Stand-By	LAN	192.168.10.101 / 255.255.255.0	Static	DHCP server / RIP	n/a	

6.3.8 Synchronize the Backup

- 1 Connect the backup to the same network as the master.
- 2 Click **Network > Device HA > Synchronize**.

- 3 Type the password for synchronization in the **Password** field. Enter the IP address of the master (on a secure network), and click **Sync Now** to get the configuration from the master.

Figure 87 Network > Device HA > Synchronize

The screenshot shows the 'Synchronize' configuration page for a VRRP Group. Under the 'Authentication' section, the 'Password' field is masked with four asterisks. The 'Synchronize from' field contains the IP address '192.168.10.254', which is circled in red. To its right is the label 'IP or FQDN'. The 'on port' field is set to '21'. A 'Sync. Now' button is located to the right of the 'Synchronize from' field. Below these fields, there is an unchecked checkbox for 'Auto Synchronize' and an 'Interval' field set to '5' minutes (with a range of 1-1440). At the bottom of the form are 'Apply' and 'Reset' buttons.

You can also set up the backup to synchronize with the master at regular intervals.

6.4 User-Aware Access Control

You can configure many policies and security settings for specific users or groups of users. This is illustrated in the following example, where you will set up the following policies.

Table 32 User-Aware Access Control Example

GROUP (USER)	WEB SURFING	WEB BANDWIDTH	MSN	LAN-TO-DMZ ACCESS
Finance (Leo)	Yes	200K	No	Yes
Engineer (Steven)	Yes	100K	No	No
Sales (Debbie)	Yes	100K	Yes (M-F, 08:30~18:00)	Yes
Boss (Andy)	Yes	100K	Yes	Yes
Guest (guest)	Yes	50K	No	No
Others	No	---	No	No

The users are authenticated by an external RADIUS server at 192.168.1.200.

First, set up the user accounts and user groups in the ZyWALL. Then, set up user authentication using the RADIUS server. Finally, set up the policies in the table above.

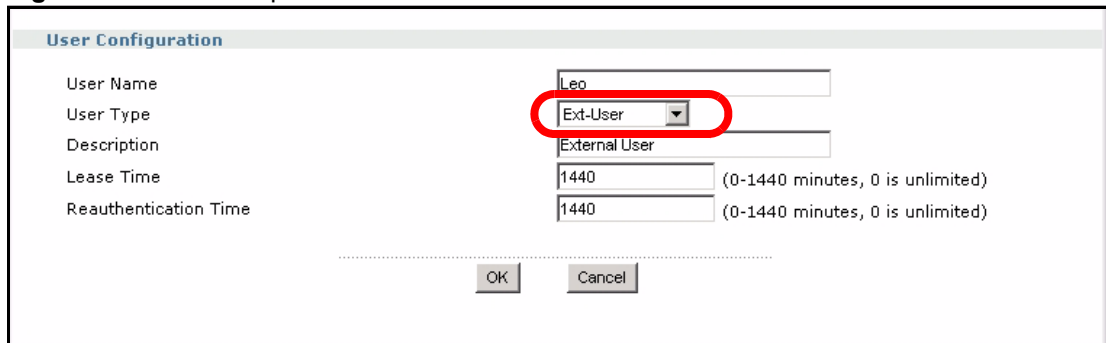
The ZyWALL has its default settings.

6.4.1 Set up User Accounts

Set up one user account for each user account in the RADIUS server. If it is possible to export user names from the RADIUS server to a text file, then you might create a script to create the user accounts instead. This example uses the web configurator.

- 1 Click **User/Group > User**. Click the **Add** icon.
- 2 Enter the same user name that is used in the RADIUS server, and set the **User Type** to **Ext-User** because this user account is authenticated by an external server. Click **OK**.

Figure 88 User/Group > User > add



The screenshot shows a web form titled "User Configuration". It contains the following fields and values:

Field	Value	Notes
User Name	Leo	
User Type	Ext-User	Selected in a dropdown menu, circled in red.
Description	External User	
Lease Time	1440	(0-1440 minutes, 0 is unlimited)
Reauthentication Time	1440	(0-1440 minutes, 0 is unlimited)

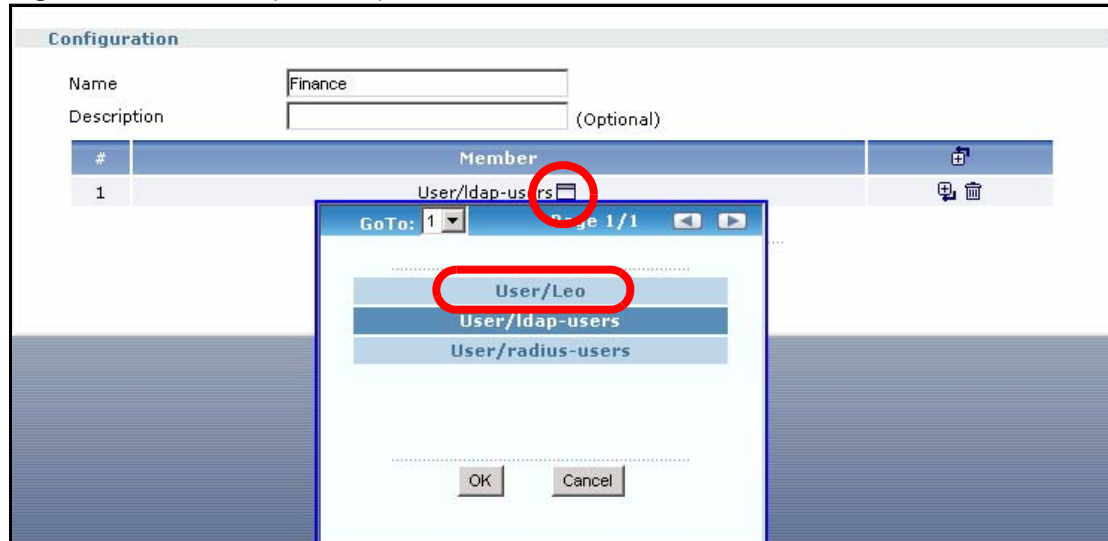
At the bottom of the form, there are two buttons: "OK" and "Cancel".

- 3 Repeat this process to set up the remaining user accounts.

6.4.2 Set up User Groups

Set up the user groups and assign the users to each one.

- 1 Click **User/Group > Group**. Click the **Add** icon.
- 2 Enter the name of the group that is used in [Table 32 on page 141](#). In this example, it is "Finance". Then, click the **Add** icon. The new member is not the correct one, so click the **Popup** icon to change it. Select **User/Leo**, and click **OK**. There is only one member in this group, so click **OK**. If there were other members in the group, you would add them first.

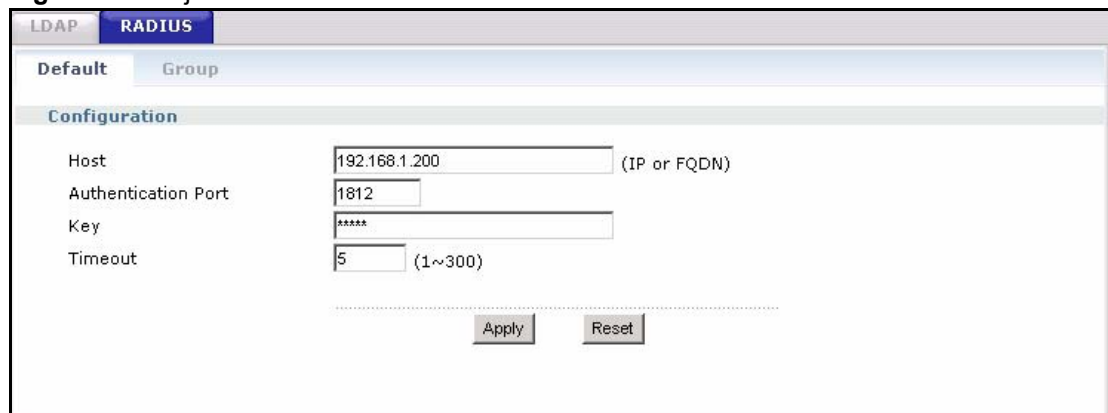
Figure 89 User/Group > Group > add

- 3 Repeat this process to set up the remaining user groups.

6.4.3 Set up User Authentication Using the RADIUS Server

This step sets up user authentication (for HTTP/HTTPS access) using the RADIUS server. First, configure the settings for the RADIUS server. Then, set up the authentication method, and configure the ZyWALL to use the authentication method for HTTP/HTTPS access. Finally, force users to log in to the ZyWALL before it routes HTTP/HTTPS traffic for them.

- 1 Click **Object > AAA Server > RADIUS > Default**. Configure the RADIUS server, and click **Apply**.

Figure 90 Object > AAA Server > RADIUS > Default

- 2 Click **User/Group > Group**. Click the **Add** icon.
- 3 Give the new authentication method a descriptive name, and click the **Add** icon. Select **group radius** because the ZyWALL should use the specified RADIUS server for authentication. Click **OK**.

Figure 91 Object > AAA Server > RADIUS > Default

#	Method List	
1	group radius	

4 Click **System > WWW**. In the **Authentication** section, select the new authentication method in the **Client Authentication Method** field. Click **Apply**.

Figure 92 System > WWW > Authentication

5 Click **User/Group > Setting**. In the **Force User Authentication Policy** section, click the **Add** icon.

6 Set up a default policy that forces every user to log in to the ZyWALL before the ZyWALL routes HTTP/HTTPS traffic for them. Select **Enable**. Then, select **force** in the **Authentication** field. Keep the rest of the default settings, and click **OK**.

Figure 93 User/Group > Setting > Add (Force User Authentication Policy)

When the users try to browse the web (or use any HTTP/HTTPS application), the **Login** screen appears. They have to log in using the user name and password in the RADIUS server.

6.4.4 Set up Web Surfing Policies

Use application patrol to enforce the web surfing policies.

- 1 Click **Policy > App Patrol**. If application patrol is not enabled, enable it, and click **Apply**.
- 2 Click the **Edit** icon next to **http**.
- 3 Change the default policy to **drop** because you do not want anyone except authorized user groups to browse the web. Then, click the **Add** icon in the exception list (not the **Allow Port** list). In the new exception, select one of the user groups that is allowed to browse the web. Repeat this process to add exceptions for all the other user groups that are allowed to browse the web, and then click **OK**.

Figure 94 Policy > App Patrol > http > edit

Service

Enable Service

Service Identification

Name: http

Classification: Port-less Port-base


Default Policy

Access: Drop



Log: no

Enable Bandwidth Shaping: 1 kbps

Exception Policy

Allow Port: 

Action: Forward

#	Schedule	User	Source	Destination	Log	
1	none	Finance	any	any	no	

6.4.5 Set up Bandwidth Restrictions

You have to use policy routes to set up bandwidth restrictions for user groups.

- 1 Click **Policy > Route > Policy Route**. This policy route should have higher priority than the default policy route for the trunk, so click the **Add** icon at the top of the column, not the one next to the existing policy route.

Figure 95 Policy > Route > Policy Route

#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM
1	any	none	ge1	LAN_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0

- 2 This policy route is similar to the default policy route, except for user and bandwidth restrictions. Select one of the user groups in the **User** field, and set the corresponding bandwidth restriction in the **Maximum Bandwidth** field. Configure the rest of the policy route the same way the default policy route is configured, and click **OK**.

Figure 96 Policy > Route > Policy Route > add

- 3 Repeat this process to set up policy routes for the other bandwidth restrictions

6.4.6 Set up MSN Policies

Set up a recurring schedule object first because Sales can only use MSN during specified times on specified days.

- 1 Click **Object > Schedule**. Click the **Add** icon for recurring schedules.
- 2 Give the schedule a descriptive name. Set up the days (Monday through Friday) and the times (8:30 - 18:00) when Sales is allowed to use MSN. Click **OK**.

Figure 97 Object > Schedule > Recurring > add

Configuration						
Name	<input type="text" value="WORKHOURS"/>					
Day Time						
Item #	Day			Time		
	Year	Month	Day	Hour	minute	
Start	<input type="text"/>	<input type="text"/>	<input type="text"/>	8	30	
Stop	<input type="text"/>	<input type="text"/>	<input type="text"/>	18	0	
Weekly						
Week Days	<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday	<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input type="checkbox"/> Saturday
	<input type="checkbox"/> Sunday					
<input type="button" value="OK"/> <input type="button" value="Cancel"/>						

- 3 Follow the steps in [Section 6.4.4 on page 144](#) to set up the appropriate policies for MSN in application patrol.

6.4.7 Set up LAN-to-DMZ Policies

Use the firewall to control access to the DMZ.

- 1 Click **Policy > Firewall**. In **From Zone**, select **LAN**; in **To Zone**, select **DMZ**. The default rule for LAN-to-DMZ traffic allows all traffic. You want to limit access to specific groups, so change the default rule first. Click the **Edit** icon next to it.
- 2 Change the **Access** field to deny, and click **OK**.

Figure 98 Policy > Firewall > LAN > DMZ > edit

The screenshot shows the 'Configuration' window for editing a DMZ rule. The 'Access' dropdown menu is highlighted with a red circle and set to 'deny'. Other settings include 'Enable' checked, 'From' LAN, 'To' DMZ, 'Schedule' none, 'User' any, 'Source' any, 'Destination' any, 'Service' any, and 'Log' no. 'OK' and 'Cancel' buttons are at the bottom.

- 3 Click the **Add** icon at the top of the rule list to create an exception for one of the user groups that is allowed to access the DMZ.
- 4 Select one of the user groups that is allowed to access the DMZ, and click **OK**.

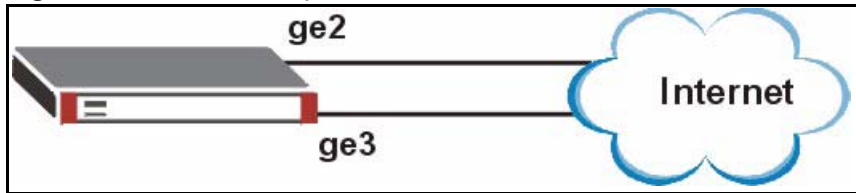
Figure 99 Policy > Firewall > LAN > DMZ > add

The screenshot shows the 'Configuration' window for adding a new DMZ rule. The 'User' dropdown menu is highlighted with a red circle and set to 'Finance'. Other settings include 'Enable' checked, 'From' LAN, 'To' DMZ, 'Description' (Optional), 'Schedule' none, 'Source' any, 'Destination' any, 'Service' any, 'Access' allow, and 'Log' no. 'OK' and 'Cancel' buttons are at the bottom.

- 5 Repeat this process to set up firewall rules for the other user groups that are allowed to access the DMZ.

6.5 Trunks

The following example shows how to set up a trunk for two connections (ge2 and ge3) to the Internet. The available bandwidth for each connections is 1M (ge2) and 512K (ge3). As these connections have somewhat different bandwidth, you have decided to use the **Weighted Round Robin** algorithm and to send traffic to ge2 and ge3 in a 2:1 ratio.

Figure 100 Trunk Example

The ZyWALL has its default settings, and you do not have to change many of them to set up this trunk. You only have to set up the bandwidth on ge2 and ge3 and change the algorithm that WAN_TRUNK uses.

6.5.1 Set up Available Bandwidth on Ethernet Interfaces

- 1 Click **Network > Interface > Ethernet**. Click the **Edit** icon for ge2, and enter the available bandwidth (1000 kbps) in the **Upstream Bandwidth** and **Downstream Bandwidth** fields. Click **OK**.

Figure 101 Network > Interface > Ethernet > edit > ge2

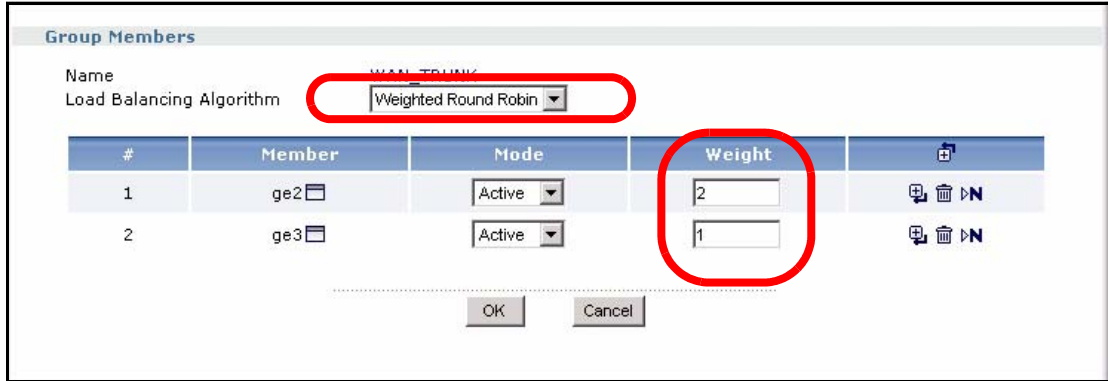
The screenshot shows the 'Ethernet Interface Properties' configuration page for interface 'ge2'. The 'Interface Name' is set to 'ge2'. Under 'IP Address Assignment', 'Get Automatically' is selected with the IP address '172.23.23.144'. Under 'Interface Parameters', the 'Upstream Bandwidth' and 'Downstream Bandwidth' fields are both set to '1000 Kbps' and are circled in red. The 'MTU' is set to '1500 Bytes'.

- 2 Click the **Edit** icon for ge3, and enter the available bandwidth (512 kbps) in the **Upstream Bandwidth** and **Downstream Bandwidth** fields. Click **OK**.

6.5.2 Change WAN Trunk Algorithm

- 1 Click **Network > Interface > Trunk**. Click the **Edit** icon next to WAN_TRUNK.
- 2 In the **Load Balancing Algorithm** field, select **Weighted Round Robin**. After the screen refreshes, enter 2 and 1 in the **Weight** column for ge2 and ge3, respectively. Click **OK**.

Figure 102 Network > Interface > Trunk > WAN_TRUNK > edit



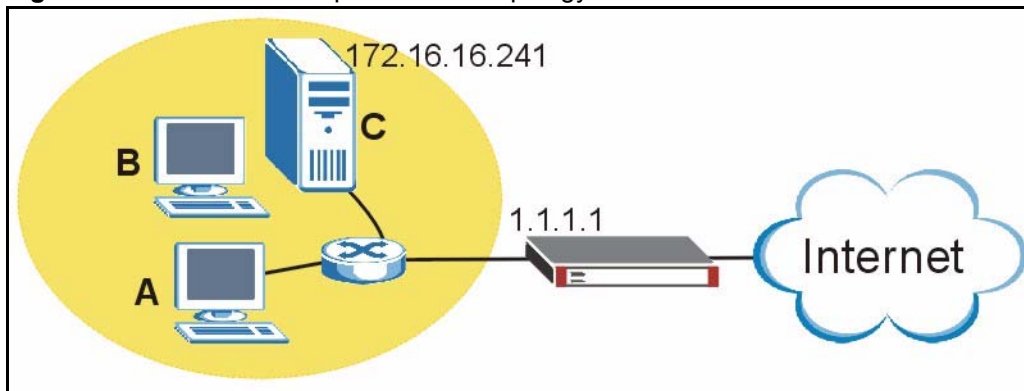
6.6 NAT 1:1 Example

In this example, C is an SMTP mail server in our LAN zone. It has a private IP address of 172.16.16.241. The public IP address of the server is 1.1.1.1.

In order for C to be accessible to people from the Internet (WAN zone), you need to create a 1:1 mapping from the public IP address to its private one.

The firewall is enabled, so you also need to create a rule to allow traffic in from the WAN zone.

Figure 103 1-1 NAT Example Network Topology



6.6.1 Address Objects

First create two address objects for the public and private IP addresses (WAN_EG and LAN_EG) in the **Object > Address** screen as shown next.

Figure 104 Create Address Objects

Figure 104 shows two screenshots of the 'Create Address Object' dialog box. The first screenshot shows the 'Name' field set to 'LAN_EG', 'Address Type' set to 'HOST', and 'IP Address' set to '172.16.16.241'. The second screenshot shows the 'Name' field set to 'WAN_EG', 'Address Type' set to 'HOST', and 'IP Address' set to '1.1.1.1'. Red circles highlight the IP address fields in both screenshots.

Figure 105 Address Objects

Figure 105 shows the 'Address Objects' configuration table. The table has columns for '#', 'Name', 'Type', 'Address', and a set of icons. The 'WAN_EG' row is circled in red.

#	Name	Type	Address	
1	LAN_SUBNET	SUBNET	192.168.1.0/24	
2	TW_SUBNET	SUBNET	172.23.37.0/24	
3	WIZ_VPN_LOCAL	SUBNET	1.1.1.0/24	
4	WIZ_VPN_REMOTE	SUBNET	2.2.2.0/24	
5	WAN_EG	HOST	1.1.1.1	
6	LAN_EG	HOST	172.16.16.241	

6.6.2 Interface

The ge3 WAN interface has a different IP address than 1.1.1.1, so in order for the ZyWALL gateway to be able to do ARP resolution correctly, you need to create a ge3 virtual interface. In the **Network > Interface > Ethernet** screen, click the + symbol in the ge3 row to create a virtual interface for ge3.

Figure 106 Create a WAN Virtual Interface

Figure 106 shows the 'Virtual Interface Properties' dialog box. The 'Interface Name' is 'ge3:1' and the 'Description' is 'NAT 1:1'. The 'IP Address' is '1.1.1.1' and the 'Subnet Mask' is '255.0.0.0'. The 'Gateway' is optional and the 'Metric' is '0'. The 'Upstream Bandwidth' and 'Downstream Bandwidth' are both '1048576 Kbps'. Red circles highlight the 'IP Address' and 'Subnet Mask' fields.

Figure 107 Virtual WAN Interface

Configuration				
#	Name	IP Address	Mask	Modify
1	ge1	STATIC -- 192.168.1.1	255.255.255.0	
2	ge2	DHCP -- 0.0.0.0	0.0.0.0	
3	ge3	STATIC -- 172.23.37.240	255.255.255.0	
4	ge3:1	STATIC -- 1.1.1.1	255.0.0.0	
5	ge4	STATIC -- 0.0.0.0	0.0.0.0	
6	ge5	STATIC -- 0.0.0.0	0.0.0.0	

6.6.3 Policy Route

Now create a policy route (in the **Policy > Route > Add** screen) that defines the criteria for the address mapping as shown in the next screen. Be careful of where you create the route as routes are ordered in descending priority.

Figure 108 Create a Policy Route

Configuration

Enable

Description: NAT 1:1 EG (Optional)

Criteria

User: any

Incoming: Interface / any

Source Address: LAN_EG

Destination Address: any

Schedule: WorkTime

Service: any

Next-Hop

Type: Interface

Gateway: WAN_EG

Interface: ge3

VPN Tunnel: WIZ_VPN

Trunk: WAN_TRUNK

Address Translation

Source Network Address Translation: WAN_EG

Bandwidth Shaping

Maximum Bandwidth: 0 Kbps

Bandwidth Priority: 0 (1-1024, 1 is highest priority)

6.6.4 Firewall Rule

Create a firewall rule to allow access from the WAN zone to the mail server in the LAN zone. Be careful of where you create the rule as firewall rules are ordered in descending priority.

Create a Firewall Rule

Configuration

<input checked="" type="checkbox"/> Enable	
From	WAN
To	LAN
Description	to LAN_EG server (Optional)
Schedule	none
User	any
Source	any
Destination	LAN_EG
Service	SMTP
Access	allow
Log	no

OK Cancel

CHAPTER 7

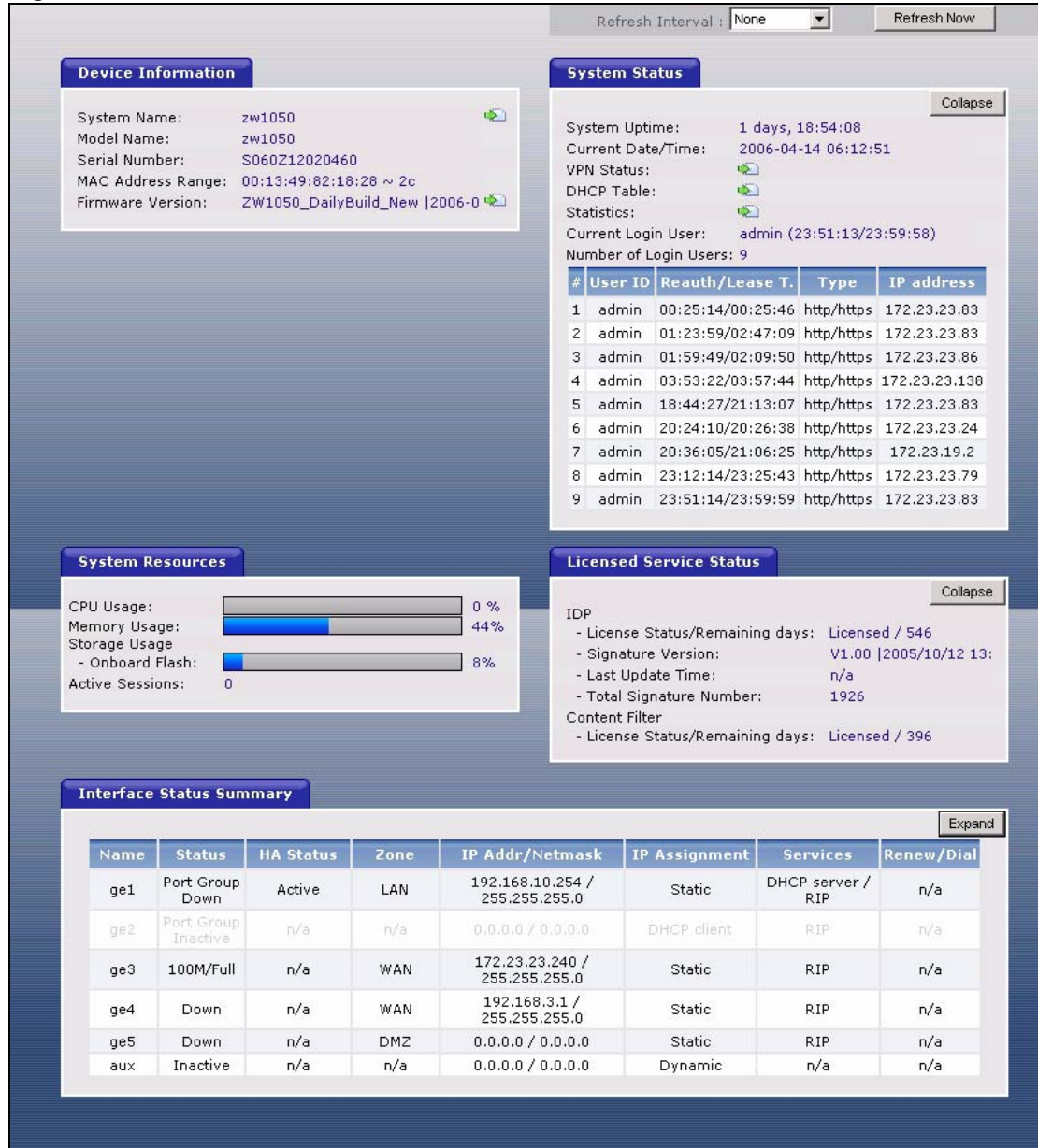
Status

This chapter explains the **Status** screen, which is the screen you see when you first log in to the ZyWALL or when you click **Status**.

7.1 Status Screen

Use these screens to look at the ZyWALL's general device information, system status, system resource usage, licensed service status, and interface status. To access this screen, click **Status**.

Figure 109 Status



The following table describes the labels in this screen.

Table 33 Status

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the screen to automatically refresh.
Refresh Now	Click this to update the screen immediately.
Device Information	
System Name	This field displays the name used to identify the ZyWALL on any network. Click the icon on the right to open the screen where you can change it. See Section 34.2 on page 489 .

Table 33 Status (continued)

LABEL	DESCRIPTION
Model Name	This field displays the model name of this ZyWALL.
Serial Number	This field displays the serial number of this ZyWALL.
MAC Address Range	This field displays the MAC addresses used by the ZyWALL. Each physical port has one MAC address. The first MAC address is assigned to physical port 1, the second MAC address is assigned to physical port 2, and so on.
Firmware Version	This field displays the version number and date of the firmware the ZyWALL is currently running. Click the icon on the right to open the screen where you can upload firmware. See Section 9.3 on page 172 .
System Status	
Expand / Collapse	Click this to look at the users who are currently logged in to the ZyWALL. See the Current Login List field.
System Uptime	This field displays how long the ZyWALL has been running since it last restarted or was turned on.
Current Date/ Time	This field displays the current date and time in the ZyWALL. The format is yyyy-mm-dd hh:mm:ss.
VPN Status	Click this to look at the VPN tunnel that are currently established. See Section 7.2 on page 160 .
DHCP Table	Click this to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. See Section 7.3 on page 161 .
Statistics	Click this to look at packet statistics for each physical port. See Section 7.4 on page 161 .
Current Login User	This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining. See Chapter 27 on page 423 .
Number of Login Users	This field displays the number of users currently logged in to the ZyWALL. Click Expand to list the users who are currently logged in to the ZyWALL. Click Collapse to hide this information.
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the ZyWALL.
Reauth/Lease T.	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user. See Chapter 27 on page 423 .
Type	This field displays the way the user logged in to the ZyWALL.
IP address	This field displays the IP address of the computer used to log in to the ZyWALL.
System Resource	
CPU Usage	This field displays what percentage of the ZyWALL's processing capability is currently being used.
Memory Usage	This field displays what percentage of the ZyWALL's RAM is currently being used.
Storage Usage - Onboard Flash	This field displays what percentage of the ZyWALL's onboard flash memory is currently being used.
Active Sessions	This field displays how many traffic sessions are currently open on the ZyWALL. These are the sessions that are traversing the ZyWALL.
Licensed Service Status	
Expand / Collapse	Click this to look at more information about services that are currently licensed.

Table 33 Status (continued)

LABEL	DESCRIPTION
IDP	
License Status / Remaining Days	This field displays the current status of the license and how many days longer it is still valid. If it displays 0 days, the license has expired. If the status is not Licensed , click this to open the screen where you can activate or extend the license. See Chapter 8 on page 163 .
Signature Version	This field displays the version number, date, and time of the current set of signatures the ZyWALL is using.
Last Update Time	This field displays the last time the ZyWALL received updated signatures.
Total Signature Number	This field displays the total number of signatures in the current signature version.
Content Filter	
License Status / Remaining Days	This field displays the current status of the license and how many days longer it is still valid. If it displays 0 days, the license has expired. If the status is not Licensed , click this to open the screen where you can activate or extend the license. See Chapter 8 on page 163 .
Interface Status Summary	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text.
Expand / Collapse	Click this to look at information about active VLAN, bridge, and PPPoE/PPTP interfaces, as well as Ethernet and auxiliary interfaces.
Name	This field displays the name of each interface. If there is a blue plus-sign icon next to the name, click this to look at the status of virtual interfaces on top of this interface.

Table 33 Status (continued)

LABEL	DESCRIPTION
Status	<p>This field displays the current status of each interface. The possible values depend on what type of interface it is.</p> <p>For port groups:</p> <p>Inactive - The port group is disabled.</p> <p>Port Group Down - The port group is enabled but not connected.</p> <p>Port Group Up - The port group is enabled, and at least one of the physical ports associated with it is connected.</p> <p>For Ethernet interfaces:</p> <p>Port Group Inactive - The Ethernet interface does not have any physical ports associated with it.</p> <p>Inactive - The Ethernet interface is disabled.</p> <p>Down - The Ethernet interface is enabled but not connected.</p> <p>Speed / Duplex - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (Full or Half).</p> <p>For the auxiliary interface:</p> <p>Inactive - The auxiliary interface is disabled.</p> <p>Connected - The auxiliary interface is enabled and connected.</p> <p>Disconnected - The auxiliary interface is not connected.</p> <p>For virtual interfaces, this field always displays Up. If the virtual interface is disabled, it does not appear in the list.</p> <p>For VLAN and bridge interfaces, this field always displays Up. If the VLAN or bridge interface is disabled, it does not appear in the list.</p> <p>For PPPoE/PPTP interfaces:</p> <p>Connected - The PPPoE/PPTP interface is connected.</p> <p>Disconnected - The PPPoE/PPTP interface is not connected.</p> <p>If the PPPoE/PPTP interface is disabled, it does not appear in the list.</p>
HA Status	<p>This field displays the status of the interface in the virtual router.</p> <p>Active - This interface is the master interface in the virtual router.</p> <p>Stand-By - This interface is a backup interface in the virtual router.</p> <p>Fault - This VRRP group is not functioning in the virtual router right now. For example, this might happen if the interface is down.</p> <p>n/a - Device HA is not active on the interface.</p>
Zone	<p>This field displays the zone to which the interface is currently assigned.</p>
IP Addr/Netmask	<p>This field displays the current IP address and subnet mask assigned to the interface. If the IP address and subnet mask are 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP.</p> <p>If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).</p>
IP Assignment	<p>This field displays how the interface gets its IP address.</p> <p>Static - This interface has a static IP address.</p> <p>DHCP Client - This interface gets its IP address from a DHCP server.</p> <p>Dynamic - This is the auxiliary interface.</p>

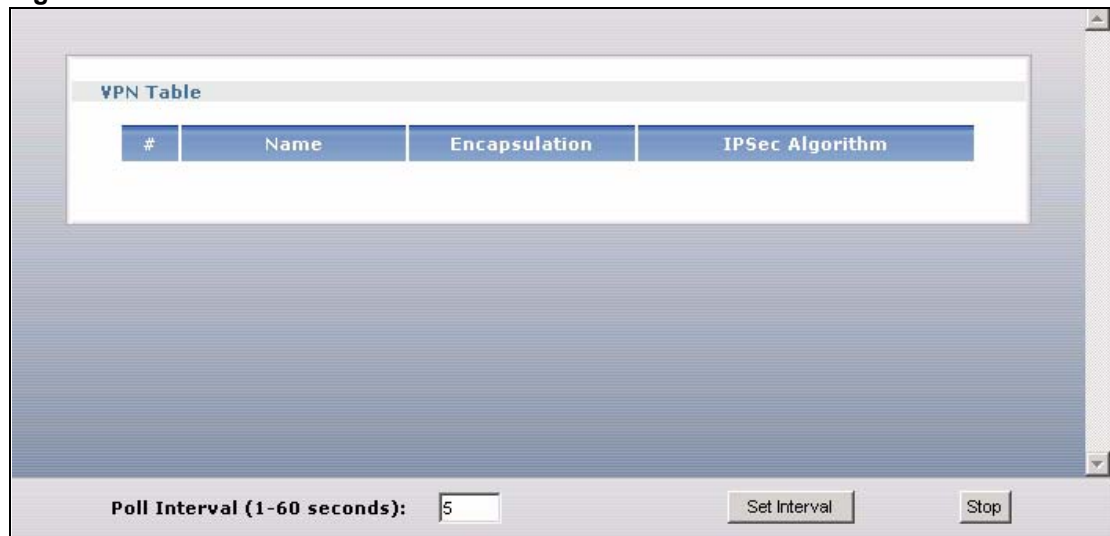
Table 33 Status (continued)

LABEL	DESCRIPTION
Services	This field lists which services the interface provides to the network. Examples include DHCP relay , DHCP server , DDNS , RIP , and OSPF . This field displays n/a if the interface does not provide any services to the network.
Renew/Dial	Use this field to get or to update the IP address for the interface. Click Renew to send a new DHCP request to a DHCP server. Click the Connect icon to try to connect the auxiliary interface or a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays n/a .

7.2 VPN Status

Use this screen to look at the VPN tunnels that are currently established. To access this screen, click **VPN Status** in the **Status** screen.

Figure 110 Status > VPN Status



The following table describes the labels in this screen.

Table 34 Status > VPN Status

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPsec SA.
Encapsulation	This field displays how the IPsec SA is encapsulated.
IPSec Algorithm	This field displays the encryption and authentication algorithms used in the SA.
Poll Interval	Enter how often you want this window to be updated automatically, and click Set Interval .
Set Interval	Click this to set the Poll Interval the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the Poll Interval and clicking Set Interval .

7.3 DHCP Table

Use this screen to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. To access this screen, click **DHCP Table** in the **Status** screen.

Figure 111 Status > DHCP Table

The screenshot shows the DHCP Table configuration interface. At the top, there is a title 'DHCP Table' and a dropdown menu for 'Interface' currently set to 'ge1'. Below this is a table with the following data:

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.44	none	05:01:0D:1F:1C:47	<input checked="" type="checkbox"/>

Below the table, there are two buttons: 'Apply' and 'Refresh'.

The following table describes the labels in this screen.

Table 35 Status > DHCP Table

LABEL	DESCRIPTION
Interface	Select for which interface you want to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address.
Host Name	This field displays the name used to identify this device on the network (the computer name). The ZyWALL learns these from the DHCP client requests. You can use CLI commands to set this value for static DHCP entries.
MAC Address	This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved.
Reserve	<p>If this field is selected, this entry is a static DHCP entry. The IP address is reserved for the MAC address.</p> <p>If this field is clear, this entry is a dynamic DHCP entry. The IP address is assigned to a DHCP client.</p> <p>To create a static DHCP entry using an existing dynamic DHCP entry, select this field, and then click Apply.</p> <p>To remove a static DHCP entry, clear this field, and then click Apply.</p>
Apply	Click this to save your settings to the ZyWALL.
Refresh	Click this to update the screen immediately.

7.4 Statistics

Use this screen to look at packet statistics for each physical port. To access this screen, click **Statistics** in the **Status** screen.

Figure 112 Status > Statistics

Statistics Table							
Port	status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
1	100M/Full	3613	45102	0	0	960	30:03:17
2	Down	634139	1349	0	0	0	00:00:00
3	100M/Full	393398	2932808	0	3020	640	53:23:26
4	Down	1185	88	0	0	0	00:00:00
5	Down	1997	0	0	0	0	00:00:00

System Up Time : 22 days, 01:45:51

Poll Interval (1-60 seconds):

The following table describes the labels in this screen.

Table 36 Status > Statistics

LABEL	DESCRIPTION
Port	This field displays the physical port number.
status	This field displays the current status of the physical port. Down - The physical port is not connected. Speed / Duplex - The physical port is connected. This field displays the port speed and duplex setting (Full or Half).
TxPkts	This field displays the number of packets transmitted from the ZyWALL on the physical port since it was last connected.
RxPkts	This field displays the number of packets received by the ZyWALL on the physical port since it was last connected.
Collisions	This field displays the number of collisions on the physical port since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Up Time	This field displays how long the physical port has been connected.
System Up Time	This field displays how long the ZyWALL has been running since it last restarted or was turned on.
Poll Interval	Enter how often you want this window to be updated automatically, and click Set Interval .
Set Interval	Click this to set the Poll Interval the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the Poll Interval and clicking Set Interval .

CHAPTER 8

Registration

This chapter shows you how to register for IDP and Content Filtering service.

8.1 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.

8.1.1 Subscription Services Available on the ZyWALL

The ZyWALL can use content filtering and IDP (Intrusion Detection and Prevention) subscription services.

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

The IDP feature uses the signature files on the ZyWALL to detect malicious or suspicious packets and respond immediately. After the service is activated, the ZyWALL can download the up-to-date signature files from the update server (<http://myupdate.zywall.zyxel.com>).

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

See the chapters about content filtering and IDP for more information.

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

8.2 Registration

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

Figure 113 Registration

The following table describes the labels in this screen.

Table 37 Registration

LABEL	DESCRIPTION
Device Registration	If you select existing myZyXEL.com account , only the User Name and Password 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.
UserName	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.

Table 37 Registration (continued)

LABEL	DESCRIPTION
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 Code	Select your country from the drop-down box list.
Trial Service Activation	You can try a trial service subscription. After the trial expires, you can buy an iCard and enter the license key in the Registration Service screen to extend the service.
IDP Content Filtering	Select the check box to activate a trial. The trial period starts the day you activate the trial.
Apply	Click Apply to save your changes back to the ZyWALL.

Note: If the ZyWALL is registered already, this screen is read-only and indicates whether trial services are activated (if any). You can still select the unchecked trial service(s) to activate it after registration. Use the **Service** screen to update your service subscription status.

Figure 114 Registration: Registered Device

The screenshot shows the ZyWALL web interface. At the top, there are two tabs: 'Registration' and 'Service'. The 'Registration' tab is active. Below the tabs, the page is divided into two main sections. The first section, 'Device Registration', contains two input fields: 'UserName' with the value 'alexctsui' and 'Password' with the value '*****'. The second section, 'Trial Service Activation', contains two checkboxes: 'IDP' which is checked, and 'Content Filtering' which is unchecked. At the bottom center of the form, there is an 'Apply' button.

8.3 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.

Figure 115 Registration: Service

Service	Status	Registration Type	Expiration day
IDP Signature Update Service	Licensed	Trial	2006-3-24
Content Filter Service	Expired	Trial	2006-1-23

License Key

Note: Sync with myZyXEL.com to download license Info

The following table describes the labels in this screen.

Table 38 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 (Licensed) or not (Not Licensed) or expired (Expired).
Registration Type	This field displays whether you applied for a trial application (Trial) or registered a service with your iCard's PIN number (Standard). This field is blank when a service is not activated.
Expiration Day	This field displays the date your service expires.
License Upgrade	
License Key	Enter your iCard's PIN number and click Update 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 registration status and expiration day).

CHAPTER 9

File Manager

This chapter covers how to use the ZyWALL's **File Manager** screens to handle the ZyWALL's configuration, firmware and shell script files.

9.1 Configuration Files and Shell Scripts Overview

The **File Manager** screens allow you to store multiple configuration files and shell script files.

When you apply a configuration file, the ZyWALL uses the factory default settings for any features that the configuration file does not include. Shell scripts are files of commands that you can store on the ZyWALL and run when you need them. When you run a shell script, the ZyWALL only applies the commands that it contains. Other settings do not change.

You can edit configuration files or shell scripts in a text editor and upload them to the ZyWALL. Configuration files use a .conf extension and shell scripts use a .zysh extension.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 116 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-ZyWALL firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-ZyWALL firewall for TW_TEAM for remote management
firewall WAN ZyWALL insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the ZyWALL applies configuration files differently than it runs shell scripts. This is explained below.

Table 39 Configuration Files and Shell Scripts in the ZyWALL

Configuration Files (.conf)	Shell Scripts (.zysh)
<ul style="list-style-type: none">• Resets to default configuration.• Goes into CLI Configuration mode.• Runs the commands in the configuration file.	<ul style="list-style-type: none">• Goes into CLI Privilege mode.• Runs the commands in the shell script.

You have to run the example in [Table 116 on page 167](#) as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode.

9.1.1 Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the ZyWALL treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the ZyWALL exit sub command mode.

Note: “exit” or “!” must follow sub commands if it is to make the ZyWALL exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface gel
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface gel
# this interface is a DHCP client
!
```


Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2006/06/05
interface ge1
ip address dhcp
!
```

9.1.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the ZyWALL processes the file line-by-line. The ZyWALL checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the ZyWALL finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The ZyWALL ignores any errors in the configuration file or shell script and applies all of the valid commands. The ZyWALL still generates a log for any errors.

9.1.3 ZyWALL Configuration File Details

You can store multiple configuration files on the ZyWALL. You can also have the ZyWALL use a different configuration file without the ZyWALL restarting.

- When you first receive the ZyWALL, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the ZyWALL creates a **startup-config.conf** file of the current configuration.
- The ZyWALL checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the ZyWALL copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file.
- When the ZyWALL reboots, if the **startup-config.conf** file passes the error check, the ZyWALL keeps a copy of the **startup-config.conf** file as the **lastgood.conf** configuration file for you as a back up file. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.

9.1.4 Configuration File Flow at Restart

If there is not a **startup-config.conf** when you restart the ZyWALL (whether through a management interface or by physically turning the power off and back on), the ZyWALL uses the **system-default.conf** configuration file with the ZyWALL's default settings.

If there is a **startup-config.conf**, the ZyWALL checks it for errors and applies it. If there are no errors, the ZyWALL uses it and copies it to the **lastgood.conf** configuration file. If there is an error, the ZyWALL generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the ZyWALL applies the **system-default.conf** configuration file.

You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The ZyWALL ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The ZyWALL still generates a log for any errors.

9.2 Configuration File Screen

Click **File Manager > Configuration File** to open the **Configuration File** screen. Use the **Configuration File** screen to store and name configuration files. You can also download configuration files from the ZyWALL to your computer and upload configuration files from your computer to the ZyWALL.

Once your ZyWALL is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Figure 117 File Manager > Configuration File

Configuration File Firmware Package Shell Script

Configuration Files

Select the file

#	File Name	Size	Modify
1	system-default.conf	17386	2006-03-30 04:18:10
2	startup-config.conf	7176	2006-04-13 09:01:51
3	lastgood.conf	17601	2006-04-12 05:57:17
4	startup-config-back.conf	17601	2003-01-03 02:28:17
5	startup-config-bad.conf	20094	2006-04-12 11:19:04

Download Copy Rename Delete Apply

Upload Configuration File

To upload a configuration file, browse to the location of the file (.conf) and then click Upload.

File Path: Browse... Upload

The following table describes the labels in this screen.

Table 40 File Manager > Configuration File



LABEL	DESCRIPTION
Download	Click a configuration file's row to select it and click Download to save the configuration to your computer.
Copy	<p>Use this button to save a duplicate of a configuration file on the ZyWALL. Click a configuration file's row to select it and click Copy to open the Copy File screen.</p> <p>Figure 118 File Manager > Configuration File > Copy</p>  <p>Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;~!@#\$\$%^&()_+[]{}',.-).</p> <p>Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.</p>
Rename	<p>Use this button to change the label of a configuration file on the ZyWALL. You can only rename manually saved configuration files. You cannot rename the lastgood.conf, system-default.conf and startup-config.conf files.</p> <p>You cannot rename a configuration file to the name of another configuration file in the ZyWALL.</p> <p>Click a configuration file's row to select it and click Rename to open the Rename File screen.</p> <p>Figure 119 File Manager > Configuration File > Rename</p>  <p>Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;~!@#\$\$%^&()_+[]{}',.-).</p> <p>Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.</p>
Remove	<p>Click a configuration file's row to select it and click Remove to delete the configuration file from the ZyWALL. You can only delete manually saved configuration files. You cannot delete the system-default.conf, startup-config.conf and lastgood.conf files.</p> <p>A pop-up window asks you to confirm that you want to delete the configuration file. Click OK to delete the configuration file or click Cancel to close the screen without deleting the configuration file.</p>
Apply	<p>Use this button to have the ZyWALL use a specific configuration file.</p> <p>Click a configuration file's row to select it and click Apply to have the ZyWALL use that configuration file. The ZyWALL does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures.</p>

Table 40 File Manager > Configuration File (continued)

LABEL	DESCRIPTION
#	This column displays the number for each configuration file entry. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.
File Name	<p>This column displays the label that identifies a configuration file.</p> <p>You cannot delete the following configuration files or change their file names.</p> <p>The system-default.conf file contains the ZyWALL's default settings. Select this file and click Apply to reset all of the ZyWALL settings to the factory defaults. This configuration file is included when you upload a firmware package.</p> <p>The startup-config.conf file is the configuration file that the ZyWALL is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.</p> <p>The lastgood.conf is the most recently used (valid) configuration file that was saved when the device last restarted.</p>
Size	This column displays the size (in KB) of a configuration file.
Modify	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File	<p>The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your ZyWALL.</p> <p>You cannot upload a configuration file named system-default.conf or lastgood.conf. If you upload startup-config.conf, it will replace the current configuration and immediately apply the new settings.</p>
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a file of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	<p>Click Upload to begin the upload process. This process may take up to two minutes.</p> <p>Note: Do not turn off the ZyWALL while configuration file upload is in progress.</p>

9.3 Firmware Package Screen

Click **File Manager > Firmware Package** to open the **Firmware Package** screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the ZyWALL.

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "zywall.bin". The ZyWALL automatically reboots after a successful upload.

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

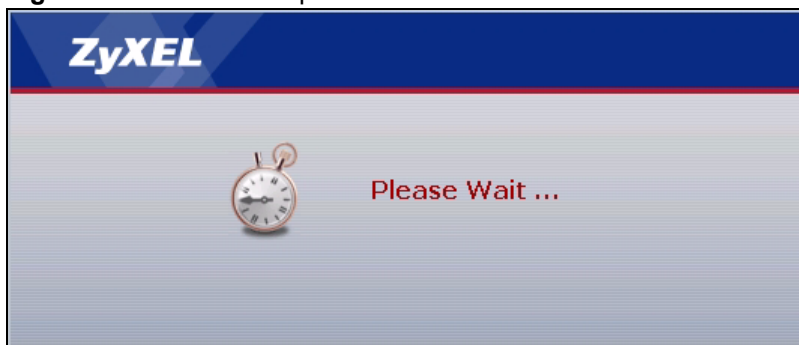
Figure 120 File Manager > Firmware Package

The following table describes the labels in this screen.

Table 41 File Manager > Firmware Package

LABEL	DESCRIPTION
Boot Module	This is the version of the boot module that is currently on the ZyWALL.
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.

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

Figure 121 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.

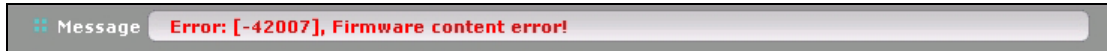
Figure 122 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **HOME** screen.

If the upload was not successful, the following message appears in the status bar at the bottom of the screen.

Figure 123 Firmware Upload Error



9.4 Shell Script Screen

Use shell script files to have the ZyWALL use commands that you specify. Use a text editor to create the shell script files. They must use a “.zysh” filename extension.

Click **File Manager > Shell Script** to open the **Shell Script** screen. Use the **Shell Script** screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the ZyWALL at the same time.

Note: You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the ZyWALL restarts. You could multiple `write` commands in a long script.

Figure 124 File Manager > Shell Script



Each field is described in the following table.

Table 42 File Manager > Shell Script



LABEL	DESCRIPTION
Download	Click a shell script file's row to select it and click Download to save the configuration to your computer.
Copy	<p>Use this button to save a duplicate of a shell script file on the ZyWALL. Click a shell script file's row to select it and click Copy to open the Copy File screen.</p> <p>Figure 125 File Manager > Shell Script > Copy</p>  <p>Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;~!@#%&()_+[]{}',.-).</p> <p>Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.</p>
Rename	<p>Use this button to change the label of a shell script file on the ZyWALL. You cannot rename a shell script to the name of another shell script in the ZyWALL. Click a shell script's row to select it and click Rename to open the Rename File screen.</p> <p>Figure 126 File Manager > Shell Script > Rename</p>  <p>Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;~!@#%&()_+[]{}',.-).</p> <p>Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.</p>
Delete	<p>Click a shell script file's row to select it and click Delete to delete the shell script file from the ZyWALL.</p> <p>A pop-up window asks you to confirm that you want to delete the shell script file. Click OK to delete the shell script file or click Cancel to close the screen without deleting the shell script file.</p>
Run	<p>Use this button to have the ZyWALL use a specific shell script file. Click a shell script file's row to select it and click Run to have the ZyWALL use that shell script file. You may need to wait awhile for the ZyWALL to finish applying the commands.</p>
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.

Table 42 File Manager > Shell Script (continued)

LABEL	DESCRIPTION
Modify	This column displays the date and time that the individual shell script files were last changed or saved.
	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your ZyWALL.
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .zysh file you want to upload.
Upload	Click Upload to begin the upload process. This process may take up to several minutes.

CHAPTER 10

Interface

See the [Interface section](#) in the Configuration Overview chapter for related information on these screens.

10.1 Interface Overview

In general, an interface has the following characteristics.

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.
- An interface is bound to at most one zone.
- Many interface can belong to the same zone.
- Layer-3 virtualization (IP alias, for example) is a kind of interface.

Some characteristics do not apply to some types of interfaces.

10.1.1 Types of Interfaces

You can create several types of interfaces in the ZyWALL.

- **Port groups** create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **VLAN interfaces** receive and send tagged frames. The ZyWALL automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the ZyWALL. You can also assign an IP address and subnet mask to the bridge.
- **PPPoE/PPTP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Virtual interfaces** provide additional routing information in the ZyWALL. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.

- The **auxiliary interface**, along with an external modem, provides an interface the ZyWALL can use to dial out. This interface can be used as a backup WAN interface, for example. The auxiliary interface controls the **DIAL BACKUP** port.
- **Trunks** manage load balancing between interfaces.

Port groups, trunks, and the auxiliary interface have a lot of characteristics that are specific to each type of interface. They are discussed in more detail in [Section 10.3.1 on page 190](#), [Chapter 11 on page 215](#), and [Section 10.7.1 on page 211](#), respectively. The other types of interfaces--Ethernet, VLAN, bridge, PPPoE/PPTP, and virtual--have a lot of similar characteristics. These characteristics are listed in the following table and discussed in more detail below.

Table 43 Ethernet, VLAN, Bridge, PPPoE/PPTP, and Virtual Interfaces Characteristics

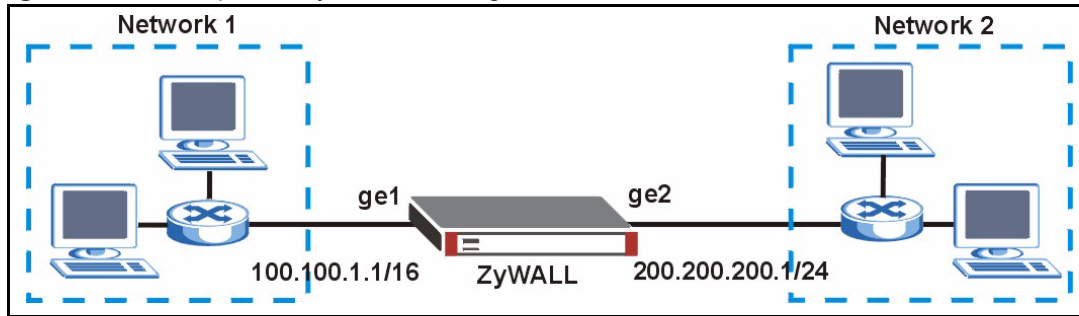
CHARACTERISTICS	ETHERNET	VLAN	BRIDGE	PPPOE/PPTP	VIRTUAL
Name*	gex	vlanx	brx	pppx	**
IP Address Assignment					
static IP address	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	Yes	Yes	Yes	No
routing metric	Yes	Yes	Yes	Yes	Yes
Interface Parameters					
bandwidth restrictions	Yes	Yes	Yes	Yes	Yes
packet size (MTU)	Yes	Yes	Yes	Yes	No
DHCP					
DHCP server	Yes	Yes	Yes	No	No
DHCP relay	Yes	Yes	Yes	No	No
Ping Check	Yes	Yes	Yes	Yes	No

* - The format of interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (x, limited by the maximum number of each type of interface). For example, Ethernet interface names are ge1, ge2, ge3, ...; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface ge1 are called ge1:1, ge1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the web configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

10.1.2 IP Address Assignment

Most interfaces have an IP address and a subnet mask. This information is used to create an entry in the routing table.

Figure 127 Example: Entry in the Routing Table Derived from Interfaces**Table 44** Example: Routing Table Entries for Interfaces

IP ADDRESS(ES)	DESTINATION
100.100.1.1/16	ge1
200.200.200.1/24	ge2

For example, if the ZyWALL gets a packet with a destination address of 100.100.25.25, it routes the packet to interface ge1. If the ZyWALL gets a packet with a destination address of 200.200.200.200, it routes the packet to interface ge2.

In most interfaces, you can enter the IP address and subnet mask manually. In PPPoE/PPTP interfaces, however, the subnet mask is always 255.255.255.255 because it is a point-to-point interface. For these interfaces, you can only enter the IP address.

In many interfaces, you can also let the IP address and subnet mask be assigned by an external DHCP server on the network. In this case, the interface is a DHCP client. Virtual interfaces, however, cannot be DHCP clients. You have to assign the IP address and subnet mask manually.

In general, the IP address and subnet mask of each interface should not overlap, though it is possible for this to happen with DHCP clients.

In the example above, if the ZyWALL gets a packet with a destination address of 5.5.5.5, it might not find any entries in the routing table. In this case, the packet is dropped. However, if there is a default router to which the ZyWALL should send this packet, you can specify it as a gateway in one of the interfaces. For example, if there is a default router at 200.200.200.100, you can create a gateway at 200.200.200.100 on ge2. In this case, the ZyWALL creates the following entry in the routing table.

Table 45 Example: Routing Table Entry for a Gateway

IP ADDRESS(ES)	DESTINATION
0.0.0.0/0	200.200.200.100

The gateway is an optional setting for each interface. If there is more than one gateway, the ZyWALL uses the gateway with the lowest metric, or cost. If two or more gateways have the same metric, the ZyWALL uses the one that was set up first (the first entry in the routing table). In PPPoE/PPTP interfaces, the other computer is the gateway for the interface by default. In this case, you should specify the metric.

If the interface gets its IP address and subnet mask from a DHCP server, the DHCP server also specifies the gateway, if any.

10.1.3 Interface Parameters

The ZyWALL restricts the amount of traffic into and out of the ZyWALL through each interface.

- Upstream bandwidth is the amount of traffic from the ZyWALL through the interface to the network.
- Downstream bandwidth is the amount of traffic from the network through the interface into the ZyWALL.¹

If you set the bandwidth restrictions very high, you effectively remove the restrictions.

The ZyWALL also restricts the size of each data packet. The maximum number of bytes in each packet is called the maximum transmission unit (MTU). If a packet is larger than the MTU, the ZyWALL divides it into smaller fragments. Each fragment is sent separately, and the original packet is re-assembled later. The smaller the MTU, the more fragments sent, and the more work required to re-assemble packets correctly. On the other hand, some communication channels, such as Ethernet over ATM, might not be able to handle large data packets.

10.1.4 DHCP Settings

Dynamic Host Configuration Protocol (DHCP, RFC 2131, RFC 2132) provides a way to automatically set up and maintain IP addresses, subnet masks, gateways, and some network information (such as the IP addresses of DNS servers) on computers in the network. This reduces the amount of manual configuration you have to do and usually uses available IP addresses more efficiently.

In DHCP, every network has at least one DHCP server. When a computer (a DHCP client) joins the network, it submits a DHCP request. The DHCP servers get the request; assign an IP address; and provide the IP address, subnet mask, gateway, and available network information to the DHCP client. When the DHCP client leaves the network, the DHCP servers can assign its IP address to another DHCP client.

In the ZyWALL, some interfaces can provide DHCP services to the network. In this case, the interface can be a DHCP relay or a DHCP server.

1. At the time of writing, the ZyWALL does not support downstream bandwidth management.

As a DHCP relay, the interface routes DHCP requests to DHCP servers on different networks. You can specify more than one DHCP server. If you do, the interface routes DHCP requests to all of them. It is possible for an interface to be a DHCP relay and a DHCP client simultaneously.

As a DHCP server, the interface provides the following information to DHCP clients.

- IP address - If the DHCP client's MAC address is in the ZyWALL's static DHCP table, the interface assigns the corresponding IP address. If not, the interface assigns IP addresses from a pool, defined by the starting address of the pool and the pool size.

Table 46 Example: Assigning IP Addresses from a Pool

START IP ADDRESS	POOL SIZE	RANGE OF ASSIGNED IP ADDRESS
50.50.50.33	5	50.50.50.33 - 50.50.50.37
75.75.75.1	200	75.75.75.1 - 75.75.75.200
99.99.1.1	1023	99.99.1.1 - 99.99.4.255
120.120.120.100	100	120.120.120.100 - 120.120.120.199

The ZyWALL cannot assign the first address (network address) or the last address (broadcast address) in the subnet defined by the interface's IP address and subnet mask. For example, in the first entry, if the subnet mask is 255.255.255.0, the ZyWALL cannot assign 50.50.50.0 or 50.50.50.255. If the subnet mask is 255.255.0.0, the ZyWALL cannot assign 50.50.0.0 or 50.50.255.255. Otherwise, it can assign every IP address in the range, except the interface's IP address.

If you do not specify the starting address or the pool size, the interface the maximum range of IP addresses allowed by the interface's IP address and subnet mask. For example, if the interface's IP address is 9.9.9.1 and subnet mask is 255.255.255.0, the starting IP address in the pool is 9.9.9.2, and the pool size is 253.

- Subnet mask - The interface provides the same subnet mask you specify for the interface. See [Section 10.1.2 on page 178](#).
- Gateway - The interface provides the same gateway you specify for the interface. See [Section 10.1.2 on page 178](#).
- DNS servers - The interface provides IP addresses for up to three DNS servers that provide DNS services for DHCP clients. You can specify each IP address manually (for example, a company's own DNS server), or you can refer to DNS servers that other interfaces received from DHCP servers (for example, a DNS server at an ISP). These other interfaces have to be DHCP clients.

It is not possible for an interface to be the DHCP server and a DHCP client simultaneously.

10.1.5 Ping Check Settings

The interface can regularly ping the gateway you specified (see [Section 10.1.2 on page 178](#)) to make sure it is still available. You specify how often the interface pings the gateway, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway acknowledges the ping.

10.1.6 Relationships Between Interfaces

In the ZyWALL, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports (or port groups). The relationships between interfaces are explained in the following table.

Table 47 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
auxiliary interface	auxiliary port
port group	physical port
Ethernet interface	physical port port group
VLAN interface	Ethernet interface
bridge interface	Ethernet interface* VLAN interface*
PPPoE/PPTP interface	Ethernet interface* VLAN interface* bridge interface
virtual interface (virtual Ethernet interface) (virtual VLAN interface) (virtual bridge interface)	Ethernet interface* VLAN interface* bridge interface
trunk	Ethernet interface VLAN interface bridge interface PPPoE/PPTP interface auxiliary interface

* - You cannot set up a PPPoE/PPTP interface, virtual Ethernet interface or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPPoE/PPTP interface on top of it.

10.2 Ethernet Interfaces

This section introduces Ethernet interfaces and then explains the screens for Ethernet interfaces.

10.2.1 Ethernet Interfaces Overview

The ZyWALL has five Ethernet interfaces: ge1, ge2, ge3, ge4, and ge5. Unlike other types of interfaces, you cannot create new Ethernet interfaces nor can you delete any of these five. If you do not assign any physical ports to an Ethernet interface (see [Section 10.3.1 on page 190](#)), the Ethernet interface is effectively removed from the ZyWALL, but you can still configure it.

Ethernet interfaces are similar to other types of interfaces in many other ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict the amount of bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

In addition, you use Ethernet interfaces to control which physical ports exchange routing information with other routers and how much information is exchanged through each one. The more routing information is exchanged, the more efficient the routers should be. However, the routers also generate more network traffic, and some routing protocols require a significant amount of configuration and management.

The ZyWALL supports two routing protocols, RIP and OSPF. See [Chapter 13 on page 255](#) for background information about these routing protocols.

With RIP, you can use Ethernet interfaces to do the following things.

- Enable and disable RIP in the underlying physical port or port group.
- Select which direction(s) routing information is exchanged - The ZyWALL can receive routing information, send routing information, or do both.
- Select which version of RIP to support in each direction - The ZyWALL supports RIP-1, RIP-2, and both versions.
- Select the broadcasting method used by RIP-2 packets - The ZyWALL can use subnet broadcasting or multicasting.



















With OSPF, you can use Ethernet interfaces to do the following things.

- Enable and disable OSPF in the underlying physical port or port group.
- Select the area to which the interface belongs.
- Override the default link cost and authentication method for the selected area.
- Select in which direction(s) routing information is exchanged - The ZyWALL can receive routing information, send routing information, or do both.
- Set the priority used to identify the DR or BDR if one does not exist.

10.2.2 Ethernet Summary Screen

This screen lists every Ethernet interface and virtual interface created on top of Ethernet interfaces. To access this screen, click **Network > Interface**.

Figure 128 Network > Interface > Ethernet

#	Name	IP Address	Mask	Modify
1	ge1	STATIC -- 192.168.105.1	255.255.255.0	  
2	ge2	STATIC -- 211.72.158.115	255.255.255.240	  
3	ge3	STATIC -- 172.23.19.224	255.255.255.0	  
4	ge3:1	192.168.1.100	255.255.255.0	  
5	ge4	STATIC -- 192.168.3.1	255.255.255.0	  
6	ge5	STATIC -- 0.0.0.0	0.0.0.0	  

Each field is described in the following table.

Table 48 Network > Interface > Ethernet

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the interface.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (STATIC) or dynamically assigned (DHCP). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Modify	This column lets you create, edit, remove, activate, and deactivate interfaces. You cannot add or remove Ethernet interfaces, however. To create a virtual Ethernet interface, click the Add icon next to the corresponding Ethernet interface. The Virtual Interface Add/Edit screen appears. See Section 10.8 on page 213 . To edit an interface, click the Edit icon next to it. The Ethernet Edit screen or Virtual Interface Add/Edit screen appears accordingly. To remove a virtual interface, click the Remove icon next to it. The ZyWALL confirms you want to remove it before doing so. To activate or deactivate an interface, click the Active icon next to it.

10.2.3 Ethernet Edit

The **Ethernet Edit** screen lets you configure IP address assignment, interface parameters, RIP settings, OSPF settings, DHCP settings, and ping check settings. To access this screen, click an **Edit** icon in the **Ethernet Summary** screen. (See [Section 10.2.2 on page 184](#).)

Figure 129 Network > Interface > Ethernet > Edit

Ethernet Interface Properties	
<input checked="" type="checkbox"/> Enable	
Interface Name	ge1
Description	<input type="text"/> (Optional)
IP Address Assignment	
<input type="radio"/> Get Automatically	<input type="text"/>
<input checked="" type="radio"/> Use Fixed IP Address	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	<input type="text"/> (Optional)
Metric	0 (0-15)
Interface Parameters	
Upstream Bandwidth	1048576 Kbps
Downstream Bandwidth	1048576 Kbps
MTU	1500 Bytes
RIP Setting	
<input type="checkbox"/> Enable RIP	
Direction	BiDir
Send Version	2
Receive Version	2
<input type="checkbox"/> V2-Broadcast	
OSPF Setting	
Area	None
Priority	1 (0-255)
Link Cost	10 (1-65535)
<input type="checkbox"/> Passive Interface	
Authentication	None
DHCP Setting	
DHCP	DHCP Server
IP Pool Start Address (Optional)	192.168.1.33
First DNS Server (Optional)	From ISP
Second DNS server (Optional)	From ISP
Third DNS Server (Optional)	Custom Defined
Lease time	<input type="radio"/> infinite <input checked="" type="radio"/> 2 days 0 hours (Optional) 0 minutes
Static DHCP Table	<input type="button" value="Add Static DHCP"/>
Ping Check	
<input type="checkbox"/> Enable	
Check Period	<input type="text"/> (5-30 seconds)
Check Timeout	<input type="text"/> (1-10 seconds)
Check Fail Tolerance	<input type="text"/> (1-10)
<input type="radio"/> Ping Default Gateway	0.0.0.0
<input checked="" type="radio"/> Ping this address	<input type="text"/> (Domain Name or IP Address)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Each field is described in the table below.

Table 49 Network > Interface > Ethernet > Edit

LABEL	DESCRIPTION
Ethernet Interface Properties	
Enable	Select this to enable this interface. Clear this to disable this interface.
Interface Name	This field is read-only. This is the name of the Ethernet interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically. You should not select this if the interface is assigned to a VRRP group. See Chapter 16 on page 275 .
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select Use Fixed IP Address . Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select Use Fixed IP Address . Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select Use Fixed IP Address . Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Parameters	
Upstream Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Downstream Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
RIP Settings	See Section 13.1.1 on page 255 for more information about RIP.
Enable RIP	Select this to enable RIP in this interface.

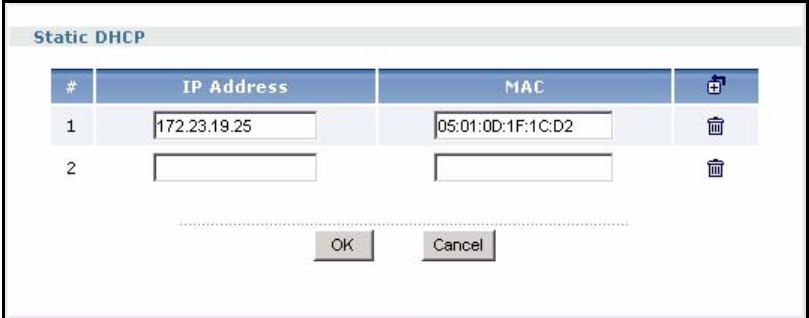
Table 49 Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Direction	<p>This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box.</p> <p>BiDir - This interface sends and receives routing information.</p> <p>In-Only - This interface receives routing information.</p> <p>Out-Only - This interface sends routing information.</p>
Send Version	<p>This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are 1, 2, and 1 and 2.</p>
Receive Version	<p>This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are 1, 2, and 1 and 2.</p>
V2-Broadcast	<p>This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the ZyWALL uses multicasting.</p>
OSPF Settings	<p>See Section 13.3 on page 258 for more information about OSPF.</p>
Area	<p>Select the area in which this interface belongs. Select None to disable OSPF in this interface.</p>
Priority	<p>Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.</p>
Link Cost	<p>Enter the cost (between 1 and 65,535) to route packets through this interface.</p>
Passive Interface	<p>Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.</p>
Authentication	<p>Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are:</p> <p>Same-as-Area - use the default authentication method in the area</p> <p>None - disable authentication</p> <p>Text - authenticate OSPF routing information using a plain-text password</p> <p>MD5 - authenticate OSPF routing information using MD5 encryption</p>
Text Authentication Key	<p>This field is available if the Authentication is Text. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to eight characters long.</p>
MD5 Authentication ID	<p>This field is available if the Authentication is MD5. Type the ID for MD5 authentication. The ID can be between 1 and 255.</p>
MD5 Authentication Key	<p>This field is available if the Authentication is MD5. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.</p>
DHCP Settings	
DHCP	<p>Select what type of DHCP service the ZyWALL provides to the network. Choices are:</p> <p>None - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network.</p> <p>DHCP Relay - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.</p> <p>DHCP Server - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network.</p>
	<p>These fields appear if the ZyWALL is a DHCP Relay.</p>

Table 49 Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
These fields appear if the ZyWALL is a DHCP Server .	
IP Pool Start Address	Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click Add Static DHCP . If this field is blank, the Pool Size must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask . For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the IP Pool Start Address must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses of a maximum of three DNS servers that the network can use. The ZyWALL provides these IP addresses to DHCP clients. You can specify these IP addresses two ways. Custom Defined - enter a static IP address. From ISP - use the IP address of a DNS server that another interface received from its DHCP server.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: infinite - select this if IP addresses never expire. days, hours, and minutes - select this to enter how long IP addresses are valid.

Table 49 Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
<p>Add Static DHCP</p>	<p>Click this if you want the ZyWALL to assign static IP addresses to computers. The Static DHCP screen appears.</p> <p>Figure 130 Network > Interface > Edit > Add Static DHCP</p>  <p>The ZyWALL checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the ZyWALL assigns the corresponding IP address. Otherwise, the ZyWALL assigns the IP address dynamically using the IP Pool Start Address and Pool Size.</p> <p>Note: You must click OK in the Static DHCP screen and then click OK in this screen to save your changes.</p>
<p>Ping Check</p>	<p>The interface can regularly ping the gateway you specified to make sure it is still available. You specify how often the interface pings the gateway, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway acknowledges the ping.</p>
<p>Enable</p>	<p>Select this to enable the ping check.</p>
<p>Check Period</p>	<p>Enter the number of seconds between ping attempts.</p>
<p>Check Timeout</p>	<p>Enter the number of seconds to wait for a response before the attempt is a failure.</p>
<p>Check Fail Tolerance</p>	<p>Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.</p>
<p>Ping Default Gateway</p>	<p>Select this to ping the default gateway.</p>
<p>Ping this address</p>	<p>Select this to ping a specified domain name or IP address. Enter that domain name or IP address in the field next to it.</p>

10.3 Port Grouping

This section introduces port groups and then explains the screen for port groups.

10.3.1 Port Grouping Overview

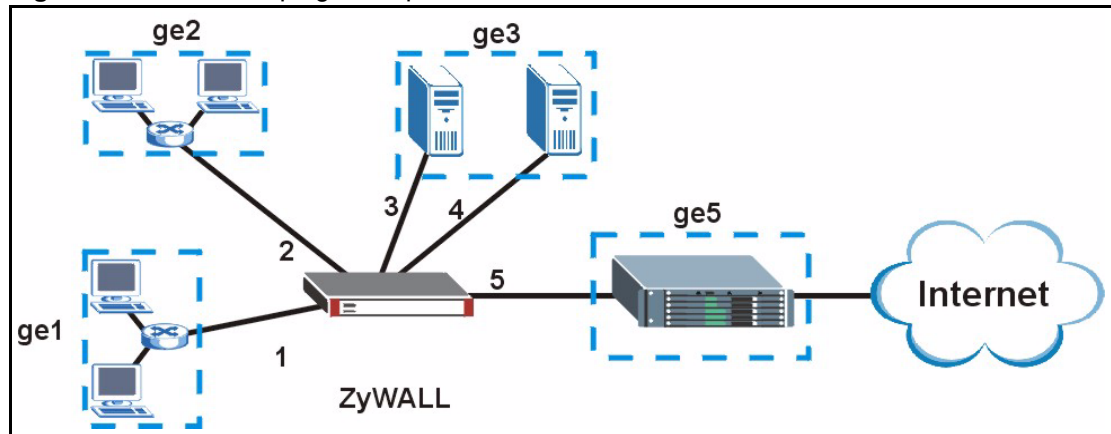
Use port grouping to create port groups and to assign physical ports and port groups to Ethernet interfaces.

Each physical port is assigned to one Ethernet interface. In port grouping, the Ethernet interfaces are called **representative interfaces**. If you assign more than one physical port to a representative interface, you create a **port group**. Port groups have the following characteristics:

- There is a layer-2 Ethernet switch between physical ports in the port group. This provides wire-speed throughput but no security.
- It can increase the bandwidth between the port group and other interfaces.

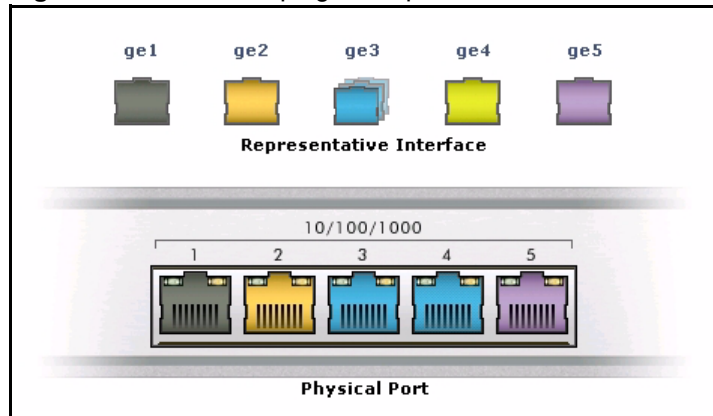
In the example below, you might combine physical ports 3 and 4 into port group ge3.

Figure 131 Port Grouping Example: Network



In this case, click [Network > Interface > Port Grouping](#), and set up the screen like this.

Figure 132 Port Grouping Example: Screen

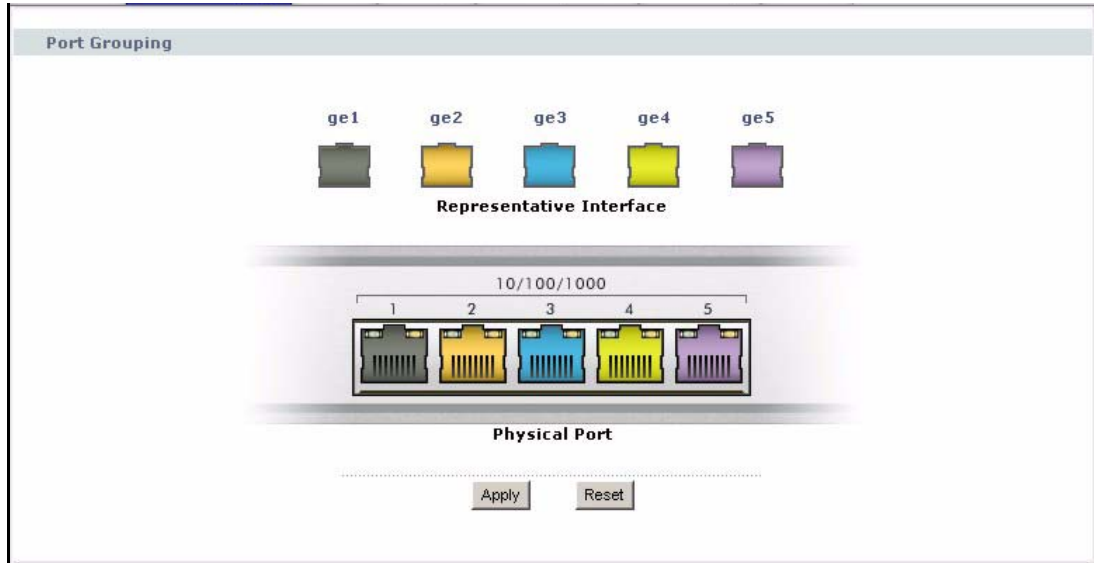


There are no ports assigned to ge4. If you do not assign any physical ports to a representative interface, you cannot use this interface to create other interfaces or create IPsec VPN tunnels. The Ethernet interface is still displayed in the screen, however, and the existing configuration remains.

10.3.2 Port Grouping Screen

You can maintain the relationship between physical ports, port groups, and Ethernet interfaces in the **Port Grouping** screen. To access this screen, click **Network > Interface > Port Grouping**.

Figure 133 Network > Interface > Port Grouping



Each section in this screen is described below.

Table 50 Network > Interface > Port Grouping

LABEL	DESCRIPTION
Representative Interface (ge1, ge2, ge3, ge4, ge5)	These are Ethernet interfaces. To add a physical port to a representative interface, drag the physical port onto the corresponding representative interface.
Physical Port (1, 2, 3, 4, 5)	These are the physical ports as they appear on the front panel of the ZyWALL. To add a physical port to a representative interface, drag the physical port onto the corresponding representative interface.
Apply	Click this button to save your changes and apply them to the ZyWALL.
Reset	Click this button to change the port groups to their current configuration (last-saved values).

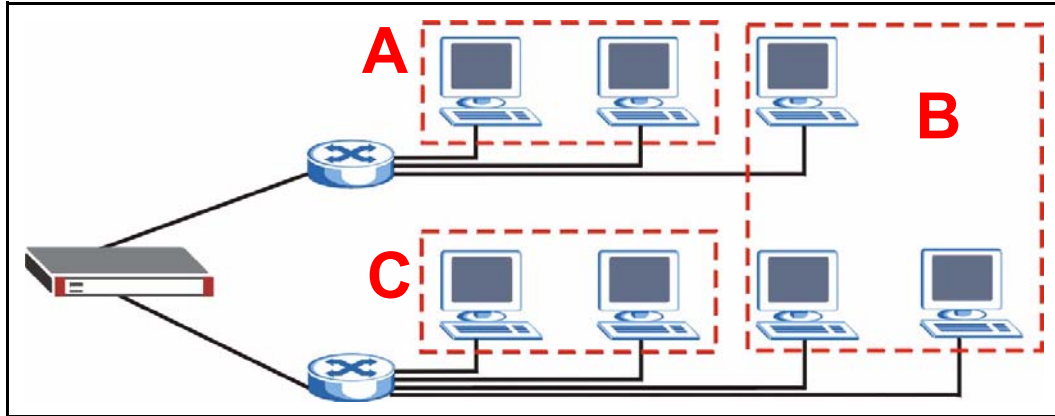
10.4 VLAN Interfaces

This section introduces VLAN and VLAN interfaces and then explains the screens for VLAN interfaces.

10.4.1 VLAN Overview

A Virtual Local Area Network (VLAN) divides a physical network into multiple logical networks. The standard is defined in IEEE 802.1q.

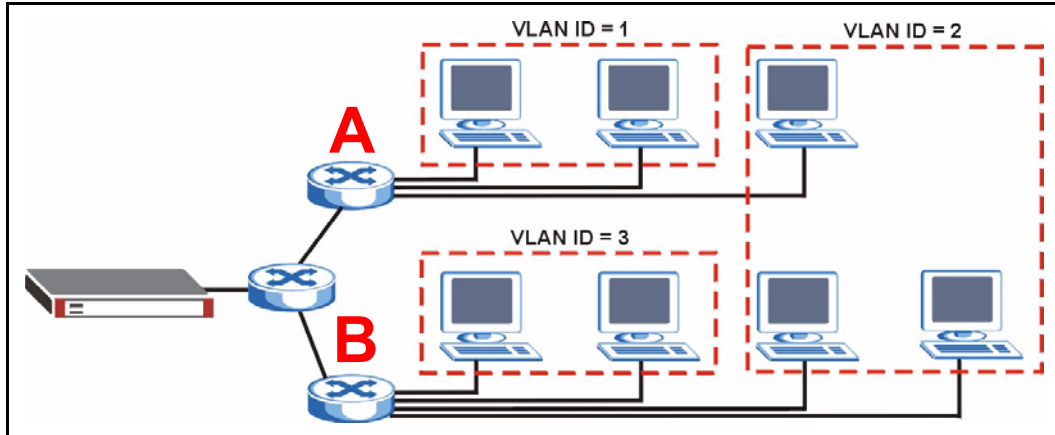
Figure 134 Example: Before VLAN



In this example, there are two physical networks and three departments **A**, **B**, and **C**. The physical networks are connected to hubs, and the hubs are connected to the router.

Alternatively, you can divide the physical networks into three VLANs.

Figure 135 Example: After VLAN



Each VLAN is a separate network with separate IP addresses, subnet masks, and gateways. Each VLAN also has a unique identification number (ID). The ID is a 12-bit value that is stored in the MAC header. The VLANs are connected to switches, and the switches are connected to the router. (If one switch has enough connections for the entire network, the network does not need switches **A** and **B**.)

- Traffic inside each VLAN is layer-2 communication (data link layer, MAC addresses). It is handled by the switches. As a result, the new switch is required to handle traffic inside VLAN 2. Traffic is only broadcast inside each VLAN, not each physical network.
- Traffic between VLANs (or between a VLAN and another type of network) is layer-3 communication (network layer, IP addresses). It is handled by the router.

This approach provides a few advantages.

- Increased performance - In VLAN 2, the extra switch should route traffic inside the sales department faster than the router does. In addition, broadcasts are limited to smaller, more logical groups of users.
- Higher security - If each computer has a separate physical connection to the switch, then broadcast traffic in each VLAN is never sent to computers in another VLAN.
- Better manageability - You can align network policies more appropriately for users. For example, you can create different content filtering rules for each VLAN (each department in the example above), and you can set different bandwidth limits for each VLAN. These rules are also independent of the physical network, so you can change the physical network without changing policies.

In this example, the new switch handles the following types of traffic:

- Inside VLAN 2.
- Between the router and VLAN 1.
- Between the router and VLAN 2.
- Between the router and VLAN 3.

10.4.2 VLAN Interfaces Overview

In the ZyWALL, each VLAN is called a VLAN interface. As a router, the ZyWALL routes traffic between VLAN interfaces, but it does not route traffic within a VLAN interface. All traffic for each VLAN interface can go through only one Ethernet interface, though each Ethernet interface can have one or more VLAN interfaces.

Note: Each VLAN interface is created on top of only one Ethernet interface.

Otherwise, VLAN interfaces are similar to other interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

10.4.3 VLAN Summary Screen

This screen lists every VLAN interface and virtual interface created on top of VLAN interfaces. To access this screen, click **Network > Interface > VLAN**.

Figure 136 Network > Interface > VLAN

#	Name	Port/VID	IP Address	Mask	
1	vlan0	ge1/1234	DHCP --0.0.0.0	0.0.0.0	
2	vlan0:1		199.100.111.255	255.255.255.0	
3	vlan4	ge3/300	STATIC --192.100.111.0	255.255.255.0	

Each field is explained in the following table.

Table 51 Network > Interface > VLAN

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the interface.
Port/VID	For VLAN interfaces, this field displays <ul style="list-style-type: none"> the Ethernet interface on which the VLAN interface is created the VLAN ID For virtual interfaces, this field is blank.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (STATIC) or dynamically assigned (DHCP). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Add icon	This column lets you create, edit, remove, activate, and deactivate interfaces. To create a VLAN interface, click the Add icon at the top of the column. The VLAN Add/Edit screen appears. To create a virtual VLAN interface, click the Add icon next to the corresponding VLAN interface. The Virtual Interface Add/Edit screen appears. See Section 10.8 on page 213 . To edit an interface, click the Edit icon next to it. The VLAN Add/Edit screen or Virtual Interface Add/Edit screen appears accordingly. To remove an interface, click the Remove icon next to it. The ZyWALL confirms you want to remove it before doing so. To activate or deactivate an interface, click the Active icon next to it.

10.4.4 VLAN Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and ping check for each VLAN interface. To access this screen, click the **Add** icon at the top of the **Add** column or click an **Edit** icon next to a VLAN interface in the **VLAN Summary** screen. The following screen appears.

Figure 137 Network > Interface > VLAN > Edit

VLAN Interface Properties

Enable

Interface Name: vlan1

Port: ge4

Virtual LAN Tag: 666 (1-4094)

Description: (Optional)

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address: 25.25.25.1

Subnet Mask: 255.255.255.0

Gateway: (Optional)

Metric: 0 (0-15)

Interface Parameters

Upstream Bandwidth: 1048576 Kbps

Downstream Bandwidth: 1048576 Kbps

MTU: 1500 Bytes

DHCP Setting

DHCP: DHCP Server

IP Pool Start Address (Optional): Pool Size:

First DNS Server (Optional): Custom Defined

Second DNS server (Optional): Custom Defined

Third DNS Server (Optional): Custom Defined

Lease time: infinite

3 days 0 hours (Optional) 0 minutes

Static DHCP Table:

Ping Check

Enable

Check Period: 30 (5-30 seconds)

Check Timeout: 5 (1-10 seconds)

Check Fail Tolerance: 5 (1-10)

Ping Default Gateway: 0.0.0.0

Ping this address: (Domain Name or IP Address)

Each field is explained in the following table.

Table 52 Network > Interface > VLAN > Edit

LABEL	DESCRIPTION
VLAN Interface Properties	
Enable	Select this to enable this interface. Clear this to disable this interface.

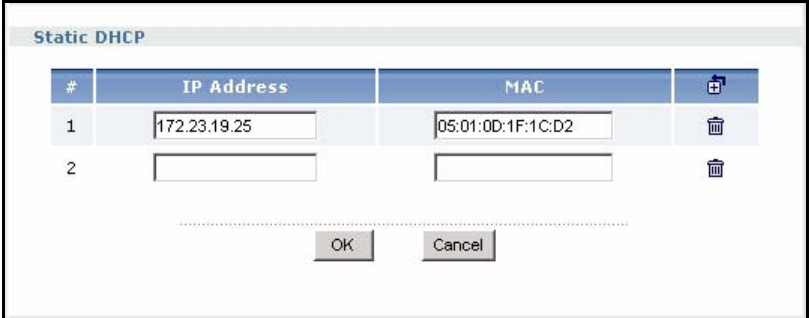
Table 52 Network > Interface > VLAN > Edit (continued)

LABEL	DESCRIPTION
Interface Name	This field is read-only if you are editing the interface. Enter the name of the VLAN interface. The format is vlanx, where x is 0 - 31. For example, vlan0, vlan8, and so on.
Port	Select the Ethernet interface on which the VLAN interface runs.
Virtual LAN Tag	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically. You should not select this if the interface is assigned to a VRRP group. See Chapter 16 on page 275 .
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select Use Fixed IP Address . Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select Use Fixed IP Address . Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select Use Fixed IP Address . Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Parameters	
Upstream Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Downstream Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
DHCP Settings	

Table 52 Network > Interface > VLAN > Edit (continued)

LABEL	DESCRIPTION
DHCP	<p>Select what type of DHCP service the ZyWALL provides to the network. Choices are:</p> <p>None - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network.</p> <p>DHCP Relay - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.</p> <p>DHCP Server - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network.</p>
	These fields appear if the ZyWALL is a DHCP Relay .
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the ZyWALL is a DHCP Server .
IP Pool Start Address	<p>Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click Add Static DHCP.</p> <p>If this field is blank, the Pool Size must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.</p>
Pool Size	<p>Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.</p> <p>If this field is blank, the IP Pool Start Address must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.</p>
First DNS Server Second DNS Server Third DNS Server	<p>Specify the IP addresses of a maximum of three DNS servers that the network can use. You can specify these IP addresses two ways.</p> <p>Custom Defined - enter a static IP address</p> <p>From ISP - use the IP address of a DNS server that another interface received from its DHCP server.</p>
Lease time	<p>Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are:</p> <p>infinite - select this if IP addresses never expire</p> <p>days, hours, and minutes - select this to enter how long IP addresses are valid.</p>

Table 52 Network > Interface > VLAN > Edit (continued)

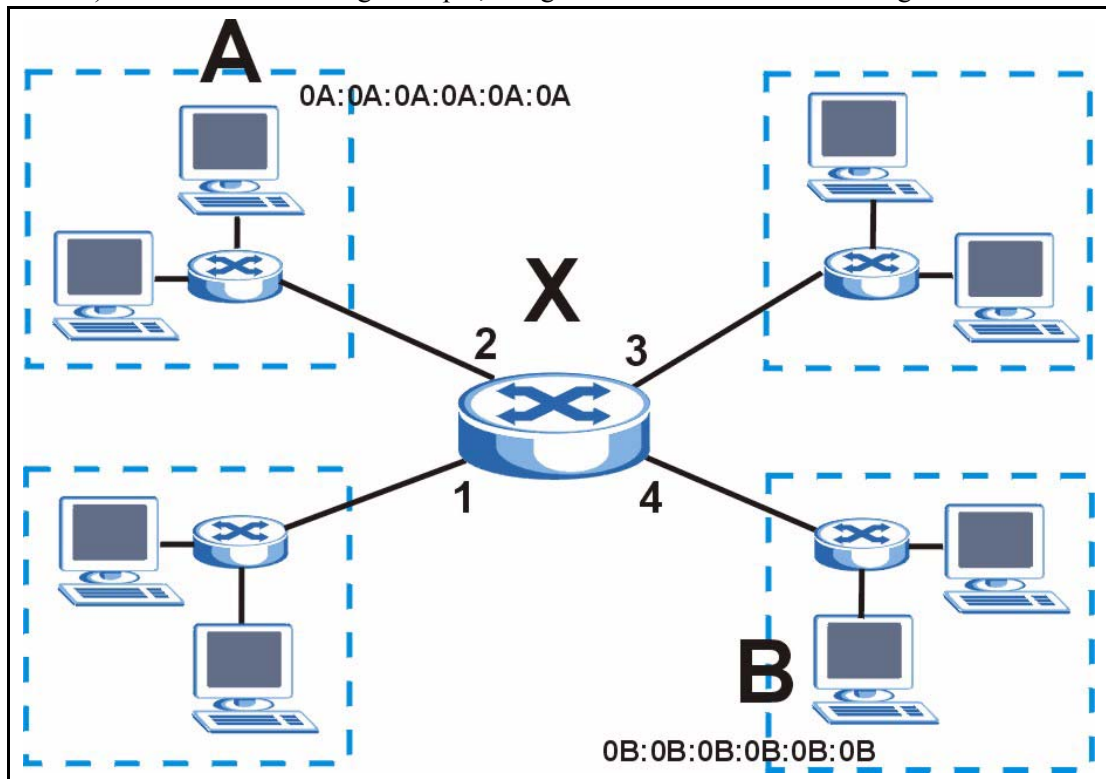
LABEL	DESCRIPTION
Add Static DHCP	<p>Click this if you want the ZyWALL to assign static IP addresses to computers. The Static DHCP screen appears.</p> <p>Figure 138 Network > Interface > Edit > Add Static DHCP</p>  <p>The ZyWALL checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the ZyWALL assigns the corresponding IP address. Otherwise, the ZyWALL assigns the IP address dynamically using the IP Pool Start Address and Pool Size.</p> <p>Note: You must click OK in the Static DHCP screen and then click OK in this screen to save your changes.</p>
Ping Check	The interface can regularly ping the gateway you specified to make sure it is still available. You specify how often the interface pings the gateway, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway acknowledges the ping.
Enable	Select this to enable the ping check.
Check Period	Enter the number of seconds between ping attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Ping Default Gateway	Select this to ping the default gateway.
Ping this address	Select this to ping a specified domain name or IP address. Enter that domain name or IP address in the field next to it.

10.5 Bridge Interfaces

This section introduces bridges and bridge interfaces and then explains the screens for bridge interfaces.

10.5.1 Bridge Overview

A bridge creates a connection between two or more network segments at the layer-2 (MAC address) level. In the following example, bridge X connects four network segments.



When the bridge receives a packet, the bridge records the source MAC address and the port on which it was received in a table. It also looks up the destination MAC address in the table. If the bridge knows on which port the destination MAC address is located, it sends the packet to that port. If the destination MAC address is not in the table, the bridge broadcasts the packet on every port (except the one on which it was received).

In the example above, computer A sends a packet to computer B. Bridge X records the source address 0A:0A:0A:0A:0A:0A and port 2 in the table. It also looks up 0B:0B:0B:0B:0B:0B in the table. There is no entry yet, so the bridge broadcasts the packet on ports 1, 3, and 4.

Table 53 Example: Bridge Table After Computer A Sends a Packet to Computer B

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2

If computer B responds to computer A, bridge X records the source address 0B:0B:0B:0B:0B:0B and port 4 in the table. It also looks up 0A:0A:0A:0A:0A:0A in the table and sends the packet to port 2 accordingly.

Table 54 Example: Bridge Table After Computer B Responds to Computer A

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2
0B:0B:0B:0B:0B:0B	4

10.5.2 Bridge Interface Overview

A bridge interface creates a software bridge between the members of the bridge interface. It also becomes the ZyWALL's interface for the resulting network.

A bridge interface may consist of the following members:

- Zero or one VLAN interfaces (and any associated virtual VLAN interfaces)
- Any number of Ethernet interfaces (and any associated virtual Ethernet interfaces)

When you create a bridge interface, the ZyWALL removes the members' entries from the routing table and adds the bridge interface's entries to the routing table. For example, this table shows the routing table before and after you create bridge interface br0 (250.250.250.0/23) between ge1 and vlan1.

Table 55 Example: Routing Table Before and After Bridge Interface br0 Is Created

IP ADDRESS(ES)	DESTINATION
210.210.210.0/24	ge1
210.211.1.0/24	ge1:1
221.221.221.0/24	vlan0
222.222.222.0/24	vlan1
230.230.230.192/26	ge3
241.241.241.241/32	ge4
242.242.242.242/32	ge5

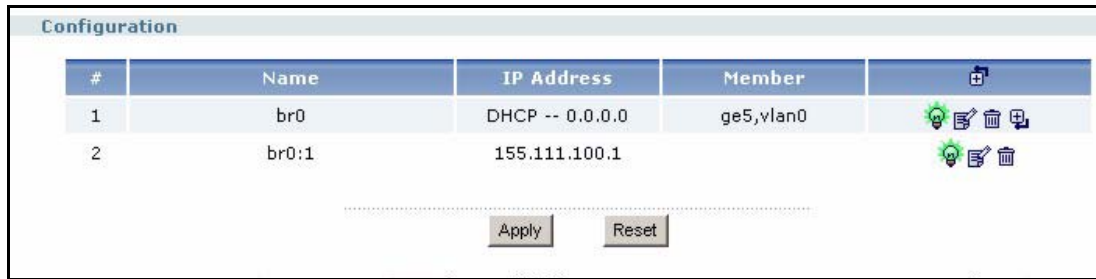
IP ADDRESS(ES)	DESTINATION
221.221.221.0/24	vlan0
230.230.230.192/26	ge3
241.241.241.241/32	ge4
242.242.242.242/32	ge5
250.250.250.0/23	br0

In this example, virtual Ethernet interface ge1:1 is also removed from the routing table when ge1 is added to br0. Virtual interfaces are automatically added to or removed from a bridge interface when the underlying interface is added or removed.

10.5.3 Bridge Summary

This screen lists every bridge interface and virtual interface created on top of bridge interfaces. To access this screen, click **Network > Interface > Bridge**.

Figure 139 Network > Interface > Bridge



Each field is described in the following table.

Table 56 Network > Interface > Bridge

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the interface.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (STATIC) or dynamically assigned (DHCP). IP addresses are always static in virtual interfaces.
Member	This field displays the Ethernet interfaces and VLAN interfaces in the bridge interface. It is blank for virtual interfaces.
Add icon	This column lets you create, edit, remove, activate, and deactivate interfaces. To create a bridge interface, click the Add icon at the top of the column. The Bridge Add/Edit screen appears. To create a virtual interface, click the Add icon next to the corresponding bridge interface. The Virtual Interface Add/Edit screen appears. See Section 10.8 on page 213 . To edit an interface, click the Edit icon next to it. The Bridge Add/Edit screen or Virtual Interface Add/Edit screen appears accordingly. To remove an interface, click the Remove icon next to it. The ZyWALL confirms you want to remove it before doing so. To activate or deactivate an interface, click the Active icon next to it.

10.5.4 Bridge Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and ping check for each bridge interface. To access this screen, click the **Add** icon at the top of the **Add** column in the **Bridge Summary** screen, or click an **Edit** icon in the **Bridge Summary** screen. The following screen appears.

Figure 140 Network > Interface > Bridge > Edit

Bridge Interface Properties	
<input checked="" type="checkbox"/> Enable	
Interface Name	<input type="text" value="br"/>
Description	<input type="text"/> (Optional)
Member Configuration	
Available	Member
ge1	>>
ge3	
ge4	
ge5	
vlan1	<<
IP Address Assignment	
<input type="radio"/> Get Automatically	<input type="text"/>
<input checked="" type="radio"/> Use Fixed IP Address	
IP Address	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="0.0.0.0"/>
Gateway	<input type="text"/> (Optional)
Metric	<input type="text" value="0"/> (0-15)
Interface Parameters	
Upstream Bandwidth	<input type="text" value="1048576"/> Kbps
Downstream Bandwidth	<input type="text" value="1048576"/> Kbps
MTU	<input type="text" value="1500"/> Bytes
DHCP Setting	
DHCP	<input type="text" value="DHCP Server"/>
IP Pool Start Address (Optional)	<input type="text"/> Pool Size <input type="text"/>
First DNS Server (Optional)	<input type="text" value="Custom Defined"/>
Second DNS server (Optional)	<input type="text" value="Custom Defined"/>
Third DNS Server (Optional)	<input type="text" value="Custom Defined"/>
Lease time	<input type="radio"/> infinite <input checked="" type="radio"/> 3 days 0 hours (Optional) 0 minutes
Static DHCP Table	<input type="text"/> <input type="button" value="Add Static DHCP"/>
Ping Check	
<input type="checkbox"/> Enable	
Check Period	<input type="text" value="30"/> (5-30 seconds)
Check Timeout	<input type="text" value="5"/> (1-10 seconds)
Check Fail Tolerance	<input type="text" value="5"/> (1-10)
<input checked="" type="radio"/> Ping Default Gateway	<input type="text" value="0.0.0.0"/>
<input type="radio"/> Ping this address	<input type="text"/> (Domain Name or IP Address)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

In this example, you are creating a new bridge. If you are editing a bridge, the **Interface Name**

field is read-only. Each field is described in the table below.

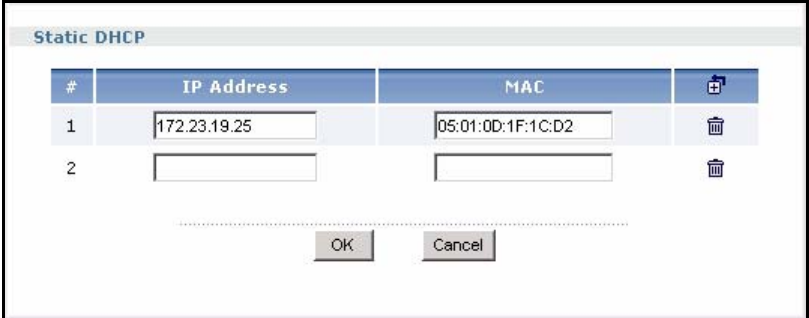
Table 57 Network > Interface > Bridge > Edit

LABEL	DESCRIPTION
Bridge Interface Properties	
Enable	Select this to enable this interface. Clear this to disable this interface.
Interface Name	This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is brx, where x is 0 - 11. For example, br0, br3, and so on.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
Member Configuration	
Available	<p>This field displays Ethernet interfaces and VLAN interfaces that can become part of the bridge interface. An interface is not available in the following situations:</p> <ul style="list-style-type: none"> • There is a virtual interface on top of it • It is already used in a different bridge interface <p>Select one, and click the >> arrow to add it to the bridge interface. Each bridge interface can only have one VLAN interface.</p>
Member	This field displays the interfaces that are part of the bridge interface. Select one, and click the << arrow to remove it from the bridge interface.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select Use Fixed IP Address . Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select Use Fixed IP Address . Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select Use Fixed IP Address . Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Parameters	
Upstream Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Downstream Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.

Table 57 Network > Interface > Bridge > Edit (continued)

LABEL	DESCRIPTION
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
DHCP Settings	
DHCP	<p>Select what type of DHCP service the ZyWALL provides to the network. Choices are:</p> <p>None - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network.</p> <p>DHCP Relay - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.</p> <p>DHCP Server - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network.</p>
	These fields appear if the ZyWALL is a DHCP Relay .
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the ZyWALL is a DHCP Server .
IP Pool Start Address	<p>Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click Add Static DHCP.</p> <p>If this field is blank, the Pool Size must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.</p>
Pool Size	<p>Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.</p> <p>If this field is blank, the IP Pool Start Address must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.</p>
First DNS Server Second DNS Server Third DNS Server	<p>Specify the IP addresses of a maximum of three DNS servers that the network can use. You can specify these IP addresses two ways.</p> <p>Custom Defined - enter a static IP address</p> <p>From ISP - use the IP address of a DNS server that another interface received from its DHCP server.</p>
Lease time	<p>Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are:</p> <p>infinite - select this if IP addresses never expire</p> <p>days, hours, and minutes - select this to enter how long IP addresses are valid.</p>

Table 57 Network > Interface > Bridge > Edit (continued)

LABEL	DESCRIPTION
<p>Add Static DHCP</p>	<p>Click this if you want the ZyWALL to assign static IP addresses to computers. The Static DHCP screen appears.</p> <p>Figure 141 Network > Interface > Edit > Add Static DHCP</p>  <p>The ZyWALL checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the ZyWALL assigns the corresponding IP address. Otherwise, the ZyWALL assigns the IP address dynamically using the IP Pool Start Address and Pool Size.</p> <p>Note: You must click OK in the Static DHCP screen and then click OK in this screen to save your changes.</p>
<p>Ping Check</p>	<p>The interface can regularly ping the gateway you specified to make sure it is still available. You specify how often the interface pings the gateway, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway acknowledges the ping.</p>
<p>Enable</p>	<p>Select this to enable the ping check.</p>
<p>Check Period</p>	<p>Enter the number of seconds between ping attempts.</p>
<p>Check Timeout</p>	<p>Enter the number of seconds to wait for a response before the attempt is a failure.</p>
<p>Check Fail Tolerance</p>	<p>Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.</p>
<p>Ping Default Gateway</p>	<p>Select this to ping the default gateway.</p>
<p>Ping this address</p>	<p>Select this to ping a specified domain name or IP address. Enter that domain name or IP address in the field next to it.</p>

10.6 PPPoE/PPTP Interfaces

This section introduces PPPoE, PPTP, and PPPoE/PPTP interfaces and then explains the screens for PPPoE/PPTP interfaces.

10.6.1 PPPoE/PPTP Overview

Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) and Point-to-Point Tunneling Protocol (PPTP, RFC 2637) are usually used to connect two computers over phone lines or broadband connections.

PPPoE is often used with cable modems and DSL connections. It provides the following advantages:

- The access and authentication method works with existing systems, including RADIUS.
- You can access one of several network services. This makes it easier for the service provider to offer the service
- PPPoE does not usually require any special configuration of the modem.

PPTP is used to set up virtual private networks (VPN) in unsecure TCP/IP environments. It sets up two sessions.

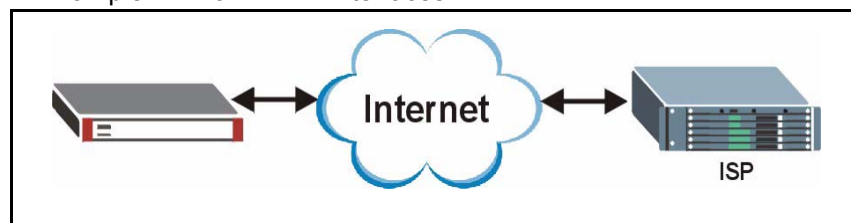
- 1 The first one runs on TCP port 1723. It is used to start and manage the second one.
- 2 The second one uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers.

PPTP is convenient and easy-to-use, but you have to make sure that firewalls support both PPTP sessions.

10.6.2 PPPoE/PPTP Interfaces Overview

In the ZyWALL, you may use PPPoE/PPTP interfaces to connect to your ISP. This way, you do not have to install or manage PPPoE/PPTP software on each computer in the network.

Figure 142 Example: PPPoE/PPTP Interfaces



PPPoE/PPTP interfaces are similar to other interfaces in some ways. They have an IP address, subnet mask, and gateway used to make routing decisions; they restrict bandwidth and packet size; and they can verify the gateway is available. There are two main differences between PPPoE/PPTP interfaces and other interfaces.

- 1 You must set up an ISP account before you create a PPPoE/PPTP interface.

Each ISP account specifies the protocol (PPPoE or PPTP), as well as your ISP account information. If you change ISPs later, you only have to create a new ISP account, not a new PPPoE/PPTP interface. You should not have to change any network policies.

2 You do not set up the subnet mask or gateway.

PPPoE/PPTP interfaces are interfaces between the ZyWALL and only one computer. Therefore, the subnet mask is always 255.255.255.255. In addition, the ZyWALL always treats the ISP as a gateway.

At the time of writing, it is possible to set up the IP address of the gateway (ISP) using CLI commands but not in the web configurator.

10.6.3 PPPoE/PPTP Interface Summary

Note: You have to set up an ISP account before you create a PPPoE/PPTP interface.

This screen lists every PPPoE/PPTP interface. To access this screen, click **Network > Interface > PPPoE/PPTP**.

Figure 143 Network > Interface > PPPoE/PPTP



Each field is described in the table below.

Table 58 Network > Interface > PPPoE/PPTP

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the interface.
Base Interface	This field displays the interface on the top of which the PPPoE/PPTP interface is.
Account Profile	This field displays the ISP account used by this PPPoE/PPTP interface.
Add icon	<p>This column lets you create, edit, remove, activate, deactivate, connect and disconnect interfaces.</p> <p>To create an interface, click the Add icon at the top of the column. The PPPoE/PPTP Interface Add/Edit screen appears.</p> <p>To edit an interface, click the Edit icon next to it. The PPPoE/PPTP Interface Add/Edit screen appears.</p> <p>To remove an interface, click the Remove icon next to it. The ZyWALL confirms you want to remove it before doing so.</p> <p>To activate or deactivate an interface, click the Active icon next to it.</p> <p>To connect or disconnect an interface, click the Connect icon next to it. You might use this icon to test the interface or to manually establish the connection for a Dial-on-Demand PPPoE/PPTP interface.</p>

10.6.4 PPPoE/PPTP Interface Add/Edit

Note: You have to set up an ISP account before you create a PPPoE/PPTP interface.

This screen lets you configure new or existing PPPoE/PPTP interfaces. To access this screen, click the **Add** icon or an **Edit** icon in the **PPPoE/PPTP Interface Summary** screen.

Figure 144 Network > Interface > PPPoE/PPTP > Edit

PPP Interface Properties

Enable

Interface Name

Nail_Up Dial-on-Demand

Description (Optional)

Base Interface

Account Profile

Protocol

User Name

Service Name

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address

Metric

Interface Parameters

Upstream Bandwidth Kbps

Downstream Bandwidth Kbps

MTU Bytes

Ping Check

Enable

Check Period (5-30 seconds)

Check Timeout (1-10 seconds)

Check Fail Tolerance (1-10)

Ping Default Gateway

Ping this address (Domain Name or IP Address)

Each field is explained in the following table.

Table 59 Network > Interface > PPPoE/PPTP > Edit

LABEL	DESCRIPTION
PPP Interface Properties	
Enable	Select this to enable this interface. Clear this to disable this interface.

Table 59 Network > Interface > PPPoE/PPTP > Edit (continued)

LABEL	DESCRIPTION
Interface Name	This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is pppx, where x is 0 - 11. For example, ppp0, ppp7, and so on.
Nail_Up	Select this if the PPPoE/PPTP connection should always be up.
Dial-on-Demand	Select this if you want the ZyWALL to establish the PPPoE/PPTP connection only when there is traffic. You might select this if there is little traffic through the interface or if it costs money to keep the connection available.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ % - characters, and it can be up to 60 characters long.
Base Interface	Select the interface on which the PPPoE/PPTP interface runs. This interface can be an Ethernet interface, VLAN interface, or bridge interface. PPPoE/PPTP interfaces cannot run on Ethernet interfaces or VLAN interfaces that are used in bridge interfaces, however.
Account Profile	Select the ISP account that this PPPoE/PPTP interface uses. The drop-down box lists ISP accounts by name.
Protocol	This field is read-only. It displays the protocol specified in the ISP account.
User Name	This field is read-only. It displays the user name for the ISP account.
Service Name	This field is read-only. It displays the PPPoE service name specified in the ISP account. This field is blank if the ISP account uses PPTP.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address automatically. The subnet mask and gateway are always defined automatically in PPPoE/PPTP interfaces.
Use Fixed IP Address	Select this if you want to specify the IP address manually.
IP Address	This field is enabled if you select Use Fixed IP Address . Enter the IP address for this interface.
Metric	Enter the priority of the gateway (the ISP) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Parameters	
Upstream Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Downstream Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Ping Check	The interface can regularly ping the gateway you specified to make sure it is still available. You specify how often the interface pings the gateway, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway acknowledges the ping.

Table 59 Network > Interface > PPPoE/PPTP > Edit (continued)

LABEL	DESCRIPTION
Enable	Select this to enable the ping check.
Check Period	Enter the number of seconds between ping attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the ZyWALL stops routing through the gateway.
Ping Default Gateway	Select this to ping the default gateway.
Ping this address	Select this to ping a specified domain name or IP address. Enter that domain name or IP address in the field next to it.

10.7 Auxiliary Interface

This section introduces the auxiliary interface and then explains the screen for it.

10.7.1 Auxiliary Interface Overview

Use the auxiliary interface to dial out from the **DIAL BACKUP** port in the ZyWALL. For example, you might use this interface as a backup WAN interface.

You have to connect an external modem to the ZyWALL's **DIAL BACKUP** port to use the auxiliary interface.

Note: You have to connect an external modem to the **DIAL BACKUP** port.

The ZyWALL uses the auxiliary interface to dial out in two situations.

- 1 You click the **Connect** icon on the ZyWALL **Status** screen.
- 2 The load auxiliary interface must connect to satisfy load-balancing requirements. You have to add the auxiliary interface to a trunk first.

When the ZyWALL hangs up the call, it drops the Data Terminal Ready (DTR) signal and issues the command `ATH`.

10.7.2 Auxiliary

Use the **Auxiliary** screen to configure the ZyWALL's **DIAL BACKUP** port. Click **Network > Interface > Auxiliary** to open it.

Figure 145 Network > Interface > Auxiliary

Each field is described in the table below.

Table 60 Network > Interface > Auxiliary

LABEL	DESCRIPTION
Auxiliary Interface Properties	
Enable	Select this to turn on the auxiliary dial up interface. The interface does not dial out, however, unless it is part of a trunk and load-balancing conditions are satisfied.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ - characters, and it can be up to 60 characters long.
Port Speed	Select the speed of the connection between the ZyWALL and external computer.
Dialing Type	Tone - select this if the telephone uses tone-based dialing. Pulse - select this if the telephone uses pulse-based dialing.
Initial String	Enter the AT command string to initialize the external modem. ATZ is the most common string, but you should check the manual for the external modem for additional commands.
Auxiliary Configuration	
Phone Number	Enter the phone number to dial here. You can use 1-20 numbers, commas (,), or plus signs (+). Use a comma to pause during dialing. Use a plus sign to tell the external modem to make an international call.
User Name	Enter the user name required for authentication.
Password	Enter the password required for authentication.
Retype to confirm	Enter the password again to make sure you have not typed it incorrectly.

Table 60 Network > Interface > Auxiliary (continued)

LABEL	DESCRIPTION
Authentication Type	Select the authentication protocol to use for outgoing calls. Choices are: CHAP/PAP - Your ZyWALL accepts either CHAP or PAP, as requested by the computer you are dialing. CHAP - Your ZyWALL accepts CHAP only. PAP - Your ZyWALL accepts PAP only. MSCHAP - Your ZyWALL accepts MSCHAP only. MSCHAP-V2 - Your ZyWALL accepts MSCHAP-V2 only.
Timeout	Type the number of seconds the ZyWALL tries to set up a connection before it stops. Allowed values are 30 - 120.
Idle timeout	Type the number of seconds the ZyWALL should wait for traffic before it automatically disconnects the connection. Set this field to zero to disable the idle timeout. Allowed values are 0 - 360.

10.8 Virtual Interfaces

Use virtual interfaces to tell the ZyWALL where to route packets. Virtual interfaces can also be used in VPN gateways (see [Chapter 12 on page 223](#)) and VRRP groups (see [Chapter 16 on page 275](#)).

Virtual interfaces can be created on top of Ethernet interfaces, VLAN interfaces, or bridge interfaces. Virtual VLAN interfaces recognize and use the same VLAN ID. Otherwise, there is no difference between each type of virtual interface. Network policies (for example, firewall rules) that apply to the underlying interface automatically apply to the virtual interface as well.

Like other interfaces, virtual interfaces have an IP address, subnet mask, and gateway used to make routing decisions. However, you have to manually specify the IP address and subnet mask; virtual interfaces cannot be DHCP clients. Like other interfaces, you can restrict bandwidth through virtual interfaces, but you cannot change the MTU. The virtual interface uses the same MTU that the underlying interface uses. Unlike other interfaces, virtual interfaces do not provide DHCP services, and they do not verify that the gateway is available.

10.8.1 Virtual Interfaces Add/Edit

This screen lets you configure IP address assignment and interface parameters for virtual interfaces. To access this screen, click an **Add** icon or **Edit** icon next to an Ethernet interface, VLAN interface, or bridge interface in the respective interface summary screen.

Figure 146 Network > Interface > Edit

Each field is described in the table below.

Table 61 Network > Interface > Edit

LABEL	DESCRIPTION
Virtual Interface Properties	
Interface Name	This field is read-only. It displays the name of the virtual interface, which is automatically derived from the underlying Ethernet interface, VLAN interface, or bridge interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
IP Address Assignment	
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first.
Interface Properties	
Upstream Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576.
Downstream Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576.

CHAPTER 11

Trunks

This chapter shows you how to configure trunks on your ZyWALL. [See the Trunks section](#) in the Configuration Overview chapter for related information on these screens.

11.1 Trunks Overview

You can group multiple interfaces together into trunks to have multiple connections share the traffic load to increase overall network throughput and enhance network reliability. If one interface's connection goes down, the ZyWALL sends traffic through another member of the trunk. For example, you can use two interfaces for WAN connections. You can connect one interface to one ISP (or network) and connect the another to a second ISP (or network). The ZyWALL can balance the load between multiple connections (see [Section 11.3 on page 215](#)). If one interface's connection goes down, the ZyWALL can automatically send its traffic through another interface.

You can use policy routing to specify through which interface to send specific traffic types. You can use trunks in combination with policy routing. You can also define multiple trunks for the same physical interfaces. This allows you to send specific traffic types through the interface that works best for that type of traffic, and if that interface's connection goes down, the ZyWALL can still send its traffic through another interface.

11.2 Trunk Scenario Examples

Suppose one of the ZyWALL's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You may want to set that interface as active and set another interface (connected to another ISP) to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface's connection is up.

Another example would be if you use multiple ISPs that provide different levels of service to different places. Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routing and trunks to send traffic for your European branch offices primarily through ISP A and traffic for your Australian branch offices primarily through ISP B.

11.3 Load Balancing Introduction

On the ZyWALL, load balancing is the process of dividing traffic loads between multiple interfaces. This allows you to improve quality of service and maximize bandwidth utilization.

Maybe you have two connections with different bandwidths. For jitter-sensitive traffic (like video for example), you could set up a trunk group that uses spillover or weighted round robin load balancing to make sure that most of the jitter-sensitive traffic goes through the higher-bandwidth interface.

For some traffic connections, you might want to use least load first load balancing in order to even out the distribution of the traffic load.

11.4 Load Balancing Algorithms

The following sections describe the load balancing algorithms that the ZyWALL can use to decide which interface the traffic (from the LAN) should use for a session¹. The available bandwidth you configure on the ZyWALL refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

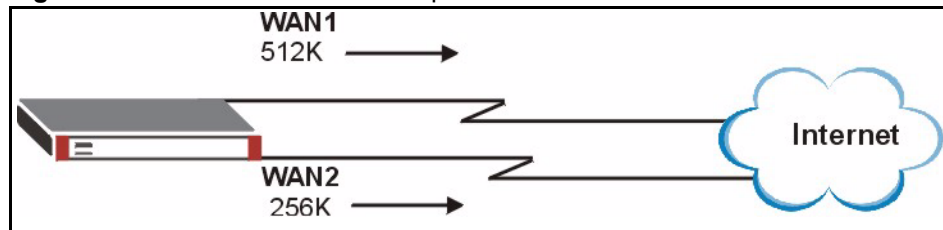
11.4.1 Least Load First

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

11.4.1.1 Least Load First Example 1

The following example shows two WAN interfaces on the ZyWALL connected to the Internet. The configured available outbound bandwidths for WAN 1 and WAN 2 are 512K and 256K respectively.

Figure 147 Least Load First Example 1



The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of WAN 1 is 412K and WAN 2 is 198K. The ZyWALL calculates the load balancing index as shown in the table below.

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

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

Table 62 Least Load First: Example 1

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

11.4.2 Weighted Round Robin

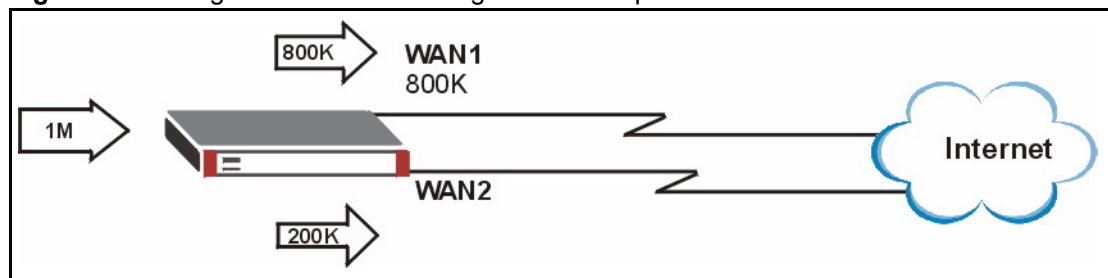
Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that interface. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

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

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

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

Figure 148 Weighted Round Robin Algorithm Example



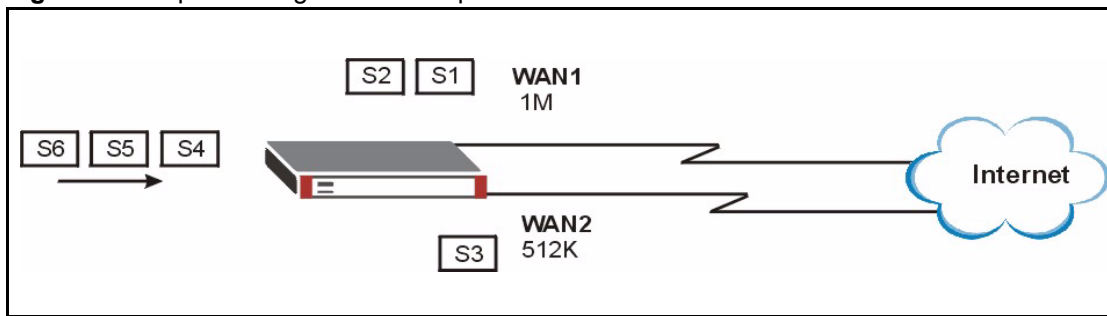
11.4.3 Spillover

With the spillover load balancing algorithm, the ZyWALL sends network traffic to the first interface in the trunk member list until the interface's maximum allowable load is reached, then the ZyWALL sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

In cases where the first interface in the trunk member list uses an unlimited access Internet connection and the secondary WAN uses a per-use timed access plan, the ZyWALL will only use the next interface in the trunk member list when the traffic load exceeds the threshold on the first interface. This allows you to fully utilize the bandwidth of the first interface to reduce Internet usage fees and avoid overloading the interface.

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

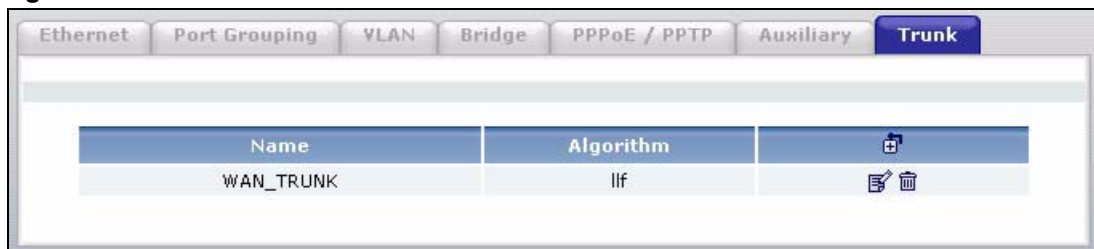
Figure 149 Spillover Algorithm Example



11.5 Trunk Summary

Click **Network > Interface > Trunk** to open the **Trunk** screen. This screen lists the configured trunks and the load balancing algorithm that each is configured to use.

Figure 150 Network > Interface > Trunk



The following table describes the items in this screen.

Table 63 Network > Interface > Trunk

LABEL	DESCRIPTION
Name	This field displays the label that you specified to identify the trunk.
Algorithm	This field displays the load balancing method that the trunk is set to use.
Add icon	<p>This column lets you create, edit and remove trunks.</p> <p>To create a trunk, click the Add icon at the top of the column. The Trunk Members screen appears.</p> <p>To edit a trunks, click the Edit icon next to it. The Trunk Members screen appears.</p> <p>To remove a trunk, click the Remove icon next to it. The ZyWALL confirms you want to remove it before doing so.</p>

11.6 Configuring a Trunk

Click **Network > Interface > Trunk** and then the add (or edit) icon to open the **Trunk Members** screen.

Figure 151 Network > Interface > Trunk > Members

Group Members

Name: WAN_TRUNK
Load Balancing Algorithm: Spillover

#	Member	Mode	Upstream Bandwidth	Spillover	
1	ge2	Active	1048576 Kbps	1 Kbps	[Add] [Edit] [Delete]
2	ge3	Active	1048576 Kbps	2 Kbps	[Add] [Edit] [Delete]

OK Cancel

Each field is described in the table below.

Table 64 Network > Interface > Trunk > Members


LABEL	DESCRIPTION
Name	Enter a descriptive name for this trunk. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Load Balancing Algorithm	<p>Select a load balancing method to use from the drop-down list box.</p> <p>Select Weighted Round Robin to balance the traffic load between interfaces based on their respective weights. Weighted round robin is activated only when the first group member interface has more traffic than it can handle.</p> <p>Select Least Load First to send new session traffic through the least utilized trunk member.</p> <p>Select Spillover to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).</p>
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	<p>Click this icon to open a screen where you can select an interface to be a group member.</p> <p>Figure 152 Network > Interface > Trunk > Members Select</p>  <p>If you select an interface that is part of another Ethernet interface, the ZyWALL does not send traffic through the interface as part of the trunk. For example, if you have physical port 5 in the ge2 representative interface, you must select interface ge2 in order to send traffic through port 5 as part of the trunk. If you select interface ge5 as a member here, the ZyWALL will not send traffic through port 5 as part of the trunk.</p>
Mode	<p>Select Active to have the ZyWALL always attempt to use this connection.</p> <p>Select Passive to have the ZyWALL only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.</p>
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the ZyWALL sends through each member interface. The higher an interface's weight is (relative to the weights of the interfaces), the more traffic the ZyWALL sends through that interface.
Downstream Bandwidth	This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the ZyWALL is to send out through the interface per second.
Upstream Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the ZyWALL is to allow to come in through the interface per second.

Table 64 Network > Interface > Trunk > Members (continued)

LABEL	DESCRIPTION
Spillover	<p>This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the ZyWALL sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The ZyWALL uses the group member interfaces in the order that they are listed.</p>
Add icon	<p>This column lets you add, remove and move trunk members.</p> <p>To add an interface to the trunk, click an Add icon. The Trunk Member Select screen appears.</p> <p>To remove an interface from a trunk, click the Remove icon next to it. The ZyWALL confirms you want to remove it before doing so.</p> <p>To move an interface to a different number in the list, click the Move icon next to it. In the field that appears, specify the number to which you want to move the interface.</p>

CHAPTER 12

IPSec VPN

This chapter explains how to set up and maintain IPSec VPNs in the ZyWALL. See the [IPSec VPN section](#) in the Configuration Overview chapter for related information on these screens.

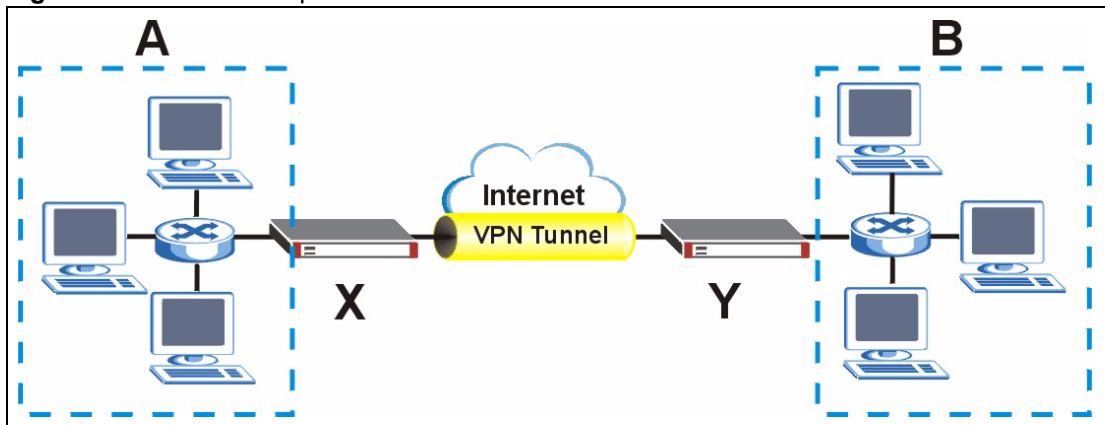
12.1 IPSec VPN Overview

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. It is 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.

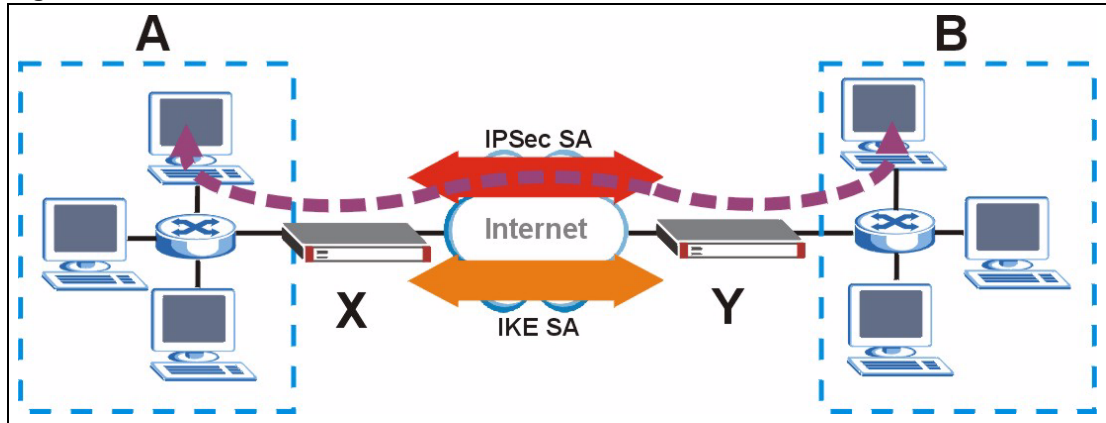
The following figure is one example of a VPN tunnel.

Figure 153 VPN: Example



The VPN tunnel 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 securely establish an IPSec SA through which the ZyWALL and remote IPsec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 154 VPN: IKE SA and IPsec SA

In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPsec SA. The IPsec SA is secure because routers **X** and **Y** established the IKE SA first.

The rest of this section discusses IKE SA and IPsec SA in more detail.

12.1.1 IPsec SA Overview

Once the ZyWALL and remote IPsec router have established the IKE SA, they can securely negotiate an IPsec SA through which to send data between computers on the networks.

Note: The IPsec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPsec SA.

12.1.1.1 Local Network and Remote Network

In IPsec SA, the local network, the one(s) connected to the ZyWALL, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPsec router, may be called the remote policy.

12.1.1.2 Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPsec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

Note: The ZyWALL and remote IPsec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

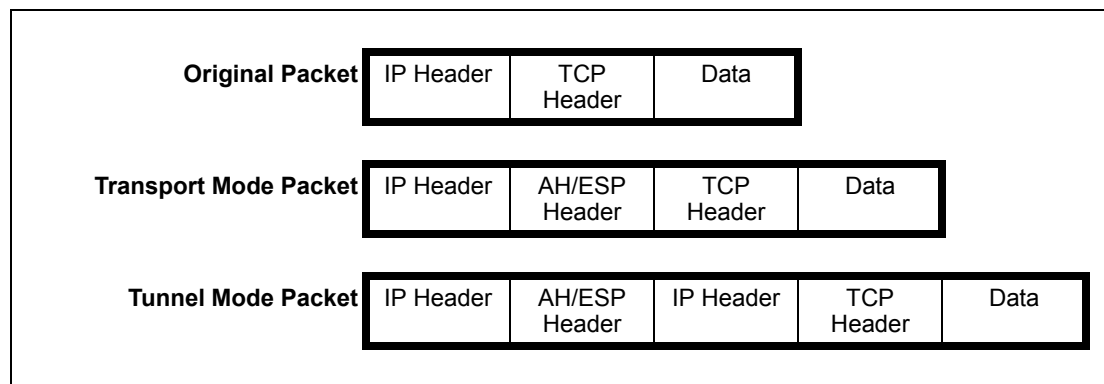
12.1.1.3 Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPsec SA is used for communication between the ZyWALL and remote IPsec router (for example, for remote management), not between computers on the local and remote networks.

Note: The ZyWALL and remote IPsec router must use the same encapsulation.

These modes are illustrated below.

Figure 155 VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the ZyWALL uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the ZyWALL or remote IPsec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the ZyWALL or remote IPsec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the ZyWALL includes part of the original IP header when it encapsulates the packet. With ESP, however, the ZyWALL does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

12.1.1.4 IPsec SA Proposal and Perfect Forward Secrecy

An IPsec SA proposal is similar to an IKE SA proposal (see [Section 12.4.1.2 on page 239](#)), except that you also have the choice whether or not the ZyWALL and remote IPsec router perform a new DH key exchange every time an IPsec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the ZyWALL and remote IPsec router perform a DH key exchange every time an IPsec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the ZyWALL and remote IPsec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

12.1.2 Additional Topics for IPsec SA

This section provides more information about IPsec SA in your ZyWALL.

12.1.2.1 IPsec SA using Manual Keys

You might set up an IPsec SA using manual keys when you want to establish a VPN tunnel quickly, for example, for troubleshooting. You should only do this as a temporary solution, however, because it is not as secure as a regular IPsec SA.

In IPsec SAs using manual keys, the ZyWALL and remote IPsec router do not establish an IKE SA. They only establish an IPsec SA. As a result, an IPsec SA using manual keys has some characteristics of IKE SA and some characteristics of IPsec SA. There are also some differences between IPsec SA using manual keys and other types of SA.

12.1.2.1.1 IPsec SA Proposal using Manual Keys

In IPsec SA using manual keys, you can only specify one encryption algorithm and one authentication algorithm. You cannot specify several proposals. There is no DH key exchange, so you have to provide the encryption key and the authentication key the ZyWALL and remote IPsec router use.

Note: The ZyWALL and remote IPsec router must use the same encryption key and authentication key.

12.1.2.1.2 Authentication and the Security Parameter Index (SPI)

For authentication, the ZyWALL and remote IPsec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

Note: The ZyWALL and remote IPsec router must use the same SPI.

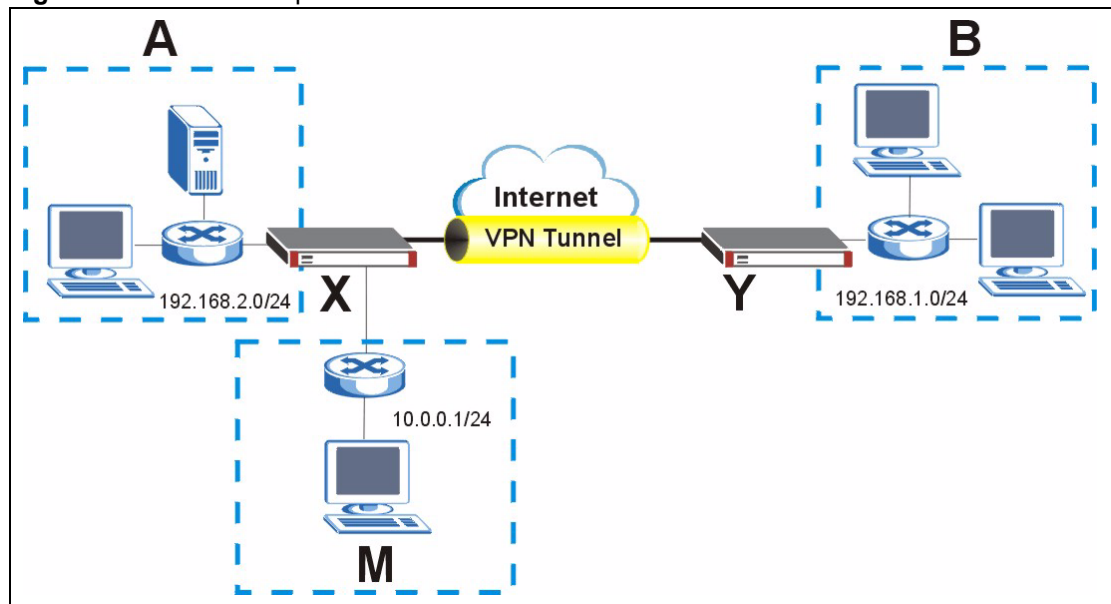
12.1.2.2 NAT for Inbound and Outbound Traffic

The ZyWALL can translate the following types of network addresses in IPsec SA.

- Source address in outbound packets - this translation is necessary if you want the ZyWALL to route packets from computers outside the local network through the IPsec SA.
- Source address in inbound packets - this translation hides the source address of computers in the remote network.
- Destination address in inbound packets - this translation is used if you want to forward packets (for example, mail) from the remote network to a specific computer (like the mail server) in the local network.

Each kind of translation is explained below. The following example is used to help explain each one.

Figure 156 VPN Example: NAT for Inbound and Outbound Traffic



12.1.2.2.1 Source Address in Outbound Packets (Outbound Traffic, Source NAT)

This translation lets the ZyWALL route packets from computers that are not part of the specified local network (local policy) through the IPsec SA. For example, in [Figure 156 on page 227](#), you have to configure this kind of translation if you want computer **M** to establish a connection with any computer in the remote network (**B**). If you do not configure it, the remote IPsec router may not route messages for computer **M** through the IPsec SA because computer **M**'s IP address is not part of its local policy.

To set up this NAT, you have to specify the following information:

- Source - the original source address; most likely, computer **M**'s network.
- Destination - the original destination address; the remote network (**B**).
- SNAT - the translated source address; the local network (**A**).

12.1.2.2.2 Source Address in Inbound Packets (Inbound Traffic, Source NAT)

You can set up this translation if you want to change the source address of computers in the remote network. To set up this NAT, you have to specify the following information:

- Source - the original source address; the remote network (**B**).
- Destination - the original destination address; the local network (**A**).
- SNAT - the translated source address; a different IP address (range of addresses) to hide the original source address.

12.1.2.2.3 Destination Address in Inbound Packets (Inbound Traffic, Destination NAT)

You can set up this translation if you want the ZyWALL to forward some packets from the remote network to a specific computer in the local network. For example, in [Figure 156 on page 227](#), you can configure this kind of translation if you want to forward mail from the remote network to the mail server in the local network (**A**).

You have to specify one or more rules when you set up this kind of NAT. The ZyWALL checks these rules similar to the way it checks rules for a firewall. The first part of these rules define the conditions in which the rule apply.

- Original IP - the original destination address; the remote network (**B**).
- Protocol - the protocol [TCP, UDP, or both] used by the service requesting the connection.
- Original Port - the original destination port or range of destination ports; in [Figure 156 on page 227](#), it might be port 25 for SMTP.

The second part of these rules controls the translation when the condition is satisfied.

- Mapped IP - the translated destination address; in [Figure 156 on page 227](#), the IP address of the mail server in the local network (**A**).
- Mapped Port - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

12.2 Related Configuration

This section briefly explains the relationship between VPN tunnels and other features. It also provides some basic suggestions for troubleshooting.

You should set up the following features before you set up the VPN tunnel.

- In any VPN connection, you have to select address objects to specify the local policy and remote policy. You should set up the address objects first.

- In a VPN gateway, you can select an Ethernet interface, virtual Ethernet interface, VLAN interface, or virtual VLAN interface to specify what address the ZyWALL uses IP address when it establishes the IKE SA. You should set up the interface first. See [Chapter 10 on page 177](#).
- In a VPN gateway, you can enable extended authentication. If the ZyWALL runs in server mode, you should set up the authentication method (AAA server) first. The authentication method specifies how the ZyWALL authenticates the remote IPSec router. See [Chapter 32 on page 465](#).
- In a VPN gateway, the ZyWALL and remote IPSec router can use certificates to authenticate each other. You should import the certificate first. See [Chapter 33 on page 469](#).

You should set up the following features before the network can use the VPN tunnel.

- The ZyWALL does not put IPSec SA in the routing table. You must create a policy route for the VPN tunnel. See [Chapter 18 on page 291](#).
- Make sure the to-ZyWALL firewall rules allow IPSec VPN traffic to the ZyWALL. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- The ZyWALL supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the to-ZyWALL firewall rules allow UDP port 4500 too.
- Make sure regular firewall rules allow traffic between the VPN tunnel and the rest of the network. Regular firewall rules check packets the ZyWALL sends before the ZyWALL encrypts them and check packets the ZyWALL receives after the ZyWALL decrypts them. This depends on the zone to which you assign the VPN tunnel and the zone from which and to which traffic may be routed.
- If you set up a VPN tunnel across the Internet, make sure your ISP supports AH or ESP.

If there are problems setting up a VPN tunnel, make sure both the ZyWALL and remote IPSec router have the same settings for the VPN tunnel. It is also helpful to have a way to look at the packets that are being sent and received by the ZyWALL and remote IPSec router (for example, packet sniffers).

12.3 VPN Connection Screens

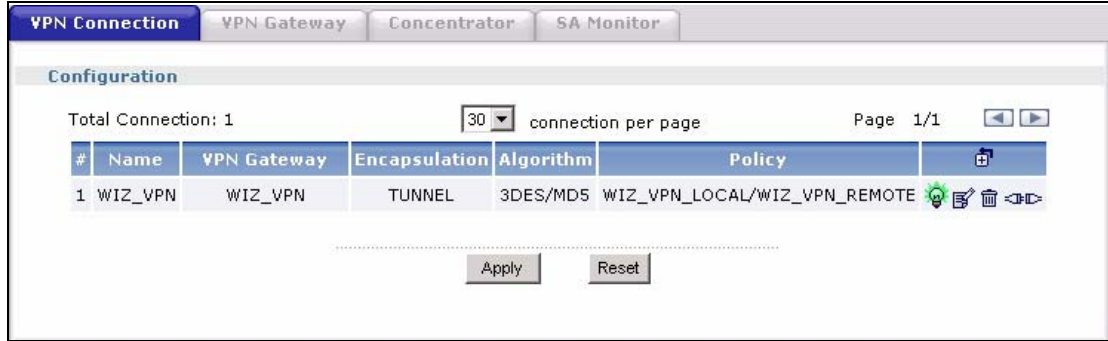
You use the **VPN Connection** summary screen to look at the VPN connections you have set up, and you use the **VPN Connection Add/Edit Manual Key** and **VPN Connection Add/Edit Gateway** screens to create or to edit VPN connections.

12.3.1 VPN Connection Summary

The **VPN Connection** summary screen displays the list of VPN connections, the associated VPN gateway(s), and various settings. In addition, it also lets you activate / deactivate and connect / disconnect each VPN connection (each IPSec SA).

To access this screen, click **Configuration > Network > IPSec VPN**. The following screen appears.

Figure 157 Network > IPsec VPN > VPN Connection



Each field is discussed in the following table. See [Section 12.3.3 on page 234](#) and [Section 12.3.2 on page 230](#) for more information.

Table 65 Network > IPsec VPN > VPN Connection

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific connection.
Name	This field displays the name of the IPsec SA.
VPN Gateway	This field displays the associated VPN gateway(s). If there is no VPN gateway, this field displays “manual key”.
Encapsulation	This field displays what encapsulation the IPsec SA uses.
Algorithm	This field displays what encryption and authentication methods, respectively, the IPsec SA uses.
Policy	This field displays the local policy and the remote policy, respectively.
Add icon	<p>This column provides icons to add, edit, and remove VPN connections, as well as to activate / deactivate and connect / disconnect VPN connections.</p> <p>To add a VPN connection, click the Add icon at the top of the column. The VPN Connection Add/Edit Manual screen appears.</p> <p>To edit a VPN connection, click the Edit icon next to the connection. The VPN Connection Add/Edit Manual or VPN Connection Add/Edit Gateway screen appears accordingly.</p> <p>To delete a VPN connection, click the Remove icon next to the connection. The web configurator confirms that you want to delete the VPN connection.</p> <p>To activate or deactivate an IPsec SA, click the Active icon next to the VPN connection.</p> <p>To connect or disconnect an IPsec SA, click the Connect icon next to the VPN connection.</p>

12.3.2 VPN Connection Add/Edit IKE

The **VPN Connection Add/Edit Gateway** screen allows you to create a new VPN connection using a VPN gateway (with IKE) or edit an existing VPN connection using a VPN gateway. To access this screen, go to the **VPN Connection Summary** screen (see [Section 12.3.1 on page 229](#)), and click either the **Add** icon or an **Edit** icon. If you click the **Add** icon, you have to select a specific VPN gateway in the **VPN Gateway** field before the following screen appears.

Figure 158 Network > IPSec VPN > VPN Connection > Edit (IKE)

Each field is described in the following table.

Table 66 Network > IPSec VPN > VPN Connection > Edit

LABEL	DESCRIPTION
VPN Connection	
Connection Name	Type the name used to identify this IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
VPN Gateway	
Name	Select the VPN gateway that you want to use with this VPN connection.
Add New VPN Gateway	Click this button to add another VPN gateway this VPN connection can use.
Phase 2	

Table 66 Network > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Active Protocol	<p>Select which protocol you want to use in the IPSec SA. Choices are:</p> <p>AH (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select AH, you must select an authentication algorithm.</p> <p>ESP (RFC 2406) - provides encryption and the same services offered by AH, but its authentication is weaker. If you select ESP, you must select an encryption algorithm and authentication algorithm.</p> <p>Both AH and ESP increase processing requirements and latency (delay).</p>
Encapsulation	<p>Select which type of encapsulation the IPSec SA uses. Choices are</p> <p>Tunnel - this mode encrypts the IP header information and the data</p> <p>Transport - this mode only encrypts the data</p>
Proposal	
#	<p>This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.</p>
Encryption	<p>This field is applicable when the active protocol is ESP. Select which key size and encryption algorithm to use in the IPSec SA. Choices are:</p> <p>NULL - no encryption key or algorithm</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>AES128 - a 128-bit key with the AES encryption algorithm</p> <p>AES192 - a 192-bit key with the AES encryption algorithm</p> <p>AES256 - a 256-bit key with the AES encryption algorithm</p> <p>The ZyWALL and the remote IPSec router must use the same key. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p>
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are SHA1 and MD5. SHA1 is generally considered stronger than MD5, but it is also slower.</p>
Add icon	<p>This column contains icons to add and remove proposals.</p> <p>To add a proposal, click the Add icon at the top of the column.</p> <p>To remove a proposal, click the Remove icon next to the proposal. The ZyWALL confirms that you want to delete it before doing so.</p>
SA Life Time (Seconds)	<p>Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The ZyWALL automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.</p>
Perfect Forward Secrecy (PFS)	<p>Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are:</p> <p>none - disable PFS</p> <p>DH1 - enable PFS and use a 768-bit random number</p> <p>DH2 - enable PFS and use a 1024-bit random number</p> <p>DH5 - enable PFS and use a 1536-bit random number</p> <p>PFS changes the root key that is used to generate encryption keys for each IPSec SA. It is more secure but takes more time.</p>
Policy	

Table 66 Network > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Policy Enforcement	<p>Select this if you want the ZyWALL to drop traffic whose source and destination IP addresses do not match the local and remote policy. This makes the IPSec SA more secure.</p> <p>Note: You must clear this field, however, if you want to use the IPSec SA in a VPN concentrator.</p>
Local Policy	Select the address corresponding to the local network.
Remote Policy	Select the address corresponding to the remote network.
Property	
Nailed-Up	Select this if you want the ZyWALL to automatically renegotiate the IPSec SA when the SA life time expires.
Enable Replay Detection	Select this check box to detect and reject old or duplicate packets to protect against Denial-of-Service attacks.
Enable NetBIOS Broadcast over IPSec	<p>Select this check box if you the ZyWALL to send NetBIOS (Network Basic Input/Output System) packets through the IPSec SA.</p> <p>NetBIOS packets 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 IPSec SAs in order to allow local computers to find computers on the remote network and vice versa.</p>
Inbound/Outbound Traffic NAT	Click the Advanced button to show and hide this section.
Outbound Traffic	
Source NAT	This translation hides the source address of computers in the local network. It may also be necessary if you want the ZyWALL to route packets from computers outside the local network through the IPSec SA.
Source	Select the address object that represents the original source address. This is the address object for the computer or network outside the local network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination	Select the address object that represents the original destination address. This is the address object for the remote network.
SNAT	Select the address object that represents the translated source address. This is the address object for the local network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Inbound Traffic	
Source NAT	This translation hides the source address of computers in the remote network.
Source	Select the address object that represents the original source address. This is the address object for the remote network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination	Select the address object that represents the original destination address. This is the address object for the local network.
SNAT	Select the address object that represents the translated source address. This is the address that hides the original source address. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).

Table 66 Network > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Destination NAT	This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network.
#	This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed.
Original IP	Select the address object that represents the original destination address. This is the address object for the remote network.
Mapped IP	Select the address object that represents the desired destination address. For example, this is the address object for the mail server.
Protocol	Select the protocol required to use this translation. Choices are: TCP , UDP , or All .
Original Port	These fields are available if the protocol is TCP or UDP . Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Mapped Port	These fields are available if the protocol is TCP or UDP . Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Add icon	<p>This column contains icons to add, move, and remove NAT records.</p> <p>To add a NAT record, click the Add icon at the top of the column.</p> <p>To move a NAT record, click the Move to N icon next to the record, and then type the row number to which you want to move it. The records are renumbered automatically.</p> <p>To remove a NAT record, click the Remove icon next to the record. The ZyWALL confirms that you want to delete the NAT record before doing so.</p>
OK	Click OK to save the changes.
Cancel	Click Cancel to discard all changes and return to the main VPN screen.

12.3.3 VPN Connection Add/Edit Manual Key

The **VPN Connection Add/Edit Manual Key** screen allows you to create a new VPN connection or edit an existing one using a manual key. This is useful if you have problems with IKE key management. To access this screen, go to the **VPN Connection Summary** screen (see [Section 12.3.1 on page 229](#)), and click either the **Add** icon or an **Edit** icon.

Figure 159 Network > IPSec VPN > VPN Connection > Manual Key > Edit

The following table describes the labels in this screen.

Table 67 Network > IPSec VPN > VPN Connection > Manual Key > Edit

LABEL	DESCRIPTION
VPN Connection	
Connection Name	Type the name used to identify this IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
VPN Gateway	
Name	Select manual key in the drop-down list.
Manual Key	
SPI	Type a unique SPI (Security Parameter Index) between 256 and 4095. The SPI is used to identify the ZyWALL during authentication.

Table 67 Network > IPSec VPN > VPN Connection > Manual Key > Edit (continued)

LABEL	DESCRIPTION
Encapsulation Mode	<p>Select which type of encapsulation the IPSec SA uses. Choices are</p> <p>Tunnel - this mode encrypts the IP header information and the data</p> <p>Transport - this mode only encrypts the data. You should only select this if the IPSec SA is used for communication between the ZyWALL and remote IPSec router.</p> <p>If you select Transport mode, the ZyWALL automatically switches to Tunnel mode if the IPSec SA is not used for communication between the ZyWALL and remote IPSec router. In this case, the ZyWALL generates a log message for this change.</p>
Active Protocol	<p>Select which protocol you want to use in the IPSec SA. Choices are:</p> <p>AH (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select AH, you must select an Authentication Algorithm.</p> <p>ESP (RFC 2406) - provides encryption and the same services offered by AH, but its authentication is weaker. If you select ESP, you must select an Encryption Algorithm and Authentication Algorithm.</p>
Encryption Algorithm	<p>This field is applicable when the Active Protocol is ESP. Select which key size and encryption algorithm to use in the IPSec SA. Choices are:</p> <p>NULL - no encryption key or algorithm</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>AES128 - a 128-bit key with the AES encryption algorithm</p> <p>AES192 - a 192-bit key with the AES encryption algorithm</p> <p>AES256 - a 256-bit key with the AES encryption algorithm</p> <p>The ZyWALL and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p>
Authentication Algorithm	<p>Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are SHA1 and MD5. SHA1 is generally considered stronger than MD5, but it is also slower.</p>
Encryption Key	<p>This field is applicable when you select an Encryption Algorithm. Enter the encryption key, which depends on the encryption algorithm.</p> <p>DES - type a unique key 8-32 characters long</p> <p>3DES - type a unique key 24-32 characters long</p> <p>AES128 - type a unique key 16-32 characters long</p> <p>AES192 - type a unique key 24-32 characters long</p> <p>AES256 - type a unique key 32 characters long</p> <p>You can use any alphanumeric characters or ; '~!@#%&*()_+{}',./<>=-. If you want to enter the key in hexadecimal, type "0x" at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in "0123456789ABCDEF" is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above.</p> <p>The remote IPSec router must have the same encryption key.</p> <p>The ZyWALL ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 1234567890XYZ for a DES encryption key, the ZyWALL only uses 12345678. The ZyWALL still stores the longer key.</p>

Table 67 Network > IPSec VPN > VPN Connection > Manual Key > Edit (continued)

LABEL	DESCRIPTION
Authentication Key	<p>Enter the authentication key, which depends on the authentication algorithm.</p> <p>MD5 - type a unique key 16-20 characters long</p> <p>SHA1 - type a unique key 20 characters long</p> <p>You can use any alphanumeric characters or ; `~!@#\$%^&*()_+{}'"/.<>=,. If you want to enter the key in hexadecimal, type "0x" at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in "0123456789ABCDEF" is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above.</p> <p>The remote IPSec router must have the same authentication key.</p> <p>The ZyWALL ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 12345678901234567890 for a MD5 authentication key, the ZyWALL only uses 1234567890123456. The ZyWALL still stores the longer key.</p>
Policy	You can set up overlapping local policies or overlapping remote policies in the ZyWALL.
Local Policy	Select the address object for the local network. You must configure this before you create the IPSec SA.
Remote Policy	Select the address object for the remote network. You must configure this before you create the IPSec SA.
Property	
My Address	Type the IP address of the ZyWALL in the IPSec SA. 0.0.0.0 is invalid.
Secure Gateway Address	Type the IP address of the remote IPSec router in the IPSec SA.
Enable NetBIOS broadcast over IPSec	<p>Select this check box if you want the ZyWALL to send NetBIOS (Network Basic Input/Output System) packets through the IPSec SA.</p> <p>NetBIOS packets 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 IPSec SAs in order to allow local computers to find computers on the remote network and vice versa.</p>
Inbound/Outbound Traffic NAT	Click the Advanced button to show and hide this section.
Outbound Traffic	
Source NAT	This translation hides the source address of computers in the local network. It may also be necessary if you want the ZyWALL to route packets from computers outside the local network through the IPSec SA.
Source	Select the address object that represents the original source address. This is the address object for the computer or network outside the local network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination	Select the address object that represents the original destination address. This is the address object for the remote network.
SNAT	Select the address object that represents the translated source address. This is the address object for the local network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Inbound Traffic	
Source NAT	This translation hides the source address of computers in the remote network.

Table 67 Network > IPSec VPN > VPN Connection > Manual Key > Edit (continued)

LABEL	DESCRIPTION
Source	Select the address object that represents the original source address. This is the address object for the remote network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination	Select the address object that represents the original destination address. This is the address object for the local network.
SNAT	Select the address object that represents the translated source address. This is the address that hides the original source address. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination NAT	This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network.
#	This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed.
Original IP	Select the address object that represents the original destination address. This is the address object for the remote network.
Mapped IP	Select the address object that represents the desired destination address. For example, this is the address object for the mail server.
Protocol	Select the protocol required to use this translation. Choices are: TCP , UDP , or All .
Original Port	This field is available if the protocol is TCP or UDP . Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Mapped Port	This field is available if the protocol is TCP or UDP . Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Add icon	This column contains icons to add, move, and remove NAT records. To add a NAT record, click the Add icon at the top of the column. To move a NAT record, click the Move to N icon next to the record, and then type the row number to which you want to move it. The records are renumbered automatically. To remove a NAT record, click the Remove icon next to the record. The ZyWALL confirms that you want to delete the NAT record before doing so.
OK	Click OK to save your changes back to the ZyWALL.
Cancel	Click Cancel to exit this screen without saving.

12.4 VPN Gateway Screens

You use the **VPN Gateway** summary screen to look at the VPN gateways you have set up, and you use the **VPN Gateway Add/Edit** screen to create or to edit VPN gateways.

12.4.1 IKE SA Overview

The IKE SA provides a secure connection between the ZyWALL and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines how many. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Note: Both routers must use the same negotiation mode.

These modes are discussed in more detail in [Section 12.4.2.1 on page 242](#). Main mode is used in various examples in the rest of this section.

12.4.1.1 IP Addresses of the ZyWALL and Remote IPSec router

To set up an IKE SA, you have to specify the IP addresses of the ZyWALL and remote IPSec router. You can usually enter a static IP address or a domain name for either or both IP addresses. Sometimes, your ZyWALL might offer another alternative, such as using the IP address of a port or interface, as well.

You can also specify the IP address of the remote IPSec router as 0.0.0.0. This means that the remote IPSec router can have any IP address. In this case, only the remote IPSec router can initiate an IKE SA because the ZyWALL does not know the IP address of the remote IPSec router. This is often used for telecommuters.

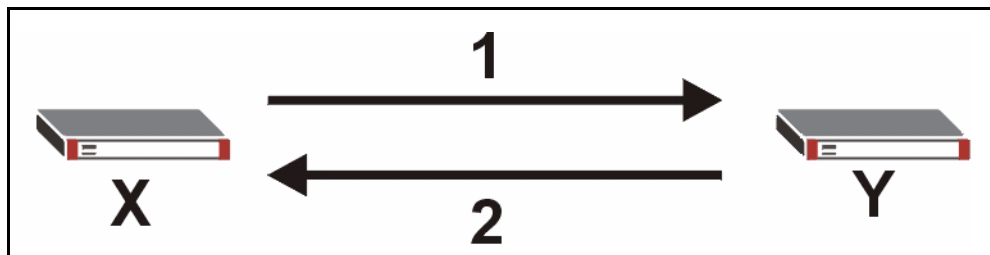
12.4.1.2 IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the ZyWALL and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated next.

Figure 160 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal

One or more proposals, each one consisting of:

- encryption algorithm
- authentication algorithm
- Diffie-Hellman key group



The ZyWALL sends one or more proposals to the remote IPSec router. (In some devices, you can only set up one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the ZyWALL wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the ZyWALL. If the remote IPSec router rejects all of the proposals, the ZyWALL and remote IPSec router cannot establish an IKE SA.

Note: Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

In most ZyWALLs, you can select one of the following encryption algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Some ZyWALLs also offer stronger forms of AES that apply 192-bit or 256-bit keys to 128-bit blocks of data.

In most ZyWALLs, you can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

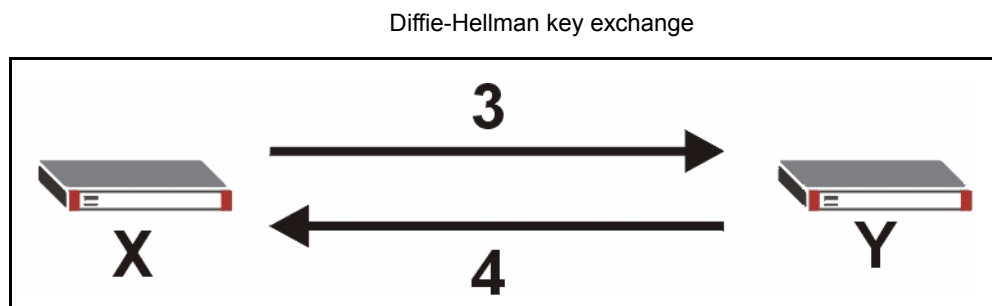
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

See [Section 12.4.1.3 on page 240](#) for more information about DH key groups.

12.4.1.3 Diffie-Hellman (DH) Key Exchange

The ZyWALL and the remote IPSec router use DH public-key cryptography to establish a shared secret. The shared secret is then used to generate encryption keys for the IKE SA and IPSec SA. In main mode, this is done in steps 3 and 4, as illustrated next.

Figure 161 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



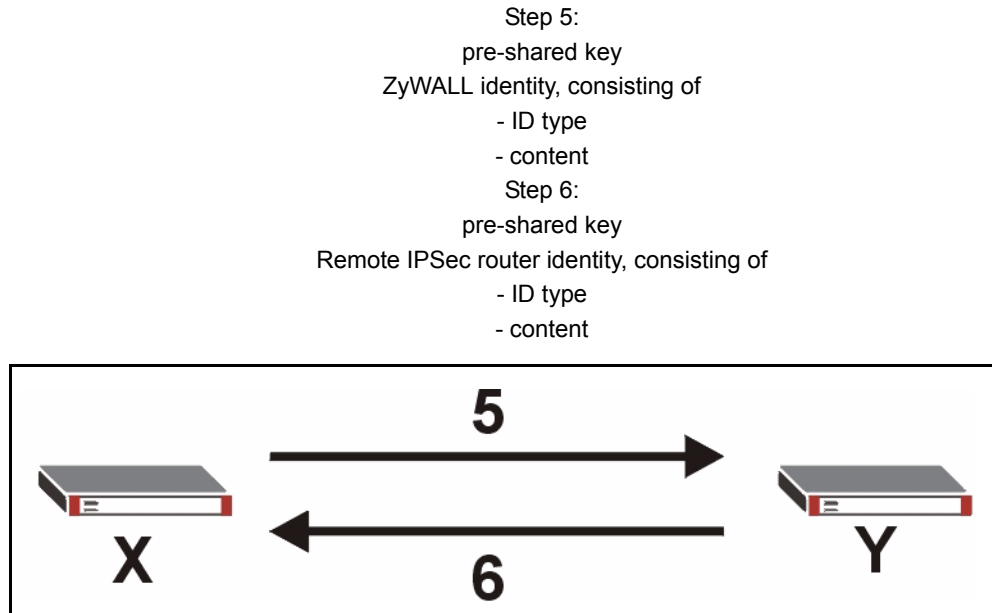
DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

12.4.1.4 Authentication

Before the ZyWALL and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the ZyWALL and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. The identities are also encrypted using the encryption algorithm and encryption key the ZyWALL and remote IPSec router selected in previous steps.

Figure 162 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication (continued)



You have to create (and distribute) a pre-shared key. The ZyWALL and remote IPSec router use it in the authentication process, though it is not actually transmitted or exchanged.

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

Router identity consists of 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 domain name or e-mail address that you enter does not have to actually exist. Similarly, any domain name or IP address that you enter does not have to correspond to the ZyWALL's or remote IPSec router's properties.

The ZyWALL and the remote IPSec router have their own identities, 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.

Note: The ZyWALL's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.

For example, in [Table 68 on page 242](#), the ZyWALL and the remote IPsec router authenticate each other successfully. In contrast, in [Table 69 on page 242](#), the ZyWALL and the remote IPsec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

Table 68 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 69 VPN Example: Mismatching 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: 1.1.1.20	Peer ID content: tom@yourcompany.com

It is also possible to configure the ZyWALL to ignore the identity of the remote IPsec router. In this case, you usually set the peer ID type to **Any**. This is less secure, so you should only use this if your ZyWALL provides another way to check the identity of the remote IPsec router (for example, extended authentication) or if you are troubleshooting a VPN tunnel.

12.4.2 Additional Topics for IKE SA

This section provides more information about IKE SA.

12.4.2.1 Negotiation Mode

There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1 - 2: The ZyWALL sends its proposals to the remote IPsec router. The remote IPsec router selects an acceptable proposal and sends it back to the ZyWALL.

Steps 3 - 4: The ZyWALL and the remote IPsec router exchange pre-shared keys for authentication and participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

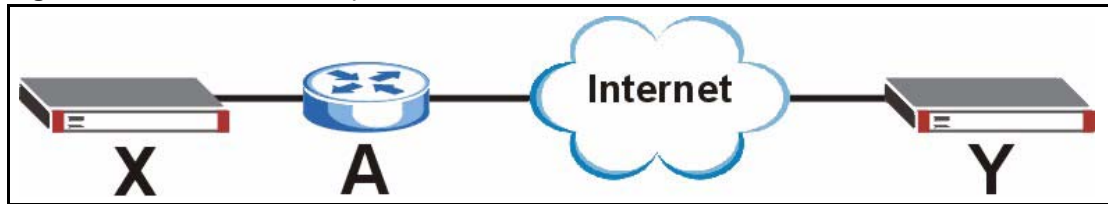
Steps 5 - 6: Finally, the ZyWALL and the remote IPsec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA. Aggressive mode does not provide as much security because the identity of the ZyWALL and the identity of the remote IPSec router are not encrypted. It is usually used 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.

12.4.2.2 VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

Figure 163 VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-thru feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See [Section 12.1.1.2 on page 224](#) for more information about active protocols.)

If router **A** does not have an IPSec pass-thru or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the ZyWALL and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the ZyWALL and remote IPSec router support.

12.4.2.3 Extended Authentication

Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters.

In extended authentication, one of the routers (the ZyWALL or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the ZyWALL to provide a user name and password to the remote IPSec router, or you can set up the ZyWALL to check a user name and password that is provided by the remote IPSec router.

If you use extended authentication, it takes four more steps to establish an IKE SA. These steps occur at the end, regardless of the negotiation mode (steps 7-10 in main mode, steps 4-7 in aggressive mode).

12.4.2.4 Certificates

It is possible for the ZyWALL and remote IPSec router to authenticate each other with certificates. In this case, you do not have to set up the pre-shared key, local identity, or remote identity because the certificates provide this information instead.

- Instead of using the pre-shared key, the ZyWALL and remote IPSec router check the signatures on each other's certificates. Unlike pre-shared keys, the signatures do not have to match.
- The local and peer ID type and content come from the certificates.

Note: You must set up the certificates for the ZyWALL and remote IPSec router first.

12.4.3 VPN Gateway Summary

The **VPN Gateway** summary screen displays the VPN gateways in the ZyWALL, as well as the ZyWALL's address, remote IPSec router's address, and associated VPN connections for each one. In addition, it also lets you activate and deactivate each VPN gateway.

To access this screen, click **Configuration > Network > IPSec VPN > VPN Gateway**. The following screen appears.

Figure 164 Network > IPSec VPN > VPN Gateway

Each field is discussed in the following table. See [Section 12.4.4 on page 245](#) for more information.

Table 70 Network > IPSec VPN > VPN Gateway

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific gateway.
Name	This field displays the name of the VPN gateway.
My address	This field displays the address of the VPN gateway. The address can be an interface or a domain name.
Secure Gateway	This field displays the IP address(es) of the remote IPSec routers.
VPN Connection	This field displays VPN connections that use this VPN gateway.
Add icon	<p>This column provides icons to add, edit, and remove VPN gateways, as well as to activate / deactivate VPN gateways.</p> <p>To add a VPN gateway, click the Add icon at the top of the column. The VPN Gateway Add/Edit screen appears.</p> <p>To edit a VPN gateway, click the Edit icon next to the gateway. The VPN Gateway Add/Edit screen appears accordingly.</p> <p>To delete a VPN gateway, click on the Remove icon next to the gateway. The web configurator confirms that you want to delete the VPN gateway.</p> <p>To activate or deactivate a VPN gateway, click the Active icon next to the gateway.</p>

12.4.4 VPN Gateway Add/Edit

The **VPN Gateway Add/Edit** screen allows you to create a new VPN gateway or edit an existing one. To access this screen, go to the **VPN Gateway Summary** screen (see [Section 12.4.3 on page 244](#)), and click either the **Add** icon or an **Edit** icon.

Figure 165 Network > IPSec VPN > VPN Gateway > Edit

VPN Gateway

VPN Gateway Name:

IKE Phase 1

Negotiation Mode:

Proposal:

#	Encryption	Authentication	
1	<input type="text" value="3DES"/>	<input type="text" value="MD5"/>	

Key Group:

SA Life Time (Seconds): <60..86400>

NAT Traversal

Dead Peer Detection (DPD)

Property

My Address:

Interface: Static -- 192.168.1.1/255.255.255.0

Domain Name:

Secure Gateway Address:

1.

2.

Authentication Method

Pre-Shared Key:

Certificate: (See [My Certificates](#))

Local ID Type:

Content:

Peer ID Type:

Content:

Extended Authentication

Enable Extended Authentication

Server Mode:

Client Mode

User Name:

Password:

.....

Each field is described in the following table.

Table 71 Network > IPSec VPN > VPN Gateway > Edit

LABEL	DESCRIPTION
VPN Gateway	
VPN Gateway Name	Type the name used to identify this VPN gateway. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IKE Phase 1	

Table 71 Network > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Negotiation Mode	<p>Select which negotiation mode you want to use to negotiate the IKE SA. Choices are</p> <p>Main - this encrypts the ZyWALL's and remote IPSec router's identities but takes more time to establish the IKE SA</p> <p>Aggressive - this is faster but does not encrypt the identities</p> <p>The ZyWALL and the remote IPSec router must use the same negotiation mode.</p>
Proposal	
#	<p>This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.</p>
Encryption	<p>Select which key size and encryption algorithm to use in the IKE SA. Choices are:</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>AES128 - a 128-bit key with the AES encryption algorithm</p> <p>AES192 - a 192-bit key with the AES encryption algorithm</p> <p>AES256 - a 256-bit key with the AES encryption algorithm</p> <p>The ZyWALL and the remote IPSec router must use the same key. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p>
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are SHA1 and MD5. SHA1 is generally considered stronger than MD5, but it is also slower.</p>
Add icon	<p>This column contains icons to add and remove protocols.</p> <p>To add a protocol, click the Add icon at the top of the column.</p> <p>To remove a protocol, click the Remove icon next to the protocol. The ZyWALL confirms that you want to delete the protocol before doing so.</p>
Key Group	<p>Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are:</p> <p>DH1 - use a 768-bit random number</p> <p>DH2 - use a 1024-bit random number</p> <p>DH5 - use a 1536-bit random number</p>
SA Life Time (Seconds)	<p>Type the maximum number of seconds the IKE SA can last. When this time has passed, the ZyWALL and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.</p>
NAT Traversal	<p>Select this if any of these conditions are satisfied.</p> <ul style="list-style-type: none"> • This IKE SA might be used to negotiate IPSec SA that use active protocol AH. • There are one or more NAT routers between the ZyWALL and remote IPSec router, and these routers do not support IPSec pass-thru or a similar feature. <p>The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged.</p>
Dead Peer Detection (DPD)	<p>Select this check box if you want the ZyWALL to make sure the remote IPSec router is there before it transmits data through the IKE SA. If there has been no traffic for at least 15 seconds, the ZyWALL sends a message to the remote IPSec server. If the remote IPSec server responds, the ZyWALL transmits the data. If the remote IPSec server does not respond, the ZyWALL shuts down the IKE SA.</p>
Property	

Table 71 Network > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
My Address	<p>Select how the IP address of the ZyWALL in the IKE SA is defined. Choices are Interface and Domain Name.</p> <p>If you select Interface, you must select an Ethernet interface, VLAN interface, virtual Ethernet interface, virtual VLAN interface, PPPoE/PPTP interface, or auxiliary interface. The IP address of the ZyWALL in the IKE SA is the IP address of the interface.</p> <p>If you select Domain Name, you must provide the domain name or the IP address of the ZyWALL. The IP address of the ZyWALL in the IKE SA is the specified IP address or the IP address corresponding to the domain name. 0.0.0.0 is invalid. If you change this value, the ZyWALL has to re-build the IKE SA.</p>
Secure Gateway Address	<p>Type the IP address or the domain name of the remote IPSec router. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic IP address. You can provide a second IP address or domain name. In this case, if the ZyWALL cannot establish an IKE SA with the first one, it tries to establish an IKE SA with the second one.</p>
Authentication Method	<p>Note: The ZyWALL and remote IPSec router must use the same authentication method to establish the IKE SA.</p>
Pre-Shared Key	<p>Select this if the ZyWALL and remote IPSec router do not use certificates to identify each other when they negotiate the IKE SA. Then, type the pre-shared key in the field to the right. The pre-shared key can be</p> <ul style="list-style-type: none"> • 8 - 32 alphanumeric characters or ; '~!@#%&*()_+{}:./<>=-. • 16 - 64 hexadecimal (0-9, A-F) characters, preceded by "0x". <p>If you want to enter the key in hexadecimal, type "0x" at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in "0123456789ABCDEF" is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above.</p> <p>The ZyWALL and remote IPSec router must use the same pre-shared key.</p>
Certificate	<p>Select this if the ZyWALL and remote IPSec router use certificates to identify each other when they negotiate the IKE SA. Then, select the certificate the remote IPSec router uses to identify the ZyWALL. This certificate is one of the certificates in My Certificates.</p> <p>Note: The ZyWALL must import the remote IPSec router's certificate before it can establish the IKE SA.</p> <p>The ZyWALL uses one of its Trusted Certificates to authenticate the remote IPSec router. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.</p>
Local ID Type	<p>This field is read-only if the ZyWALL and remote IPSec router use certificates to identify each other. Select which type of identification is used to identify the ZyWALL during authentication. Choices are:</p> <p>IP - the ZyWALL is identified by an IP address</p> <p>DNS - the ZyWALL is identified by a domain name</p> <p>E-mail - the ZyWALL is identified by an e-mail address</p>

Table 71 Network > IPSec VPN > VPN Gateway > Edit (continued)

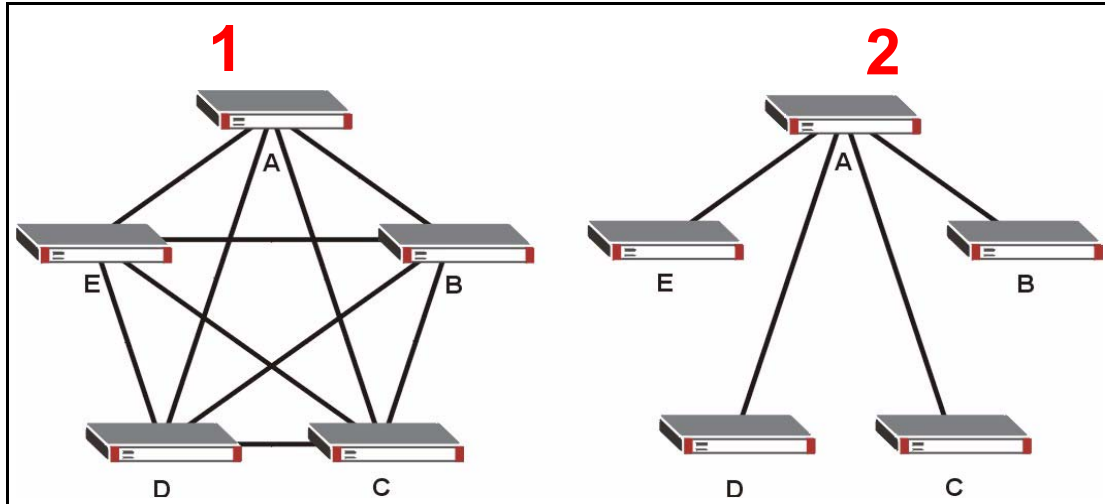
LABEL	DESCRIPTION
Content	<p>This field is read-only if the ZyWALL and remote IPSec router use certificates to identify each other. Type the identity of the ZyWALL during authentication. The identity depends on the Local ID Type.</p> <p>IP - type an IP address; if you type 0.0.0.0, the ZyWALL uses the IP address specified in the My Address field. This is not recommended in the following situations:</p> <ul style="list-style-type: none"> • There is a NAT router between the ZyWALL and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. <p>In these situations, use a different IP address, or use a different Local ID Type.</p> <p>DNS - type the domain name; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.</p> <p>E-mail - the ZyWALL is identified by an e-mail address; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.</p>
Peer ID Type	<p>Select which type of identification is used to identify the remote IPSec router during authentication. Choices are:</p> <p>IP - the remote IPSec router is identified by an IP address</p> <p>DNS - the remote IPSec router is identified by a domain name</p> <p>E-mail - the remote IPSec router is identified by an e-mail address</p> <p>Any - the ZyWALL does not check the identity of the remote IPSec router</p> <p>If the ZyWALL and remote IPSec router use certificates, there is one more choice.</p> <p>Subject Name - the remote IPSec router is identified by the subject name in the certificate</p>
Content	<p>This field is disabled if the Peer ID Type is Any. Type the identity of the remote IPSec router during authentication. The identity depends on the Peer ID Type.</p> <p>If the ZyWALL and remote IPSec router do not use certificates,</p> <p>IP - type an IP address; see the note at the end of this description.</p> <p>DNS - type the domain name; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.</p> <p>E-mail - the ZyWALL is identified by an e-mail address; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.</p> <p>If the ZyWALL and remote IPSec router use certificates, type the following fields from the certificate used by the remote IPSec router.</p> <p>IP - subject alternative name field; see the note at the end of this description.</p> <p>DNS - subject alternative name field</p> <p>E-mail - subject alternative name field</p> <p>Subject Name - subject name (maximum 255 ASCII characters, including spaces)</p> <p>Note: If Peer ID Type is IP, please read the rest of this section.</p> <p>If you type 0.0.0.0, the ZyWALL uses the IP address specified in the Secure Gateway Address field. This is not recommended in the following situations:</p> <ul style="list-style-type: none"> • There is a NAT router between the ZyWALL and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. <p>In these situations, use a different IP address, or use a different Peer ID Type.</p>

Table 71 Network > IPSec VPN > VPN Gateway > Edit (continued)

LABEL	DESCRIPTION
Extended Authentication	
Enable Extended Authentication	Select this if 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 and/or an external server.
Server Mode	Select this if the ZyWALL authenticates the user name and password from the remote IPSec router. You also have to select the authentication method, which specifies how the ZyWALL authenticates this information.
Client Mode	Select this radio button if the ZyWALL provides a username and password to the remote IPSec router for authentication. You also have to provide the User Name and the Password .
User Name	This field is required if the ZyWALL is in Client Mode for extended authentication. Type the user name the ZyWALL sends to the remote IPSec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the ZyWALL is in Client Mode for extended authentication. Type the password the ZyWALL sends to the remote IPSec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Apply	Click Apply to save your changes in the ZyWALL.
Cancel	Click Cancel to exit this screen without saving.

12.5 VPN Concentrator

A VPN concentrator combines several VPN connections into one secure network. [Figure 166 on page 251](#) shows an example of this, as well as one alternative approach.

Figure 166 VPN Topologies

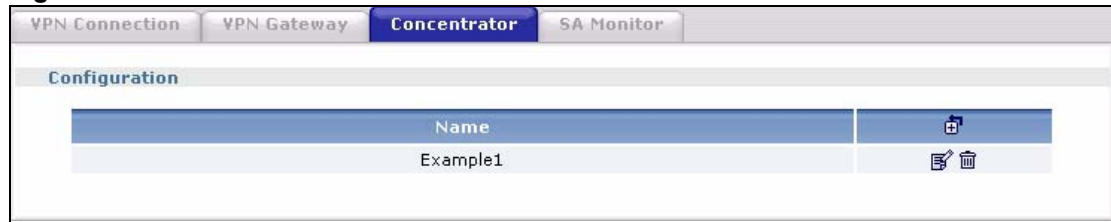
The VPN concentrator is used in the second approach. In the first (fully-meshed) approach, there is a VPN connection between every pair of routers. In the second (hub-and-spoke) approach, there is a VPN connection between each spoke router (**B**, **C**, **D**, and **E**) and the hub router (**A**), which uses the VPN concentrator. The VPN concentrator routes VPN traffic between the spoke routers and itself.

The biggest advantage of a VPN concentrator is that it reduces the number of VPN connections that you have to set up and maintain in the network. You might also be able to consolidate the policy routes in each spoke router, depending on the IP addresses and subnets of each spoke.

You should not use a VPN concentrator in every situation, however. The hub router is a single point of failure, so a VPN concentrator is not as appropriate if the connection between spoke routers cannot be down occasionally (maintenance, for example). In addition, there is a significant burden on the hub router. It receives VPN traffic from one spoke, decrypts it, inspects it to find out to which spoke to route it, encrypts it, and sends it to the appropriate spoke. Therefore, a VPN concentrator is more suitable when there is a minimum amount of traffic between spoke routers.

12.5.1 VPN Concentrator Summary

You use the **VPN Concentrator** summary screen to look at the VPN concentrators you have set up. The **VPN Concentrator** summary screen displays the VPN concentrators in the ZyWALL. To access this screen, click **Configuration > Network > IPSec VPN > Concentrator**. The following screen appears.

Figure 167 Network > IPsec VPN > Concentrator

Each field is discussed in the following table. See [Section 12.5.2 on page 252](#) for more information.

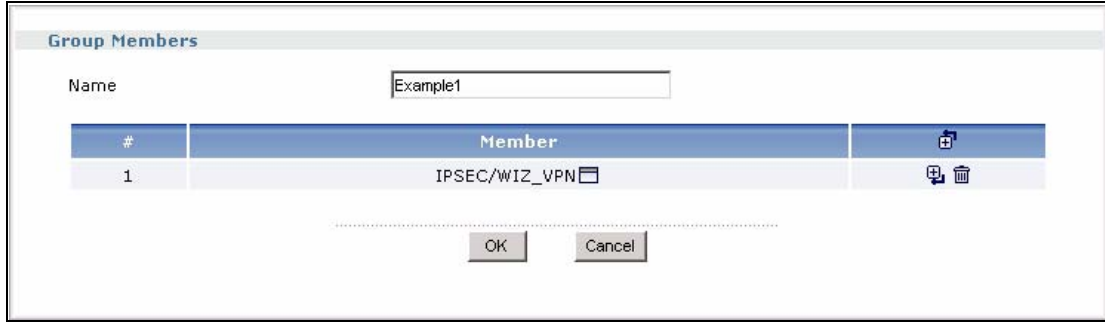
Table 72 Network > IPsec VPN > Concentrator

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific concentrator.
Name	This field displays the name of the VPN concentrator.
Add icon	This column provides icons to add, edit, and remove VPN concentrators. To add a VPN concentrator, click the Add icon at the top of the column. The VPN Concentrator Add/Edit screen appears. To edit a VPN concentrator, click the Edit icon next to the concentrator. The VPN Concentrator Add/Edit screen appears accordingly. To delete a VPN concentrator, click on the Remove icon next to the concentrator. The web configurator confirms that you want to delete the VPN concentrator.

12.5.2 VPN Concentrator Add/Edit

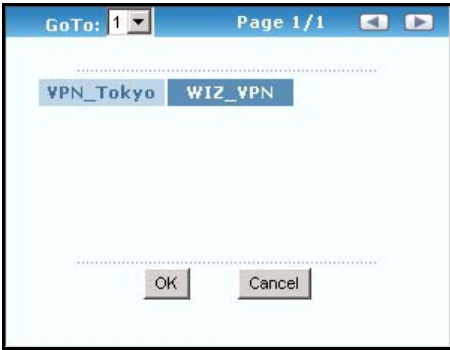
The **VPN Concentrator Add/Edit** screen allows you to create a new VPN concentrator or edit an existing one. To access this screen, go to the **VPN Concentrator Summary** screen (see [Section 12.5.1 on page 251](#)), and click either the **Add** icon or an **Edit** icon.

Figure 168 Network > IPsec VPN > Concentrator > Edit



Each field is described in the following table.

Table 73 Network > IPsec VPN > Concentrator > Edit

LABEL	DESCRIPTION
Name	Enter the name of the concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
#	This field is a sequential value, and it is not associated with a specific member in the concentrator.
Member List	<p>This field displays the name of each member in the concentrator.</p> <p>Note: You must disable policy enforcement in each member. See Section 12.3.2 on page 230.</p> <p>Click the Popup icon to change this member in the group. The following screen appears.</p> <p>Figure 169 Network > IPsec VPN > Concentrator > Edit > Member</p> 
Add icon	<p>This column provides icons to add members to and remove members from the concentrator.</p> <p>To add a member to the concentrator, click the Add icon at the top of the column to add the new member at the beginning of the list, or click the Add icon next to an existing member to add the new member after the existing one. The web configurator chooses a new member alphabetically. You can use the Popup icon next to the new member to change this.</p> <p>To remove a member from the concentrator, click on the Remove icon next to the member. The web configurator confirms that you want to remove the member.</p>
OK	Click OK to save your changes in the ZyWALL.
Cancel	Click Cancel to exit this screen without saving.

12.6 SA Monitor Screen

You can use the **SA Monitor** screen to display and to manage active IPsec SA. To access this screen, click **Configuration > Network > IPsec VPN > SA Monitor**. The following screen appears.

Figure 170 Network > IPsec VPN > SA Monitor

#	Name	Encapsulation	Policy	Algorithm	Up Time	Timeout	Inbound (Bytes)	Outbound (Bytes)	Disconnect
1	YU2	Tunnel	192.168.252.0-192.168.255.255<->192.168.248.0-192.168.251.255	NULL/MD5	35	86395	0	0	
2	ipsec4	Tunnel	192.168.29.230-192.168.29.231<->192.168.8.1-192.168.8.33	AES128/SHA1	39	86391	0	0	

Each field is described in the following table.

Table 74 Network > IPsec VPN > SA Monitor

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPsec SA.
Encapsulation	This field displays how the IPsec SA is encapsulated.
Policy	This field displays the content of the local and remote policies for this IPsec SA. The IP addresses, not the address objects, are displayed.
Algorithm	This field displays the encryption and authentication algorithms used in the SA.
Up Time	This field displays how many seconds the IPsec SA has been active. This field displays N/A if the IPsec SA uses manual keys.
Timeout	This field displays how many seconds remain in the SA life time, before the ZyWALL automatically disconnects the IPsec SA. This field displays N/A if the IPsec SA uses manual keys.
Inbound (Bytes)	This field displays the amount of traffic that has gone through the IPsec SA from the remote IPsec router to the ZyWALL since the IPsec SA was established.
Outbound (Bytes)	This field displays the amount of traffic that has gone through the IPsec SA from the ZyWALL to the remote IPsec router since the IPsec SA was established.
Disconnect	This field is displayed if the IPsec SA does not use manual keys. Click the Disconnect icon next to an IPsec SA to disconnect it.
Refresh	Click Refresh to update the information in the display.

CHAPTER 13

Routing Protocol

This chapter describes how to set up RIP and OSPF routing protocols for the ZyWALL. First, it provides an overview of RIP and OSPF, and, then, it introduces the RIP and OSPF screens used to configure routing protocols. [See the Objects section](#) in the Configuration Overview chapter for related information on these screens.

13.1 Routing Protocol Overview

Routing protocols give the ZyWALL routing information about the network from other routers. The ZyWALL then stores this routing information in the routing table, which it uses when it makes routing decisions. In turn, the ZyWALL can also provide routing information via routing protocols to other routers.

The ZyWALL supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared in [Table 75 on page 255](#), and they are discussed further in the next two sections.

Table 75 OSPF vs. RIP

	OSPF	RIP
Network Size	Large	Small (with up to 15 routers)
Metric	Bandwidth, hop count, throughput, round trip time and reliability.	Hop count
Convergence	Fast	Slow

13.1.1 RIP Overview

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers. RIP is a vector-space routing protocol, and, like most such protocols, it uses hop count to decide which route is the shortest. Unfortunately, it also broadcasts its routes asynchronously to the network and converges slowly. Therefore, RIP is more suitable for small networks (up to 15 routers).

In the ZyWALL, you can configure two sets of RIP settings before you can use it in an interface.

First, the **Authentication** field specifies how to verify that the routing information that is received is the same routing information that is sent. This is discussed in more detail in [Section 13.1.2 on page 256](#).

Second, the ZyWALL can also **redistribute** routing information from non-RIP networks, specifically OSPF networks and static routes, to the RIP network. Costs might be calculated differently, however, so you use the **Metric** field to specify the cost in RIP terms.

RIP uses UDP port 520.

13.1.2 Authentication Types

Authentication is used to guarantee the integrity, but not the confidentiality, of routing updates. The transmitting router uses its key to encrypt the original message into a smaller message, and the smaller message is transmitted with the original message. The receiving router uses its key to encrypt the received message and then verifies that it matches the smaller message sent with it. If the received message is verified, then the receiving router accepts the updated routing information. The transmitting and receiving routers must have the same key.

The ZyWALL supports three authentication methods for RIP and OSPF routing protocols:

- **None** - no authentication is used.
- **Text** – authentication using a plain text password, and the (unencrypted) password is sent over the network. This method is usually used temporarily to prevent network problems.
- **MD5** – authentication using an MD5 password and authentication ID.

MD5 is an authentication method that produces a 128-bit checksum, called a message-digest, for each packet. It also includes an authentication ID, which can be set to any value between 1 and 255. The ZyWALL only accepts packets if these conditions are satisfied.

- The packet's authentication ID is the same as the authentication ID of the interface that received it.
- The packet's message-digest is the same as the one the ZyWALL calculates using the MD5 password.

For RIP, authentication is not available in RIP version 1. In RIP version 2, you can only select one authentication type for all interfaces. For OSPF, the ZyWALL supports a default authentication type by area. If you want to use this default in an interface or virtual link, you set the associated **Authentication Type** field to **Same as Area**. As a result, you only have to update the authentication information for the area to update the authentication type used by these interfaces and virtual links. Alternatively, you can override the default in any interface or virtual link by selecting a specific authentication method. Please see the respective interface sections for more information.

13.2 RIP Screen

The **RIP** screen is used to specify the authentication method, and it is used to maintain the policies for redistribution.

To access this screen, login to the web configurator. When the main screen appears, click once on **Network** to open the **Network** tree, and then click once on **Routing Protocol**. The **RIP** tab is selected by default. The following screen appears.

Figure 171 Network > Routing Protocol > RIP

Active	Name	Metric (0-16)
<input type="checkbox"/>	OSPF	0
<input type="checkbox"/>	Static Route	0

The following table describes the labels in this screen.

Table 76 Network > Routing Protocol > RIP

LABEL	DESCRIPTION
Authentication	
Authentication	Select the authentication method used in the RIP network. Choices are: None , Text , and MD5 .
Text Authentication Key	This field is available if the Authentication is Text . Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5 . Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5 . Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Redistribute	
Active	Select this check box to advertise routes that were learned from the indicated Name .
Name	This field displays other sources of routing information that the ZyWALL can advertise in the RIP network.
Metric	Type the cost for routes provided by the indicated source. The metric represents the "cost" of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used.

13.3 OSPF Overview

OSPF (Open Shortest Path First, RFC 2328) is a link-state protocol designed to distribute routing information within a group of networks, called an Autonomous System (AS). OSPF offers some advantages over vector-space routing protocols like RIP.

- OSPF supports variable-length subnet masks, which can be set up to use available IP addresses more efficiently.
- OSPF filters and summarizes routing information, which reduces the size of routing tables throughout the network.
- OSPF responds to changes in the network, such as the loss of a router, more quickly.
- OSPF considers several factors, including bandwidth, hop count, throughput, round trip time, and reliability, when it calculates the shortest path.
- OSPF converges more quickly than RIP.

Naturally, OSPF is also more complicated than RIP, so OSPF is usually more suitable for large networks.

OSPF uses IP protocol 89.

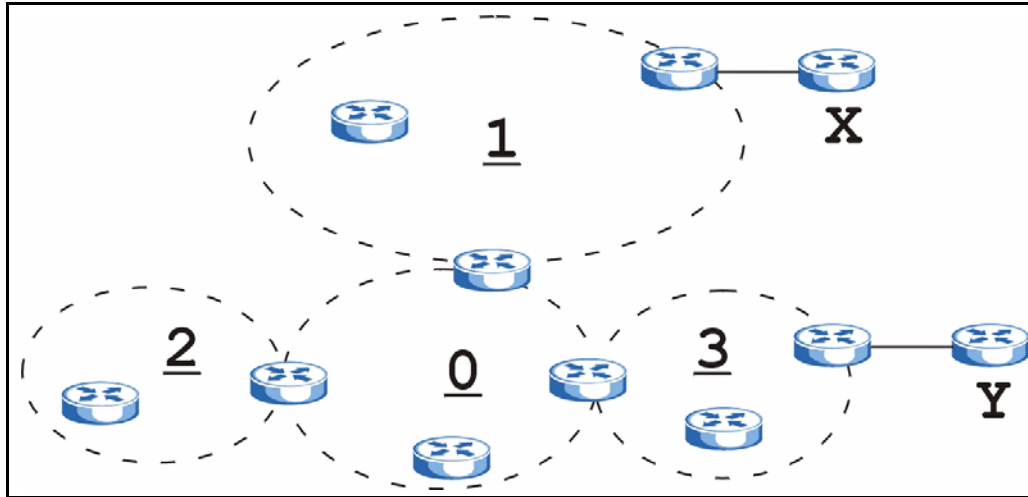
13.3.1 OSPF Areas

An OSPF Autonomous System (AS) is divided into one or more areas. Each area represents a group of adjacent networks and is identified by a 32-bit ID. In OSPF, this number may be expressed as an integer or as an IP address.

There are several types of areas.

- The backbone is the transit area that routes packets between other areas. All other areas are connected to the backbone.
- A normal area is a group of adjacent networks. A normal area has routing information about the OSPF AS, any networks outside the OSPF AS to which it is directly connected, and any networks outside the OSPF AS that provide routing information to any area in the OSPF AS.
- A stub area has routing information about the OSPF AS. It does not have any routing information about any networks outside the OSPF AS, including networks to which it is directly connected. It relies on a default route to send information outside the OSPF AS.
- A Not So Stubby Area (NSSA, RFC 1587) has routing information about the OSPF AS and networks outside the OSPF AS to which the NSSA is directly connected. It does not have any routing information about other networks outside the OSPF AS.

Each type of area is illustrated in the following figure.

Figure 172 OSPF: Types of Areas

This OSPF AS consists of four areas, areas 0-3. Area 0 is always the backbone. In this example, areas 1, 2, and 3 are all connected to it. Area 1 is a normal area. It has routing information about the OSPF AS and networks X and Y. Area 2 is a stub area. It has routing information about the OSPF AS, but it depends on a default route to send information to networks X and Y. Area 3 is a NSSA. It has routing information about the OSPF AS and network Y but not about network X.

13.3.2 OSPF Routers

Every router in the same area has the same routing information. They do this by exchanging Hello messages to confirm which neighbor (layer-3) devices exist, and then they exchange database descriptions (DDs) to create a synchronized link-state database. The link-state database contains records of router IDs, their associated links and path costs. The link-state database is then constantly updated through Link State Advertisements (LSA). Each router uses the link state database and the Dijkstra algorithm to compute the least cost paths to network destinations.

Like areas, each router has a unique 32-bit ID in the OSPF AS, and there are several types of routers. Each type is really just a different role, and it is possible for one router to play multiple roles at one time.

- An internal router (IR) only exchanges routing information with other routers in the same area.
- An Area Border Router (ABR) connects two or more areas. It is a member of all the areas to which it is connected, and it filters, summarizes, and exchanges routing information between them.

- An Autonomous System Boundary Router (ASBR) exchanges routing information with routers in networks outside the OSPF AS. This is called redistribution in OSPF.

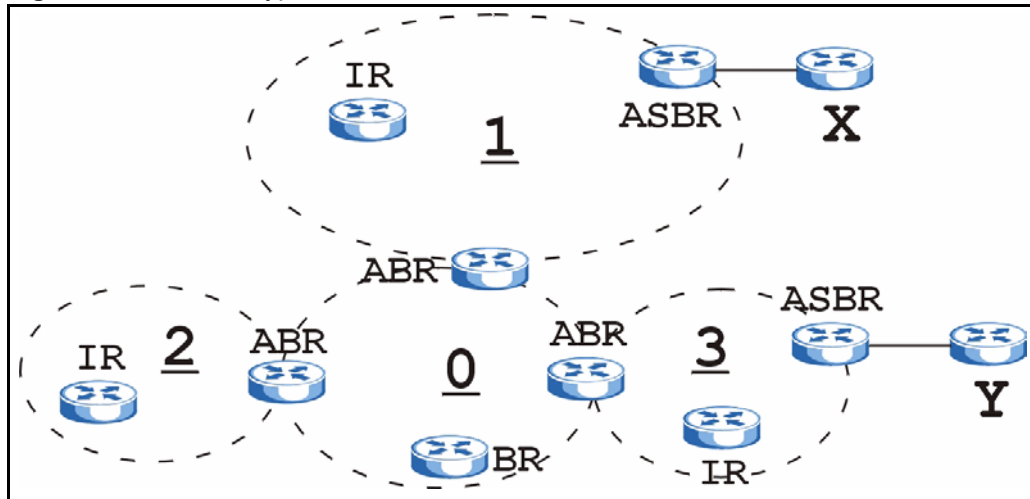
Table 77 OSPF: Redistribution from Other Sources to Each Type of Area

SOURCE \ TYPE OF AREA	NORMAL	NSSA	STUB
Static routes	Yes	Yes	No
RIP	Yes	Yes	Yes

- A backbone router (BR) has at least one interface with area 0. By default, every router in area 0 is a backbone router, and so is every ABR.

Each type of router is illustrated in the following example.

Figure 173 OSPF: Types of Routers

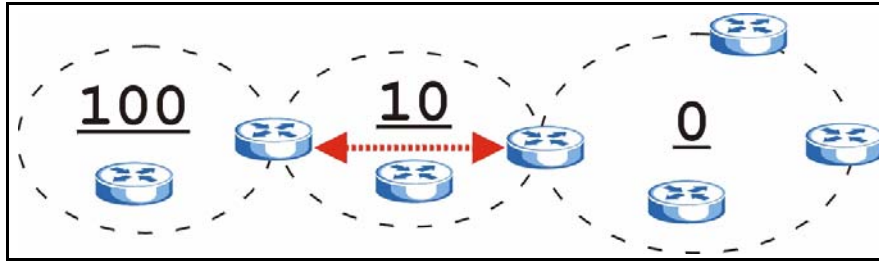


In order to reduce the amount of traffic between routers, a group of routers that are directly connected to each other selects a designated router (DR) and a backup designated router (BDR). All of the routers only exchange information with the DR and the BDR, instead of exchanging information with all of the other routers in the group. The DR and BDR are selected by priority; if two routers have the same priority, the highest router ID is used.

The DR and BDR are selected in each group of routers that are directly connected to each other. If a router is directly connected to several groups, it might be a DR in one group, a BDR in another group, and neither in a third group all at the same time.

13.3.3 Virtual Links

In some OSPF AS, it is not possible for an area to be directly connected to the backbone. In this case, you can create a virtual link through an intermediate area to logically connect the area to the backbone. This is illustrated in the following example.

Figure 174 OSPF: Virtual Link

In this example, area 100 does not have a direct connection to the backbone. As a result, you should set up a virtual link on both ABR in area 10. The virtual link becomes the connection between area 100 and the backbone.

You cannot create a virtual link to a router in a different area.

13.3.4 OSPF Configuration

Follow these steps when you configure OSPF on the ZyWALL.

- 1 Enable OSPF.
- 2 Set up the OSPF areas.
- 3 Configure the appropriate interfaces. See [Section 10.2.1 on page 183](#).
- 4 Set up virtual links, as needed.

13.4 OSPF Screens

The OSPF screens are used to specify the ID the ZyWALL uses in the OSPF AS and to maintain the policies for redistribution. In addition, they are also used to create, maintain, and remove OSPF areas.

13.4.1 OSPF Summary

The **OSPF** screen is used to specify the OSPF router and maintain the policies for redistribution. In addition, it provides a summary of OSPF areas, allows you to remove them, and opens the **OSPF Add/Edit** screen to add or edit them.

To access this screen, login to the web configurator. When the main screen appears, click once on **Network** to open the **Network** tree, and then click once on **Routing Protocol**. Click once on the **OSPF** tab. The following screen appears.

Figure 175 Network > Routing Protocol > OSPF

The following table describes the labels in this screen. See [Section 13.4.2 on page 263](#) for more information as well.

Table 78 Network > Routing Protocol > OSPF

LABEL	DESCRIPTION
OSPF Router ID	Select the 32-bit ID the ZyWALL uses in the OSPF AS. Default - the highest available IP address assigned to the interfaces is the ZyWALL's ID. User Define - enter the ID (in IP address format) in the field that appears when you select User Define .
Redistribute	
Active	Select this check box to advertise routes that were learned from the indicated source. <ul style="list-style-type: none"> If you select this for RIP, the ZyWALL advertises routes learned from RIP to Normal and NSSA areas but not to Stub areas. If you select this for static routes, the ZyWALL advertises routes learned from static routes to all types of areas.
Route	This field displays other sources of routing information that the ZyWALL can advertise in the OSPF AS.
Type	Select how OSPF calculates the cost associated with routing information from the indicated source. Choices are: Type 1 and Type 2 . Type 1 - cost = OSPF AS cost + external cost (Metric) Type 2 - cost = external cost (Metric); the OSPF AS cost is ignored.
Metric	Type the external cost for routes provided by the indicated source. The metric represents the "cost" of transmission for routing purposes. The way this is used depends on the Type field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214.
Area	This section displays information about OSPF areas in the ZyWALL.
#	This field is a sequential value, and it is not associated with a specific area.
Area	This field displays the 32-bit ID for each area in IP address format.
Type	This field displays the type of area. This type is different from the Type field above.

Table 78 Network > Routing Protocol > OSPF (continued)

LABEL	DESCRIPTION
Authentication	This field displays the default authentication method in the area.
Add icon	This column provides icons to add, edit, and remove areas. To add an area, click the Add icon at the top of the column. The OSPF Area Add/Edit screen appears. To edit an area, click the Edit icon next to the area. The Area Add/Edit screen appears. To delete an area, click on the Remove icon next to the area. The web configurator confirms that you want to delete the area before doing so.

13.4.2 OSPF Area Add/Edit

The **OSPF Area Add/Edit** screen allows you to create a new area or edit an existing one. To access this screen, go to the **OSPF** summary screen (see [Section 13.4.1 on page 261](#)), and click either the **Add** icon or an **Edit** icon.

Figure 176 Network > Routing Protocol > OSPF > Edit

The screenshot shows the 'Area Setting' configuration page. It includes fields for 'Area ID', 'Type' (set to 'Normal'), 'Authentication' (set to 'MD5'), 'MD5 Authentication ID' (set to '1'), and 'MD5 Authentication Key' (set to '0'). Below these is a 'Virtual Link' table with one entry. The table has columns for '#', 'Peer Router ID', 'Authentication', and a set of controls for 'MD5 Authentication ID' and 'MD5 Authentication Key'. The entry has '# 1', an empty 'Peer Router ID' field, 'MD5' for 'Authentication', and empty fields for the authentication ID and key. 'OK' and 'Cancel' buttons are at the bottom.

The following table describes the labels in this screen.

Table 79 Network > Routing Protocol > OSPF > Edit

LABEL	DESCRIPTION
Area ID	Type the unique, 32-bit identifier for the area in IP address format.
Type	This field displays the type of area. Normal - This area is a normal area. It has routing information about the OSPF AS and about networks outside the OSPF AS. Stub - This area is an stub area. It has routing information about the OSPF AS but not about networks outside the OSPF AS. It depends on a default route to send information outside the OSPF AS. NSSA - This area is a Not So Stubby Area (NSSA), per RFC 1587. It has routing information about the OSPF AS and networks that are outside the OSPF AS and are directly connected to the NSSA. It does not have information about other networks outside the OSPF AS.
Authentication	This field displays the default authentication method in the area. Choices are: None , Text , and MD5 .
Text Authentication Key	This field is available if the Authentication is Text . Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5 . Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5 . Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Virtual Link	This section is displayed if the Type is Normal . Create a virtual link if you want to connect a different area (that does not have a direct connection to the backbone) to the backbone. You should set up the virtual link on the ABR that is connected to the other area and on the ABR that is connected to the backbone.
#	This field is a sequential value, and it is not associated with a specific area.
Peer Router ID	Type the 32-bit ID (in IP address format) of the other ABR in the virtual link.

Table 79 Network > Routing Protocol > OSPF > Edit (continued)

LABEL	DESCRIPTION
Authentication	Select which authentication method to use in the virtual link. Choices are: None , Text , MD5 , and Same as Area . In this case, Same as Area refers to the Authentication settings above.
Text Authentication Key	This field is available if the Authentication is Text . Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5 . Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5 . Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Add icon	<p>This column provides icons to add and remove virtual links.</p> <p>To add a virtual link, click the Add icon at the top of the column. A new record appears in the virtual link list.</p> <p>To delete a virtual link, click on the Remove icon next to the virtual link. The web configurator confirms that you want to delete the virtual link.</p>

CHAPTER 14

Zones

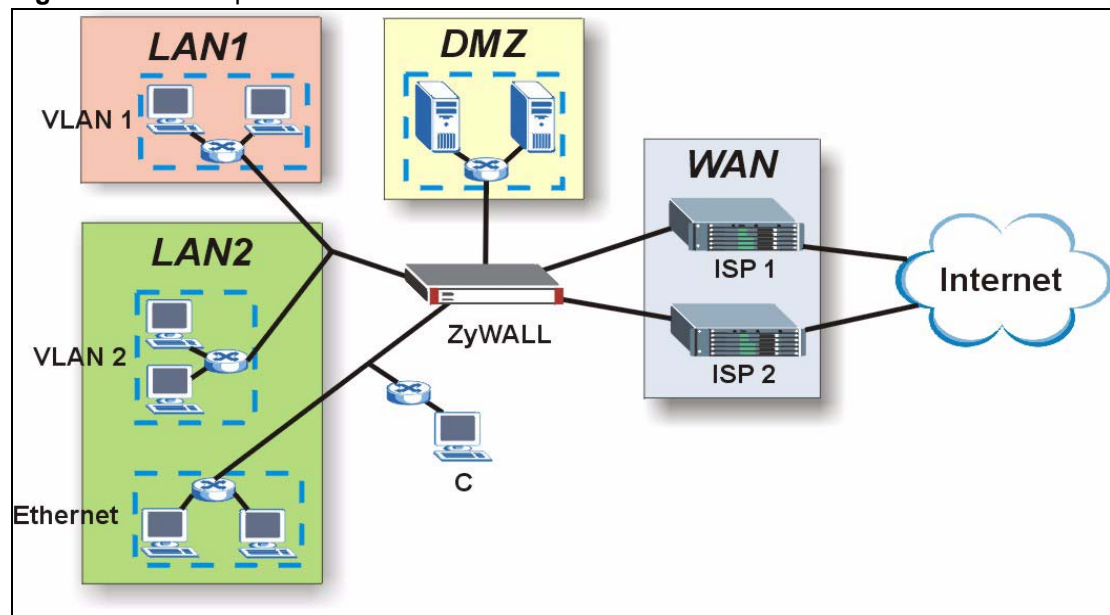
Set up zones to configure network security and network policies in the ZyWALL. [See the Zones section](#) in the Configuration Overview chapter for related information on these screens.

14.1 Zones Overview

A zone is a group of interfaces and VPN tunnels. The ZyWALL uses zones, not interfaces, in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface, auxiliary interface, and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

Figure 177 Example: Zones



14.1.1 Effect of Zones on Different Types of Traffic

Zones effectively divide traffic into three types--intra-zone traffic, inter-zone traffic, and extra-zone traffic--which are affected differently by zone-based security and policy settings.

Intra-zone traffic is traffic between interfaces or VPN tunnels in the same zone. For example, in [Figure 177 on page 267](#), traffic between VLAN 2 and the Ethernet is intra-zone traffic. In each zone, you can either allow or prohibit all intra-zone traffic. For example, in [Figure 177 on page 267](#), you might allow intra-zone traffic in the LAN2 zone but prohibit it in the WAN zone. You can also set up firewall rules to control intra-zone traffic (for example, LAN2-to-LAN2), but many other types of zone-based security and policy settings do not affect intra-zone traffic.

Inter-zone traffic is traffic between interfaces or VPN tunnels in different zones. For example, in [Figure 177 on page 267](#), traffic between VLAN 1 and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

Extra-zone traffic is traffic to or from any interface or VPN tunnel that is not assigned to a zone. For example, in [Figure 177 on page 267](#), traffic to or from computer C is extra-zone traffic. Some zone-based security and policy settings may apply to extra-zone traffic, especially if you can set the zone attribute in them to **Any** or **All**. See the specific feature for more information.

14.2 Zone Summary

The **Zone** screen provides a summary of all zones. In addition, this screen allows you to add, edit, and remove zones. To access this screen, click **Network > Zone**.

Figure 178 Network > Zone

Configuration		
Name	Block Intra-zone Traffic	
LAN	No	
WAN	Yes	
DMZ	Yes	

The following table describes the labels in this screen.

Table 80 Network > Zone

LABEL	DESCRIPTION
Name	This field displays the name of the zone.
Block Intra-zone Traffic	This field indicates whether or not the ZyWALL blocks network traffic between members in the zone.
Add icon	This column provides icons to add, edit, and remove zones. To add a zone, click the Add icon at the top of the column. The Zone Add/Edit screen appears. To edit a zone, click the Edit icon next to the zone. The Zone Add/Edit screen appears. To delete a zone, click the Remove icon next to the zone. The web configurator confirms that you want to delete the zone before doing so.

14.3 Zone Add/Edit

The **Zone Add/Edit** screen allows you to define a zone or edit an existing one. To access this screen, go to the **Zone** screen (see [Section 14.2 on page 268](#)), and click either the **Add** icon or an **Edit** icon.

Figure 179 Configuration > Network > Zone > Edit

The following table describes the labels in this screen.

Table 81 Configuration > Network > Zone > Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the zone. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Block Intra-zone Traffic	Select this check box to block network traffic between members in the zone.
#	This field is a sequential value, and it is not associated with a specific member of the zone.
Member	This field displays the name of each member in the zone. The word in front of the name indicates whether this member is an interface or a VPN tunnel. IFACE - this member is an interface. IPSEC - this member is a VPN tunnel. Click the icon next to each member to change the member. You can only add interfaces and VPN tunnels that are not assigned to a zone, however.
Add icon	This column provides icons to add members to and remove members from the zone. To add a member to the zone, click the Add icon at the top of the column to add the new member at the beginning of the list, or click the Add icon next to an existing member to add the new member after the existing one. The web configurator chooses a new member alphabetically. You can use the Popup icon next to the member to change this choice. To remove a member from the zone, click the Remove icon next to the member. The web configurator confirms that you want to remove the member.

CHAPTER 15

ISP Accounts

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE/PPTP interfaces. See the [Objects section](#) in the Configuration Overview chapter for related information on these screens.

15.1 ISP Accounts Overview

An ISP account is a profile of settings for Internet access using PPPoE or PPTP. See [Section 10.6 on page 206](#) for information about PPPoE/PPTP interfaces.

15.2 ISP Account Summary

This screen provides a summary of ISP accounts in the ZyWALL. To access this screen, click **Network > ISP Account**.

Figure 180 Network > ISP Account

Profile Name	Protocol	Authentication Type	User Name	
SunnyISP	pppoe	chap-pap	hello	
Hinet	pppoe	chap-pap	there	

The following table describes the labels in this screen. See the [ISP Account Edit section](#) below for more information as well.

Table 82 Network > ISP Account

LABEL	DESCRIPTION
Profile Name	This field displays the profile name of the ISP account. This name is used to identify the ISP account.
Protocol	This field displays the protocol used by the ISP account.
Authentication Type	This field displays the authentication type used by the ISP account.

Table 82 Network > ISP Account (continued)

LABEL	DESCRIPTION
User Name	This field displays the user name of the ISP account.
Add icon	This column provides icons to add, edit, and remove ISP accounts. To add information about a new ISP account, click the Add icon at the top of the column. The ISP Account Edit screen appears. To edit information about an existing account, click the Edit icon next to the ISP account. The ISP Account Edit screen appears. To remove information about an existing account, click the Remove icon next to the ISP account. The web configurator confirms that you want to delete the account before doing so.

15.3 ISP Account Edit

The **ISP Account Edit** screen lets you add information about new accounts and edit information about existing accounts. To open this window, open the **ISP Account** screen. (See [Section 15.2 on page 271](#).) Then, click on an **Add** icon or **Edit** icon to open the **ISP Account Edit** screen below.

Figure 181 Network > ISP Account > Edit

The following table describes the labels in this screen.

Table 83 Network > ISP Account > Edit

LABEL	DESCRIPTION
Profile Name	This field is read-only if you are editing an existing account. Type in the profile name of the ISP account. The profile name is used to refer to the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Protocol	This field is read-only if you are editing an existing account. Select the protocol used by the ISP account. Options are: pppoe - This ISP account uses the PPPoE protocol. pptp - This ISP account uses the PPTP protocol.

Table 83 Network > ISP Account > Edit (continued)

LABEL	DESCRIPTION
Encryption Method	This field is available if this ISP account uses the PPTP protocol. Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: nomppe - This ISP account does not use MPPE. mppe-40 - This ISP account uses 40-bit MPPE. mppe-128 - This ISP account uses 128-bit MMPE.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: CHAP/PAP - Your ZyWALL accepts either CHAP or PAP when requested by this remote node. CHAP - Your ZyWALL accepts CHAP only. PAP - Your ZyWALL accepts PAP only. MSCHAP - Your ZyWALL accepts MSCHAP only. MSCHAP-V2 - Your ZyWALL accepts MSCHAP-V2 only.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above. The password can only consist of alphanumeric characters (A-Z, a-z, 0-9). This field can be blank.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Server IP	If this ISP account uses the PPPoE protocol, this field is not displayed. If this ISP account uses the PPTP protocol, type the IP address of the PPTP server.
Connection ID	This field is available if this ISP account uses the PPTP protocol. Type your identification name for the PPTP server. This field can be blank.
Service Name	If this ISP account uses the PPPoE protocol, type the PPPoE service name to access. PPPoE uses the specified service name to identify and reach the PPPoE server. This field can be blank. If this ISP account uses the PPTP protocol, this field is not displayed.
Compression	Select On button to turn on stac compression, and select Off to turn off stac compression. Stac compression is a data compression technique capable of compressing data by a factor of about four.
Idle Timeout	This value specifies the number of seconds that must elapse without outbound traffic before the ZyWALL automatically disconnects from the PPPoE/PPTP server. This value must be an integer between 0 and 360. If this value is zero, this timeout is disabled.
OK	Click OK to save your changes back to the ZyWALL. If there are no errors, the program returns to the ISP Account screen. If there are errors, a message box explains the error, and the program stays in the ISP Account Edit screen.
Cancel	Click Cancel to return to the ISP Account screen without creating the profile (if it is new) or saving any changes to the profile (if it already exists).

CHAPTER 16

Device HA

Use device HA and Virtual Router Redundancy Protocol (VRRP) to increase network reliability. See the [Device HA section](#) in the Configuration Overview chapter for related information on these screens.

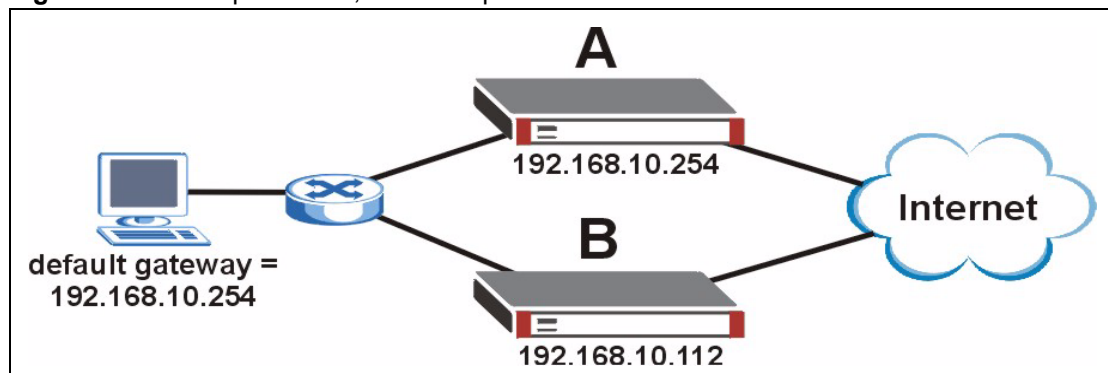
16.1 Virtual Router Redundancy Protocol (VRRP) Overview

Every computer on a network may send packets to a default gateway, which can become a single point of failure. Virtual Router Redundancy Protocol (VRRP) allows you to create redundant backup gateways to ensure that the default gateway is always available.

Note: The ZyWALL 1050 runs VRRP v2. You can only set up device HA with other ZyWALL 1050s running the same firmware version.

In VRRP, a virtual router represents a number of routers associated with one IP address, the IP address of the default gateway. Each virtual router is identified by a unique 8-bit identification number called a Virtual Router ID (VR ID). In the example below, Router A and Router B are part of virtual router 10 with IP address 192.168.10.254.

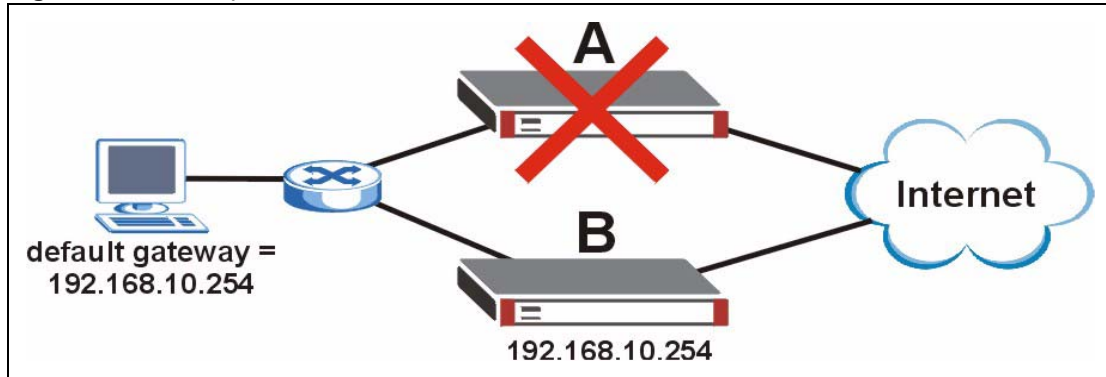
Figure 182 Example: VRRP, Normal Operation



The VR ID is not shown. In normal operation, Router A is the master router. It has the same IP address as the default gateway and forwards traffic for the network. Router B is a backup router. It is using its management IP address 192.168.10.112. Router A sends regular messages to Router B to let Router B know that Router A is available. The time interval between these messages is called the advertisement interval.

Note: Every router in a virtual router must use the same advertisement interval.

If Router A becomes unavailable, it stops sending messages to Router B. Router B detects this and assumes the role of the master router. This is illustrated below.

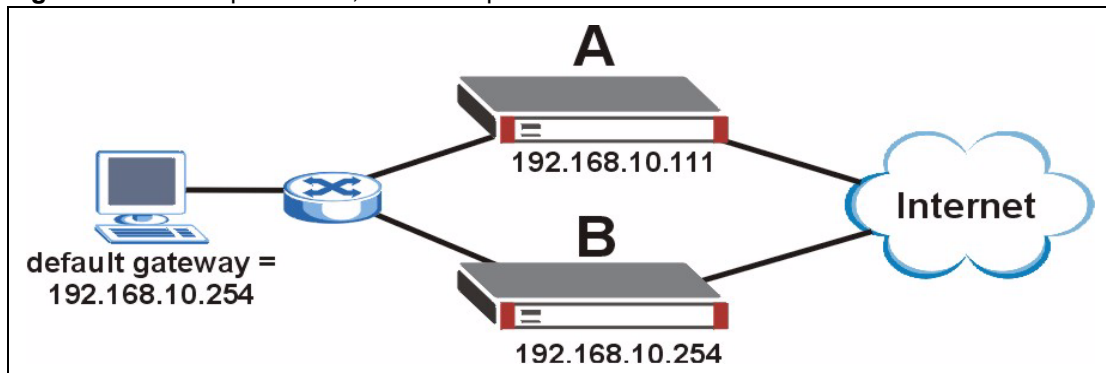
Figure 183 Example: VRRP, Master Becomes Unavailable

Router B is now using the IP address of the default gateway, and it is forwarding packets for the network. The loss of Router A has no effect on the network.

If there is more than one backup router, the backup router with the highest priority becomes the master router. The other backup routers remain backup routers.

If Router A becomes available again, one of two things can happen, depending on the settings in Router A.

- 1 Router A may preempt Router B and become the master router again. In this case, the network returns to the state shown in [Figure 182 on page 275](#).
- 2 Router A returns to the network, but Router B remains the master router. This is illustrated below.

Figure 184 Example: VRRP, No Preempt

In this case, Router A becomes a backup router, and it uses its Manage IP, 192.168.10.111. Router B remains the master router until it becomes unavailable.

16.1.1 Additional VRRP Notes

- It is possible to set up two virtual routers so that they back up each other.
- VRRP uses IP protocol 112.

16.2 VRRP Group Overview

In the ZyWALL, you should create a VRRP group to add one of its interfaces to a virtual router. You can add any Ethernet interface, VLAN interface, or virtual interface (created on top of Ethernet interfaces or VLAN interfaces) with a static IP address.

Note: You can only use interfaces that have static IP addresses.

You can only enable one VRRP group for each interface, and you can only have one active VRRP group for each virtual router.

You must set up a static IP address for the interface first, and this IP address should be the IP address of the virtual router, not the management IP address. The management IP address is assigned in the VRRP group. When the ZyWALL is the master router, the interface uses its IP address, the IP address of the virtual router. If the ZyWALL is a backup router, the interface uses its management IP address. You can look at the current IP address of the interface in the **Status** screen.

Note: You can only have one active VRRP group for each interface, and you can only have one active VRRP group for each virtual router (VR ID).

If there is a PPPoE/PPTP interface on top of an interface in a VRRP group, the PPPoE/PPTP interface cannot connect to the ISP until the interface becomes the master in the virtual router.

At the time of writing, the advertisement interval is fixed at one second.

You can also set up authentication for a VRRP group. If you select AH MD5 authentication, the VRRP group uses IP protocol 51 (AH), instead of IP protocol 112 (VRRP).

16.3 Device HA Screens

The **VRRP Group** summary screen provides information about which interfaces are in virtual routers and the role and status of each interface in the virtual router.

The **VRRP Group Add/Edit** screen allows you to add VRRP groups to the ZyWALL or to edit the configuration of an existing VRRP group. You have to go to the **VRRP Group** summary screen first to access this screen.

Finally, you can use the **Synchronize** screen to make sure ZyWALL routers have the same updated IDP signatures, and configuration information, regardless of whether each router is the master router or a backup router.

16.4 VRRP Group Summary

The **VRRP Group** summary screen provides information about which interfaces are in virtual routers and the role and status of each interface in the virtual router. To access this screen, click **Network > Device HA**.

Figure 185 Network > Device HA > VRRP Group

#	Name	VRID	Role	Interface	HA Status	
1	VR5	5	master	ge4	n/a	⚙️ 📄 🗑️
2	VR7	5	master	vlan1	Active	💡 📄 🗑️

The following table describes the labels in this screen. See [Section 16.5 on page 279](#) for more information as well.

Table 84 Network > Device HA > VRRP Group

LABEL	DESCRIPTION
Refresh	Click this button to update the information in this screen.
#	This field is a sequential value, and it is not associated with a specific VRRP group.
Name	This field displays the name of the VRRP group.
VRID	This field displays the virtual router ID number.
Role	This field displays which role the interface plays in the virtual router. Master - This interface is the master interface in the virtual router. The interface always uses its static IP address, not the management IP address of the VRRP group. Backup - This interface is a backup interface in the virtual router. The interface may use its static IP address or the management IP address of the VRRP group, depending on whether or not the backup has become the master.
Interface	This field displays which interface is part of the virtual router.

Table 84 Network > Device HA > VRRP Group (continued)

LABEL	DESCRIPTION
HA Status	<p>This field displays the status of the interface in the virtual router.</p> <p>Active - This interface is the master interface in the virtual router.</p> <p>Stand-By - This interface is a backup interface in the virtual router.</p> <p>Fault - This VRRP group is not functioning in the virtual router right now. For example, this might happen if the interface is down.</p> <p>n/a - This interface is not connected to the virtual router. For example, this might happen when the VRRP group is first set up.</p>
Add icon	<p>This column provides icons to activate, deactivate, add, edit, and remove VRRP groups.</p> <p>To activate or deactivate a VRRP group, click the Active icon next to the group.</p> <p>To add a VRRP group, click the Add icon at the top of the column. The VRRP Group Add/Edit screen appears.</p> <p>To edit a VRRP group, click the Edit icon next to the group. The VRRP Group Add/Edit screen appears.</p> <p>To delete a VRRP group, click the Remove icon next to the group. The web configurator confirms that you want to delete the VRRP group before doing so.</p>

16.5 VRRP Group Add/Edit

The **VRRP Group Add/Edit** screen allows you to add VRRP groups to the ZyWALL or to edit the configuration of an existing VRRP group.

Note: You can only use interfaces that have static IP addresses. In addition, you should set the static IP address to the IP address of the virtual router.

Note: You can only enable one VRRP group for each interface.

Note: You can only have one active VRRP group for each virtual router (VR ID).

To access this screen, go to the **VRRP Group** summary screen (see [Section 16.4 on page 278](#)), and click either the **Add** icon or an **Edit** icon.

Figure 186 Network > Device HA > VRRP Group > Edit

The following table describes the labels in this screen.

Table 85 Network > Device HA > VRRP Group > Edit

LABEL	DESCRIPTION
Enable	Select this to make the specified interface part of the virtual router. Clear this to take the specified interface out of the virtual router.
Name	This field is read-only if you are editing the VRRP group. Type the name of the VRRP group. This field must be unique in the ZyWALL, but it is not used in the virtual router. The virtual router uses the VRID . The name can consist of alphanumeric characters, the underscore, and the dash and may be up to fifteen characters long.
VRID	Type the virtual router ID number.
Description	Type the description of the VRRP group. This field is only for your reference. It may be up to sixty printable ASCII characters long.
VRRP Interface	Select the interface in this device that is part of the virtual router. You can only select interfaces that have static IP addresses.
Role	Select the role that you want the interface plays in the virtual router. Choices are: Master - This interface is the master interface in the virtual router. The interface always uses its static IP address, not the management IP address of the VRRP group. Note: Do not set this field to Master for two or more routers in the same virtual router (same VR ID). Backup - This interface is a backup interface in the virtual router. The interface may use its static IP address or the management IP address of the VRRP group, depending on its current role. The current role depends on the other routers in the virtual router.

Table 85 Network > Device HA > VRRP Group > Edit (continued)

LABEL	DESCRIPTION
Priority	This field is available if the selected interface is a Backup interface. Type the priority of the backup interface. The backup interface with the highest value takes over the role of the master interface if the master interface becomes unavailable. The priority must be between 1 and 254. (The master interface has priority 255.)
Preempt	This field is available if the selected interface is a Backup interface. Select this if the selected interface should become the master interface if a lower-priority interface is the master when this one is enabled. (If the role is Master , the interface preempts by default.)
Manage IP	This field is available if the selected interface is a Backup interface. Enter the IP address of the interface while it is in Stand-By mode. It is recommended that this IP address be in the same subnet as the interface. If it is not in the same subnet, the backup router cannot synchronize with the master.
Manage IP Subnet Mask	This field is available if the selected interface is a Backup interface.
Authentication	<p>Select the authentication method used in the virtual router. Every interface in a virtual router must use the same authentication method and password. Choices are:</p> <p>None - this virtual router does not use any authentication method.</p> <p>Text - this virtual router uses a plain text password for authentication. Type the password in the field next to the radio button. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= ; ; ! @ \$ % # ~ ' \ () ,) , and it can be up to eight characters long.</p> <p>IP AH(MD5) - this virtual router uses an encrypted MD5 password for authentication. Type the password in the field next to the radio button. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= ; ; ! @ \$ % # ~ ' \ () ,) , and it can be up to eight characters long.</p> <p>See Section 13.1.2 on page 256 for more information about authentication methods.</p>

16.6 Synchronization Overview

In a virtual router, backup routers do not automatically get configuration updates from the master router. In this case, the master ZyWALL can send backup ZyWALLs these updates. This is called synchronization.

During synchronization, the master ZyWALL sends the following information to the backup ZyWALL.

- Startup configuration file (**startup-config.conf**)
- IDP signatures
- Certificates (My Certificates, and Trusted Certificates)

Synchronization does not change the VRRP groups or synchronization settings in the backup ZyWALL, however.

Note: The backup ZyWALL reboots during synchronization.

Backup ZyWALLs cannot get updates for services to which they have not subscribed. For example, if a backup ZyWALL has not subscribed to IDP, it does not get IDP updates from the master ZyWALL.

Synchronization affects the entire device configuration. You can only configure one set of settings for synchronization, regardless of how many VRRP groups you might configure. The ZyWALL uses Secure FTP (on a port number you can change) to synchronize, but it is still recommended that the backup ZyWALL synchronize with a master ZyWALL on a secure network.

Synchronization can be either done manually or scheduled regularly, and it is initiated by the backup ZyWALL. The following restrictions apply.

- The backup ZyWALL must have at least one active VRRP group.
- The backup ZyWALL cannot be the master in any active VRRP group. This refers to the actual role at the time of synchronization, not the **Role** setting in the VRRP group.

16.6.1 Synchronize Screen

Use this screen if you want the ZyWALL to get or to send updated IDP signatures, and configuration information in the virtual router.

Note: You can only set up synchronization with other ZyWALL 1050s running the same firmware version.

Note: The backup router reboots during synchronization.

To access this screen, click **Network > Device HA > Synchronize**.

Figure 187 Network > Device HA > Synchronize

For synchronization, every ZyWALL in a virtual router should usually have the same **Password**, **Synchronize From**, and **on port** values. In addition, the management IP address must be in the same subnet as the interface (in other words, the virtual router). The following table describes the labels in this screen.

Table 86 Network > Device HA > Synchronize

LABEL	DESCRIPTION
Password	Enter the password used to verify other ZyWALL routers during synchronization. This password is different than the one that is used for authentication in the VRRP group. Every ZyWALL in the virtual router must use the same password. If you leave this field blank, the password returns to its default setting "1234".
Synchronize From	Enter the IP address or fully-qualified domain name (FQDN) of the router from which to get updated configuration and IDP signatures. Usually, you should enter the IP address or FQDN of a virtual router on a secure network.
on port	Enter the Secure FTP port number used by the ZyWALL you specified in Synchronize From . Usually, every ZyWALL in the virtual router should use the same port number. Otherwise, if the master ZyWALL changes, you might have to change this port number.
Sync. Now	Click this button to get updated configuration IDP signatures from the specified ZyWALL router. Note: The backup router reboots during synchronization.
Auto Synchronize	Select this to get updated configuration and IDP signatures automatically from the specified ZyWALL according to the specified Interval . The first synchronization begins after the specified Interval ; the ZyWALL does not synchronize immediately.
Interval	This field is only available if Auto Synchronize is checked. Type the number of minutes to wait between synchronizations. This value must be a number between 1 and 1440 (one day).

CHAPTER 17

DDNS

This chapter describes how to configure dynamic DNS (DDNS) services for the ZyWALL. First, it provides an overview, and then it introduces the screens. [See the DDNS section](#) in the Configuration Overview chapter for related information on these screens.

17.1 DDNS Overview

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current IP address.

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

Before you can use Dynamic DNS services with the ZyWALL, you first need to set up a dynamic DNS account with www.dyndns.org. (This is the only DNS service provider the ZyWALL supports at the time of writing.) DynDNS offers several DNS services. Please see www.dyndns.org for more information about each of them. When registration is complete, DynDNS gives you a password or key.

Note: You must go to DynDNS's Web site to set up a user account and a domain name before you can use the Dynamic DNS service with the ZyWALL.

After this, you configure the ZyWALL. Once the ZyWALL is configured, it automatically sends updated IP addresses to DynDNS, which helps redirect traffic accordingly.

17.1.1 DYNDNS Wildcard

Enable this feature to have *.yourhost.dyndns.org (for example, www.yourhost.dyndns.org) routed to the same IP address as yourhost.dyndns.org.

17.1.2 High Availability (HA)

The DDNS server maps a domain name to the IP address of one of the ZyWALL's WAN ports. If that WAN port loses its connection, high availability allows the ZyWALL to substitute the HA port's IP address in the domain name mapping.

17.1.3 Mail Exchanger

DynDNS can route e-mail for your domain name to a specified mail server. The server is called a mail exchanger. For example, if there is e-mail for john-doe@yourhost.dyndns.org, DynDNS routes the e-mail to the IP address you specify for the mail exchanger.

DynDNS can also provide an additional service, in which it holds onto your e-mail if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. This service is called backup.

Please see www.dyndns.org for more information about mail exchangers and backup.

17.2 DDNS Screens

Each domain name requires information about the DynDNS services and DynDNS account, as well as how the ZyWALL updates the IP address.

The **DDNS Type** indicates which DynDNS service you are using. The ZyWALL supports three services: dynamic DNS, static DNS, and custom DNS. Please see www.dyndns.org for more information about each of these services.

The ZyWALL needs to know the **Username**, **Password**, and **Domain Name** for your DynDNS account. You can also use the **wildcard** check box to indicate whether or not the wildcard feature should be supported.

You must also specify an **IP Address Update Policy**. This policy controls how the ZyWALL determines the IP address that is mapped to your domain name in the DDNS server. There are three policies: **Interface**, **Auto**, and **Custom**.

- **Interface** - You specify which **WAN Interface** (WAN port's IP address) to use for the domain name, and you can also specify an alternative **HA Interface**, in case the WAN interface is not available.
- **Auto** - The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. You might consider this if there are one or more NAT routers between the ZyWALL and the DDNS server.

Note: The ZyWALL may not determine the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.



- **Custom** - If you have a static IP address, you can specify the **Custom IP** address to use for the domain name. The ZyWALL still sends the static IP address to the DDNS server.

17.3 DDNS Summary

The **DDNS** screen provides a summary of all DDNS domain names and their configuration. In addition, this screen allows you to add new domain names, edit the configuration for existing domain names, and delete domain names.

To access this screen, login to the web configurator. When the main screen appears, click **Network > DDNS**. The following screen appears, providing a summary of the existing domain names.

Figure 188 Network > DDNS

My Domain Names							
Profile Name	Domain Name	DDNS Type	Wildcard	IP Address Update Policy	WAN Interface	HA* Interface	
zyxel-homepage	zyxel-trial.com.tw	DynDNS	no	iface	ge2	ge3	 

(*): High Availability. Enable this option to bind with another WAN interface when the specified HA interface is not available.

The following table describes the labels in this screen. See [Section 17.4 on page 288](#) for more information as well.

Table 87 Network > DDNS

LABEL	DESCRIPTION
Profile Name	This field displays the descriptive profile name for this entry.
Domain Name	This field displays each domain name the ZyWALL can route.
DDNS Type	This field displays which DynDNS service you are using.
Wildcard	This field displays whether or not *.yourhost.dyndns.org (for example, www.yourhost.dyndns.org) is routed to the same IP address as yourhost.dyndns.org .
IP Address Update Policy	This field displays how the ZyWALL determines the IP address for the domain name. iface - The IP address comes from the specified WAN Interface and HA Interface . auto -The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. custom - The IP address is fixed. See Section 17.2 on page 286 for more information.
WAN Interface	This field applies when the IP Address Update Policy is iface . This field displays which interface is mapped to the domain name.

Table 87 Network > DDNS (continued)

LABEL	DESCRIPTION
HA Interface	This field applies when the IP Address Update Policy is iface . This field displays which alternative interface is mapped to the domain name if the WAN interface is not available. If you are not using HA, the field says none .
Add icon	This column provides icons to add, edit, and remove domain names. To add a domain name, click the Add icon at the top of the column. The DDNS Add/Edit screen appears. To edit a domain name, click the Edit icon next to the domain name. The DDNS Add/Edit screen appears. To delete a domain name, click on the Remove icon next to the ISP account. The web configurator confirms that you want to delete the account before doing so.

17.4 Dynamic DNS Add/Edit

The **DDNS Add/Edit** screen allows you to add a domain name to the ZyWALL or to edit the configuration of an existing domain name. To access this screen, click **Network > DDNS**, and click either the **Add** icon or an **Edit** icon.

Figure 189 Network > DDNS > Edit

The screenshot shows the 'DDNS Profile' configuration window. It contains the following fields and options:

- Profile Name: zyxel-homepage
- DDNS Type: DynDNS (dropdown menu)
- Username: zyxel-trial
- Password: masked with asterisks
- Domain name: zyxel-trial.com.tw
- wildcard
- IP Address Update Policy: Interface (dropdown menu)
- WAN Interface: ge2 (dropdown menu)
- HA Interface: ge3 (dropdown menu)
- Mail Exchanger: (Optional)
- Backup mail exchanger

At the bottom of the form are 'OK' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 88 Network > DDNS > Edit

LABEL	DESCRIPTION
Profile Name	Type a descriptive name for this DDNS entry in the ZyWALL. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
DDNS Type	Select the type of DynDNS service you are using. See http://www.dyndns.com for more information about each one.

Table 88 Network > DDNS > Edit (continued)

LABEL	DESCRIPTION
Username	Type the user name used when you registered your domain name. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed.
Password	Type the password provided by DynDNS. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed.
Domain name	Type the domain name you registered. You can use up to 255 characters.
Wildcard	Select this if *.yourhost.dyndns.org (for example, www.yourhost.dyndns.org) should be routed to the same IP address as yourhost.dyndns.org .
IP Address Update Policy	Select how the ZyWALL determines the IP address for the domain name. iface - The IP address comes from the specified WAN Interface and HA Interface . auto -The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the ZyWALL and the DDNS server. custom - The IP address is fixed. See Section 17.2 on page 286 for more information.
WAN Interface	This field is only available when the IP Address Update Policy is Interface . Select the interface to use for updating the IP address mapped to the domain name.
HA Interface	This field is only available when the IP Address Update Policy is Interface . Select the alternative WAN interface to map to the domain name when the WAN interface is not available. If you do not want to use HA, select none .
Custom IP	This field is only available when the IP Address Update Policy is Custom . Type the IP address to use for the domain name.
Mail Exchanger	Type the name of your mail server here, if DynDNS also routes e-mail to this domain name. This field should be left blank if DynDNS does not.
Backup Mail Exchanger	Select this check box if you are using DynDNS's backup service for e-mail. Please see www.dyndns.org for more information about this service.

CHAPTER 18

Route

This chapter shows you how to configure policies for IP routing and static routes on your ZyWALL. See the [Policy Routes section](#) in the Configuration Overview chapter for related information on these screens.

18.1 Policy Route

Traditionally, routing is based on the destination address only and the ZyWALL takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

18.1.1 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Bandwidth Shaping – Organizations can allocate bandwidth to traffic that matches the routing policy and prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The ZyWALL performs NAT by default for traffic going to or from the **ge1** interface. Routing policy's SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.

18.2 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

The actions that can be taken include:

- Routing the packet to a different gateway, outgoing interface, VPN tunnel, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

18.2.1 NAT and SNAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address in a packet in one network to a different IP address in another network. Use SNAT (Source NAT) to change the source IP address in one network to a different IP address in another network.

18.2.2 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 the port(s) and IP address to forward a service (coming in from the remote server) to a client computer. The problem is that port forwarding only forwards a service to a single IP address. In order to use the same service on a different computer, you have to manually replace the client computer's IP address with another client computer's IP address.

Port triggering allows the client computer to take turns using a service dynamically. Whenever a client computer's packets match the routing policy, it can use the pre-defined port triggering setting to connect to the remote server without manually configuring a port forwarding rule for each client computer.

Port triggering is used especially when the remote server responds using a different port from the port the client computer used to request a service. The ZyWALL records the IP address of a client computer that sends traffic to a remote server to request a service (incoming service). When the ZyWALL receives a new connection (trigger service) from the remote server, the ZyWALL forwards the traffic to the IP address of the client computer that sent the request.

Note: You need to create a firewall rule to allow an incoming service before using a port triggering rule.

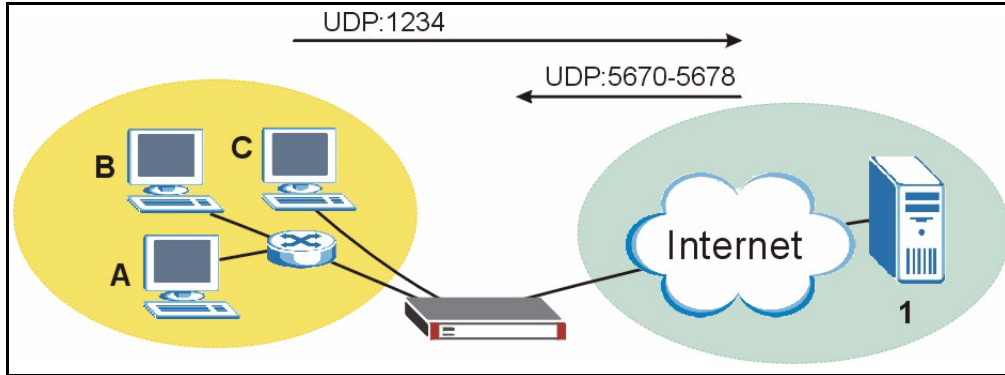
In the following example, you configure two services for port triggering:

Incoming service: Game (UDP: 1234)

Trigger service: Game-1 (UDP: 5670-5678)

- 1 Computer **A** wants to play a multiplayer online game and tries to connect to game server **1** using port 1234. The ZyWALL records the IP address of computer **A** when the packets match a policy with SNAT configured.
- 2 Game server **1** responds using a port number ranging between 5670 - 5678. The ZyWALL allows and forwards the traffic to computer **A**.
- 3 Computer **A** and game server **1** are connected to each other until the connection is closed or times out. Any other computers (such as **B** or **C**) cannot connect to remote server **1** using the same port triggering rule as computer **A** unless they are using a different next hop (gateway, outgoing interface, VPN tunnel or trunk) from computer **A** or until the connection is closed or times out.

Figure 190 Trigger Port Forwarding Example



18.3 IP Routing Policy Setup

Click **Configuration > Policy > Route** to open the **Policy Route** screen.

Figure 191 Policy Route







Policy Route										
#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM	
1	any	none	ge1	LAN_SUBNET	any	any	ge2	outgoing-interface	0	
2	any	none	ge1	LAN_SUBNET	any	any	ge2	outgoing-interface	0	
3	any	none	ge1	LAN_SUBNET	any	any	ge2	outgoing-interface	0	
4	any	none	ge1	LAN_SUBNET	any	any	ge2	outgoing-interface	0	
5	any	none	ge1	LAN_SUBNET	any	any	ge2	outgoing-interface	0	
6	any	none	ge2	WIZ_VPN_LOCAL	any	any	WIZ_VPN	none	0	
7	any	none	ge2	WIZ_VPN_LOCAL	any	any	WIZ_VPN	none	0	

The following table describes the labels in this screen.

Table 89 Policy Route

LABEL	DESCRIPTION
#	This is the number of an individual policy route.
User	This is the name of the user (group) object from which the packets are sent. any means all users.
Schedule	This is the name of the schedule object. none means the route is active at all times if enabled.
Incoming	This is the interface on which the packets are received.

Table 89 Policy Route (continued)

LABEL	DESCRIPTION
Source	This is the name of the source IP address (group) object. any means all IP addresses.
Destination	This is the name of the destination IP address (group) object. any means all IP addresses.
Service	This is the name of the service object. any means all services.
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, outgoing interface or trunk.
SNAT	This is the source IP address that the route uses. It displays none if the ZyWALL does not perform NAT for this route.
BWM	This is the maximum bandwidth allotted to the policy. 0 means there is no bandwidth limitation for this route.
	Click the Add icon in the heading row to add a new first entry.
	This displays whether the rule is enabled or not. Click the Active icon to activate or deactivate the policy.
	Click the Edit icon to go to the screen where you can edit the routing policy on the ZyWALL.
	Click the Add icon in an entry to add a rule below the current entry.
	Click the Remove icon to delete an existing routing policy from the ZyWALL. A window displays asking you to confirm that you want to delete the routing policy.
	In a numbered list, click the Move to N icon to display a field to type a number for where you want to put that rule and press [ENTER] 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.

18.4 Policy Route Edit

Click **Configuration > Policy > Route** to open the **Policy Route** screen. Then click the **Add** or **Edit** icon to open the **Policy Route Edit** screen.

Figure 192 Policy Route Edit

The following table describes the labels in this screen.

Table 90 Policy Route Edit

LABEL	DESCRIPTION
Configuration	
Enable	Select this to activate the policy.
Description	Enter a descriptive name of up to 31 printable ASCII characters for the policy.
Criteria	
User	Select a user name or user group from which the packets are sent.
Incoming Interface	Click Change... to select an interface or VPN tunnel through which the incoming packets are received.
Source Address	Select a source IP address object.
Destination Address	Select a destination IP address object.

Table 90 Policy Route Edit (continued)





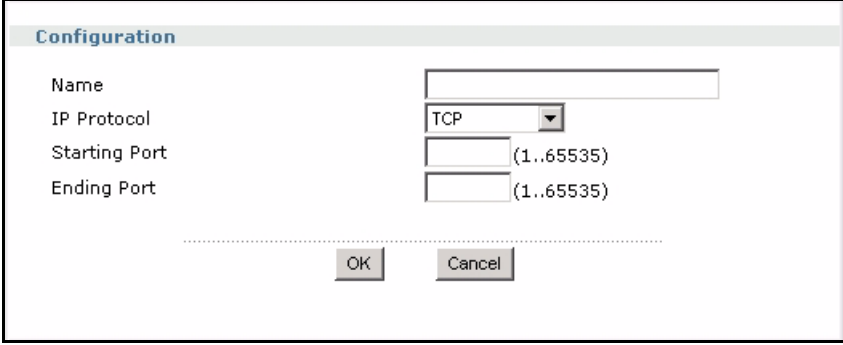
LABEL	DESCRIPTION
Schedule	Select a schedule.
Service	Select a service or service group from the drop-down list box.
New...	Click New... to add a new service. See Table 91 on page 298 for more information.
Next-Hop	
Type	<p>Select Auto to have the ZyWALL use the routing table to find a next-hop and forward the matched packets automatically.</p> <p>Select Gateway to route the matched packets to the next-hop router or switch you specified in the Gateway field. You have to set up the next-hop router or switch as a HOST address object first.</p> <p>Select VPN Tunnel to route the matched packets via the specified VPN tunnel.</p> <p>Select Trunk to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm.</p> <p>Select Interface to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).</p>
Gateway	Select Gateway in the Type field and a HOST address object in this field. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. The gateway must be a router or switch on the same segment as your ZyWALL's interface(s).
Interface	Select an interface to have the ZyWALL send traffic that matches the policy route through the specified interface.
VPN Tunnel	Select a VPN tunnel through which the packets are sent to the remote network that is connected to the ZyWALL directly.
Trunk	Select a trunk group to have the ZyWALL send the packets via the interfaces in the group.
Address Translation	
Source Network Address Translation	<p>Select none to not use NAT for the route.</p> <p>Select outgoing-interface to use the IP address of the outgoing interface as the source IP address of the packets that matches this route. If you select outgoing-interface, you can also configure port trigger settings for this interface.</p> <p>Otherwise, select a pre-defined address (group) to use as the source IP address(es) of the packets that match this route.</p>
Port Triggering	
#	This is the rule index number.
Incoming Service	<p>Select the service that the client computer sends to a remote server.</p> <p>The incoming service should have the same service or protocol type as what you configured in the Service field.</p>
Trigger Service	Select a service that a remote server sends. It causes (triggers) the ZyWALL to forward the traffic (received on the outgoing interface) to the client computer that requested the service.
	Click the Add icon in the heading row to add a new first entry.
	Click the Add icon in an entry to add a rule below the current entry.
	Click the Remove icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule.

Table 90 Policy Route Edit (continued)

LABEL	DESCRIPTION
	<p>In a numbered list, click the Move to N icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.</p> <p>The ordering of your rules is important as they are applied in order of their numbering.</p>
Bandwidth Shaping	This allows you to allocate bandwidth to a route and prioritize traffic that matches the routing policy.
Maximum Bandwidth	<p>Specify the maximum bandwidth (from 1 to 1048576) allowed for the route in kbps. If you enter 0 here, there is no bandwidth limitation for the route.</p> <p>If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.</p>
Bandwidth Priority	<p>Enter a number between 1 and 1024 to set the priority for traffic. The smaller the number, the higher the priority. If you set the maximum bandwidth to 0, the bandwidth priority will be changed to 0 after you click OK. That means the route has the highest priority and will get all the bandwidth it needs up to the maximum available.</p> <p>A route with higher priority is given bandwidth before a route with lower priority. If you set routes to have the same priority, then bandwidth is divided equally amongst those routes.</p>
OK	Click OK to save your changes back to the ZyWALL.
Cancel	Click Cancel to exit this screen without saving.

18.4.1 Adding a New Service

Click the **New...** button in the **Policy Route Edit** screen to display the screen. Use this screen to configure custom services for use in routing policies.

Figure 193 Policy Route Edit: Service


The screenshot shows a configuration window titled "Configuration" with the following fields and controls:

- Name:** A text input field.
- IP Protocol:** A dropdown menu currently set to "TCP".
- Starting Port:** A text input field with "(1..65535)" displayed to its right.
- Ending Port:** A text input field with "(1..65535)" displayed to its right.
- Buttons:** "OK" and "Cancel" buttons are located at the bottom center of the window.

The following table describes the labels in this screen.

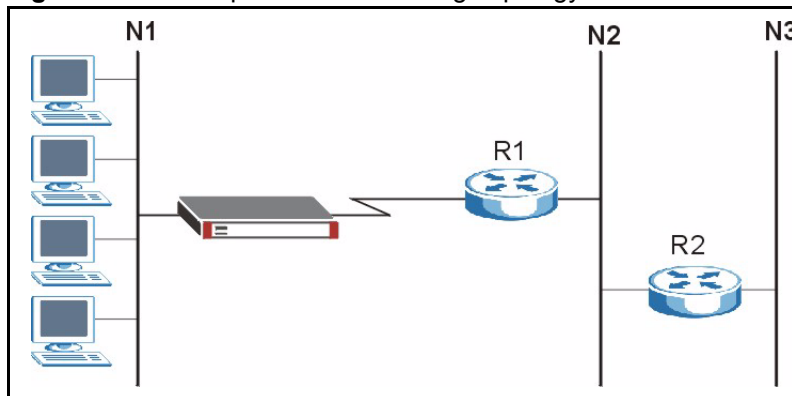
Table 91 Policy Route Edit: Service

LABEL	DESCRIPTION
Configuration	
Name	Enter a unique name for your customized service. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed
IP Protocol	Choose the IP protocol (TCP , UDP , ICMP or User Defined) that defines your customized service from the drop-down list box.
ICMP Type	This field is available only when you select ICMP in the IP Protocol field. The ICMP messages are identified by their types. Select the ICMP type from the drop-down list box.
Starting Port Ending Port	This field is grayed out when you select TCP or UDP in the IP Protocol field. Enter the port number (from 1 to 65535) that defines the service. To specify one port only, enter the port number in the Starting Port field and enter it again in the Ending Port field. To specify a span of ports, enter the first port in the Starting Port field and enter the last port in the Ending Port field.
IP Protocol Number	This field is available only when you select User Defined in the IP Protocol field. Enter the protocol number (from 1 to 255) that defines the customized service. For example, TCP=6 and UDP=17.
OK	Click OK to save your changes back to the ZyWALL.
Cancel	Click Cancel to exit this screen without saving.

18.5 IP Static Routes

The ZyWALL has no knowledge of the networks beyond the network that is directly connected to the ZyWALL. For instance, the ZyWALL knows about network **N2** in the following figure through gateway **R1**. 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 gateway **R1** (via gateway **R2**). Static routes are for you to tell the ZyWALL about the networks beyond the network connected to the ZyWALL directly.




Figure 194 Example of Static Routing Topology



18.6 Static Route Summary




Click **Configuration > Policy > Route > Static Route** to open the **Static Route** screen.

Figure 195 IP Static Route

#	Destination	Subnet Mask	Next-Hop	Metric	
1	1.2.3.4	255.255.255.0	172.23.1.2	0	  
2	10.10.10.1	255.255.255.0	ge1	0	  

The following table describes the labels in this screen.

Table 92 IP Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Destination	This is the destination IP address.
Subnet Mask	This is the IP subnet mask.
Next-Hop	This is the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or switch on the same segment as your ZyWALL's interface(s). The gateway helps forward packets to their destinations.
Metric	This is the route's priority among the ZyWALL's routes. The smaller the number, the higher priority the route has.
	Click the Add icon to go to the screen where you can set up a static route on the ZyWALL.
	Click the Edit icon to go to the screen where you can edit the static route on the ZyWALL.
	Click the Remove icon to delete an existing static route from the ZyWALL. A window displays asking you to confirm that you want to delete the routing policy.

18.7 Edit a Static Route

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 196 IP Static Route Edit

The screenshot shows a dialog box titled "Static Route Setting". It has five input fields on the left: "Destination IP", "Subnet Mask", "Gateway IP" (with a selected radio button), "Interface" (with an unselected radio button), and "Metric". The "Gateway IP" field is followed by a dropdown menu showing "ge1". The "Metric" field contains the number "0". At the bottom of the dialog are two buttons: "OK" and "Cancel".

The following table describes the labels in this screen.

Table 93 IP Static Route Edit

LABEL	DESCRIPTION
Destination IP	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.
Subnet Mask	Enter the IP subnet mask here.
Gateway IP	Select the radio button and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your ZyWALL's interface(s). The gateway helps forward packets to their destinations.
Interface	Select the radio button and a predefined interface through which the traffic is sent.
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.
OK	Click OK to save your changes back to the ZyWALL.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 19

Firewall

This chapter introduces the ZyWALL's firewall and shows you how to configure your ZyWALL's firewall. See the [Firewall section](#) in the Configuration Overview chapter for related information on these screens.

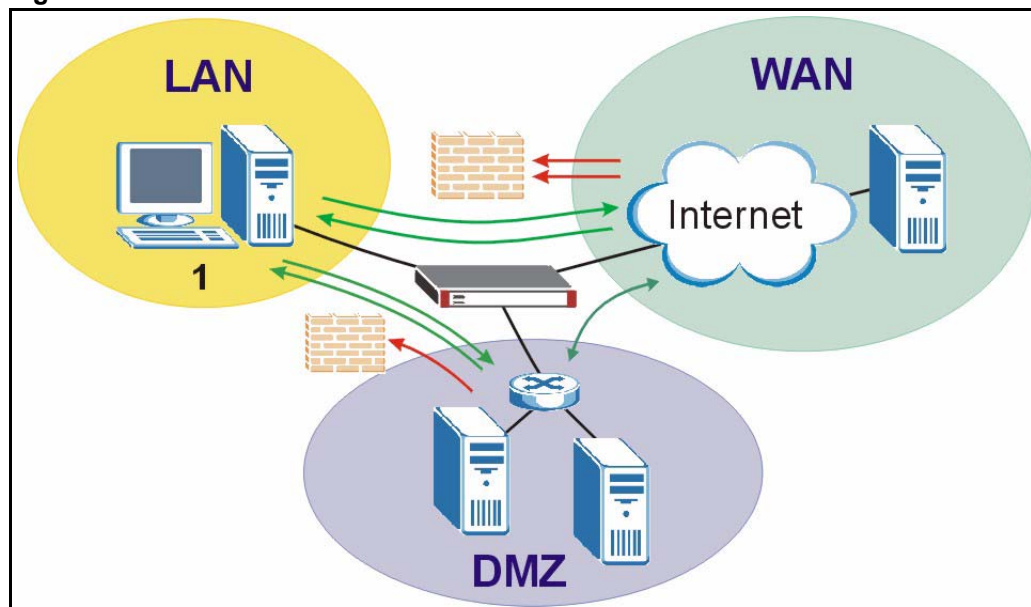
19.1 Firewall Overview

The ZyWALL's firewall is a stateful inspection firewall. The ZyWALL restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

A zone is a group of interfaces or VPN tunnels. Group the ZyWALL's interfaces into different zones based on your needs. You can configure firewall rules for data passing between zones or even between interfaces and/or VPN tunnels in a zone.

The following figure shows the ZyWALL's default firewall rules in action as well as demonstrates how stateful inspection works. User 1 can initiate a Telnet session from within the LAN zone and responses to this request are allowed. However, other Telnet traffic initiated from the WAN or DMZ zone and destined for the LAN zone is blocked. Communications between the WAN and the DMZ zones are allowed. The firewall allows VPN traffic between any of the networks.

Figure 197 Default Firewall Action



Your customized rules take precedence and override the ZyWALL's default settings. The ZyWALL checks the schedule, user name (user's login name on the ZyWALL), 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.

For example, if you want to allow a specific user from any computer to access one zone by logging in to the ZyWALL, you can set up a rule based on the user name only. If you also apply a schedule to the firewall rule, the user can only access the network at the scheduled time. A user-aware firewall rule is activated whenever the user logs in to the ZyWALL and will be disabled after the user logs out of the ZyWALL.

19.2 Firewall Rules

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

Note: The LAN, WAN and DMZ zones are default zones. Refer to the chapter about zone for more information.

Note: If you create a new zone, there is no default firewall rule for it and any packets sent to or from the new zone are allowed.

19.2.1 Through-ZyWALL Rules

The following table shows you the default firewall rules that inspect packets going through the ZyWALL.

Note: The ZyWALL checks the firewall rules before the application patrol rules for traffic going through the ZyWALL. If you want to use a service, make sure both the firewall and application patrol allow the service's packets to go through the ZyWALL.

You can use the firewall to block a service with a static port number. To block a service using a flexible/dynamic port number by inspecting the service's packets, you need to use application patrol. See the chapter about application patrol for more information.

Table 94 Default Through-ZyWALL Firewall Rules

FROM ZONE TO ZONE	STATEFUL PACKET INSPECTION
From LAN to LAN	Traffic between interfaces in the LAN is allowed.
From LAN to WAN	Traffic from the LAN to the WAN is allowed.
From LAN to DMZ	Traffic from the LAN to the DMZ is allowed.
From WAN to LAN	Traffic from the WAN to the LAN is dropped.
From WAN to WAN	Traffic between interfaces in the WAN is dropped.
From WAN to DMZ	Traffic from the WAN to the DMZ is allowed.

Table 94 Default Through-ZyWALL Firewall Rules

FROM ZONE TO ZONE	STATEFUL PACKET INSPECTION
From DMZ to LAN	Traffic from the DMZ to the LAN is dropped.
From DMZ to WAN	Traffic from the DMZ to the WAN is allowed.
From DMZ to DMZ	Traffic between interfaces in the DMZ is dropped.

Note: If you enable intra-zone traffic blocking (see the chapter about zones), the firewall automatically creates (implicit) rules to deny packet passage between the interfaces in the specified zone.

Note: You also need to configure virtual servers (NAT port forwarding) to allow computers on the WAN to access devices on the LAN. See [Chapter 24 on page 403](#) for more information.

19.2.1.1 Global Through-ZyWALL Rules

If an interface or VPN tunnel is not included in a zone, only the global through-ZyWALL firewall rules (with **from any to any** direction) apply to traffic going to and from that interface.

19.2.2 To-ZyWALL Rules

The to-ZyWALL rules are rules for traffic going to the ZyWALL itself. By default, the firewall allows any computer from the LAN zone to access or manage the ZyWALL. By default, the ZyWALL drops most packets from the WAN or DMZ zone to the ZyWALL itself, except for VRRP traffic for Device HA and ESP/AH/IKE/NATT services for VPN tunnels, and generates a log.

When you configure a to-ZyWALL rule for packets destined for the ZyWALL itself, make sure it does not conflict with your service control rule. See [Chapter 34 on page 489](#) for more information about service control (remote management).

Note: The ZyWALL checks the firewall rules before the service control rules for traffic destined for the ZyWALL.

Note: You can configure a to-ZyWALL firewall rule (with **from any to ZyWALL** direction) for traffic from an interface which is not in a zone.

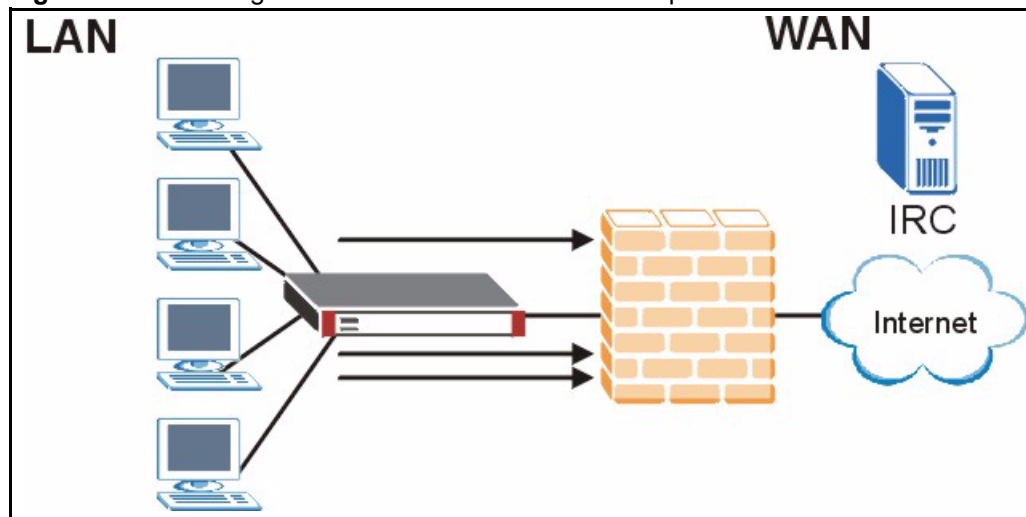
19.2.3 Firewall and VPN Traffic

After you create a VPN tunnel and apply it to a zone, you can set the firewall rules applied to VPN traffic. If you add a VPN tunnel to an existing zone (the LAN zone for example), you can configure a new LAN to LAN firewall rule or use intra-zone traffic blocking to allow or block VPN traffic transmitting between the VPN tunnel and other interfaces in the LAN zone. If you add the VPN tunnel to a new zone (the VPN zone for example), you can configure through-ZyWALL rules for VPN traffic between the VPN zone and other zones or to-ZyWALL rules for VPN traffic destined for the ZyWALL.

19.3 Firewall Rule Example Applications

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 198 Blocking All LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

Table 95 Blocking All LAN to WAN IRC Traffic Example

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	Any	IRC	Deny
Default	Any	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.

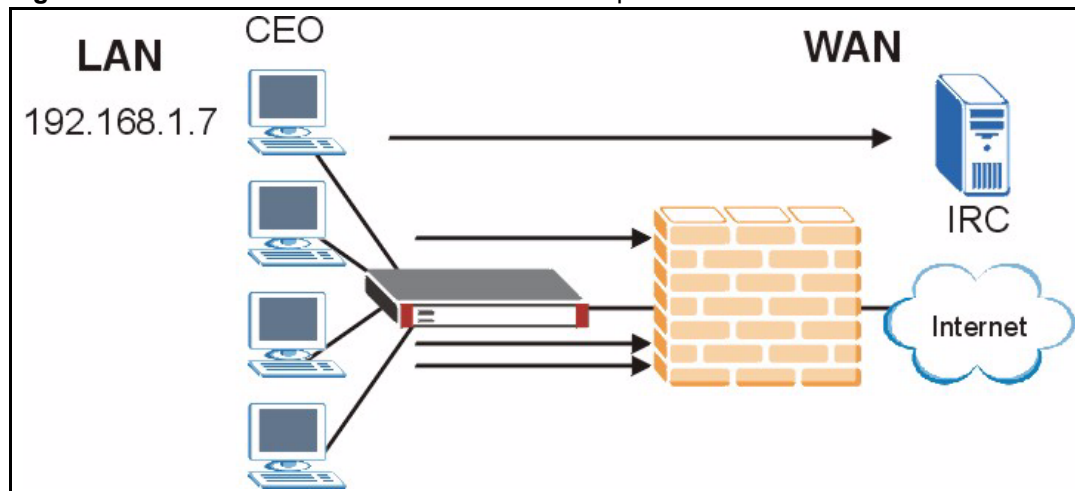
The ZyWALL applies the firewall rules in order. So for this example, when the ZyWALL receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that 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. You can also configure a LAN to WAN rule that allows IRC traffic from any computer through which the CEO logs into the ZyWALL with his/her user name. 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 10.1.4 on page 180](#) for information on 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 199 Limited LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

Table 96 Limited LAN to WAN IRC Traffic Example 1

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	192.168.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
Default	Any	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.

Alternatively, you configure a LAN to WAN rule with the CEO's user name (say CEO) to allow IRC traffic from any source IP address to go to any destination address.

Your firewall would have the following configuration.

Table 97 Limited LAN to WAN IRC Traffic Example 2

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	CEO	Any	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
Default	Any	Any	Any	Any	Any	Allow

- The first row allows any LAN computer to access the IRC service on the WAN by logging into the ZyWALL with the CEO's user name.
- 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.

19.4 Alerts

You can choose to generate an alert or log when a rule is matched and have the ZyWALL send an immediate e-mail message to you. Otherwise, see the logs created (for the categories you specified) in the **View Log** screen. Refer to the chapter on logs for details.

19.5 Asymmetrical Routes

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.

You can have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection).

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 virtual interfaces to put the ZyWALL and the backup gateway on separate subnets.

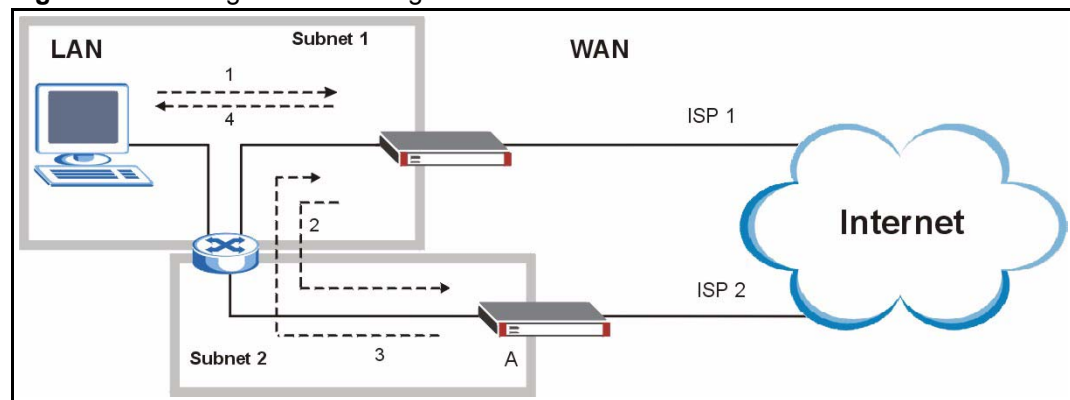
19.5.1 Virtual Interfaces and Asymmetrical Routes

You can use virtual interfaces instead of allowing asymmetrical routes. Virtual interfaces allow you to partition your network into logical sections over the same interface. See the chapter about interfaces for more information.

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 200 Triangle Route: Using Virtual Interfaces



19.6 Configuring the Firewall

Click **Configuration > Policy > Firewall** to open the **Firewall** screen. This screen varies depending on the firewall rule type and the way you choose to display the firewall rules.

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

19.6.1 Through-ZyWALL Rules with Zone Pairs

Select **Through-ZyWALL** rules to view or configure the firewall rules for packets passing through the ZyWALL.

Select **Zone Pairs** and specify from which zone packets come and to which zone packets travel to display only the rules specific to the selected direction.

Figure 201 Firewall: Zone Pairs



The following table describes the labels in this screen.

Table 98 Firewall: Zone Pairs

LABEL	DESCRIPTION
Global Setting	
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control 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>Note: 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 virtual interfaces to put the ZyWALL and the backup gateway on separate subnets. See Section 19.5 on page 306 for an example.</p>

Table 98 Firewall: Zone Pairs (continued)







LABEL	DESCRIPTION
Maximum session per host	<p>Use this field to set the highest number of sessions that the ZyWALL will permit a computer with the same IP address to have at one time.</p> <p>When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.</p> <p>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the ZyWALL.</p> <p>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using too many of the available NAT sessions.</p>
Firewall Rule	<p>Select Through-ZyWALL rules if you want to configure the firewall rules for traffic that goes through the ZyWALL. Select To-ZyWALL rules if you want to configure the firewall rules for traffic that is destined for the ZyWALL and allow or disallow a specific computer to manage the ZyWALL.</p> <p>If you select Through-ZyWALL rules, you can either</p> <ul style="list-style-type: none"> • Select Zone Pairs to display the through-firewall rules that are applied to traffic traveling between the selected zones or • Select All rules to display all through-firewall rules configured on the ZyWALL.
From Zone To Zone	<p>This is the direction of travel of packets. Select from which zone the packets come and to which zone the packets go.</p> <p>Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, From LAN to LAN means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN.</p>
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction.	
#	This is the index number of your firewall rule. It is not associated with a specific rule.
Priority	This is the position of your firewall rule in the global rule list (including all through-ZyWALL and to-ZyWALL rules). The ordering of your rules is important as rules are applied in sequence.
Schedule	This field tells you the schedule object that the rule uses.
User	This is the user name or user group name to which this firewall rule applies.
Source	This displays the source address object to which this firewall rule applies.
Destination	This displays the destination address object to which this firewall rule applies.
Service	This displays the service object to which this firewall rule applies.
Access	This field displays whether the firewall silently discards packets (deny), discards packets and sends a TCP reset packet to the sender (reject) or permits the passage of packets (allow).
Log	This field shows you whether a log (and alert) is created when packets match this rule or not.
	Click the Add icon in the heading row to add a new first entry.
	This displays whether the rule is enabled or not. Click the Active icon to activate or deactivate the rule.
	Click the Edit icon to go to the screen where you can edit the rule on the ZyWALL.

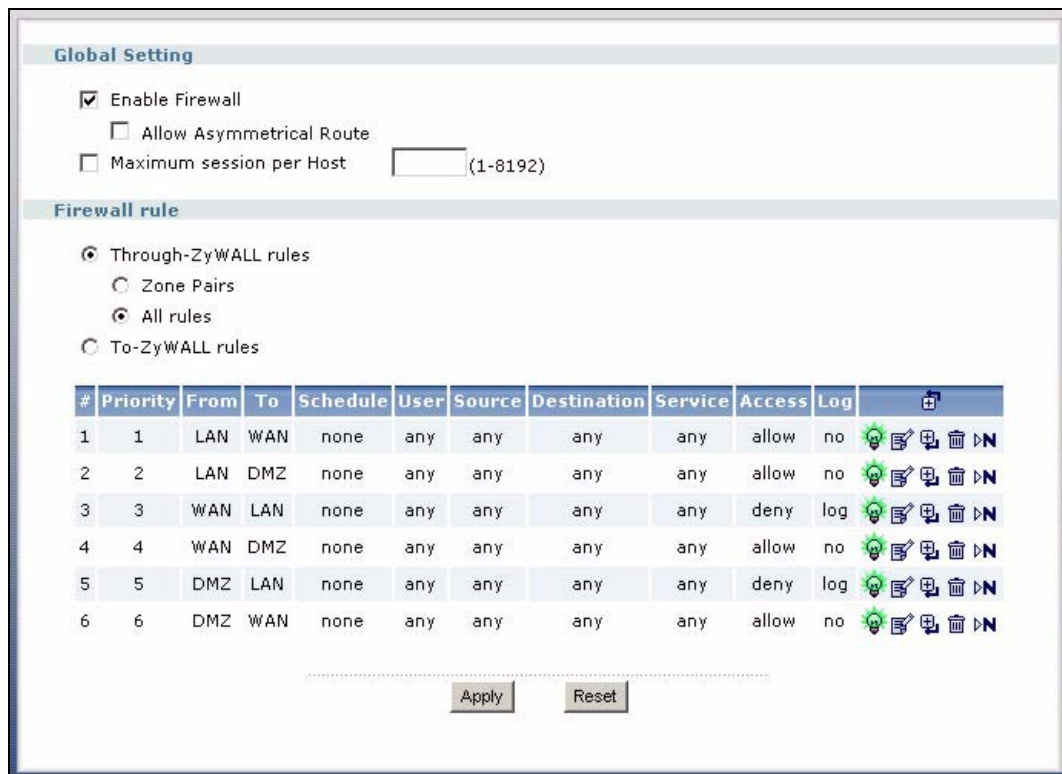
Table 98 Firewall: Zone Pairs (continued)

LABEL	DESCRIPTION
	Click the Add icon in an entry to add a rule below the current entry.
	Click the Remove icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule. Note that subsequent firewall rules move up by one when you take this action.
	In a numbered list, click the Move to N icon to display a field to type an index number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

19.6.2 Through Firewall Rules with All Rules

Select **All Rules** to display all through-firewall rules on the ZyWALL.

Figure 202 Firewall: All Rules









The following table describes the labels in this screen.

Table 99 Firewall: All Rules

LABEL	DESCRIPTION
Global Setting	
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control 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>Note: 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 virtual interfaces to put the ZyWALL and the backup gateway on separate subnets. See Section 19.5 on page 306 for an example.</p>
Maximum session per host	<p>Use this field to set the highest number of sessions that the ZyWALL will permit a computer with the same IP address to have at one time.</p> <p>When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.</p> <p>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the ZyWALL.</p> <p>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using too many of the available NAT sessions.</p>
Firewall Rule	<p>Select Through-ZyWALL rules if you want to configure the firewall rules for traffic that goes through the ZyWALL. Select To-ZyWALL rules if you want to configure the firewall rules for traffic that is destined for the ZyWALL and allow or disallow a specific computer to manage the ZyWALL.</p> <p>If you select Through-ZyWALL rules, you can either</p> <ul style="list-style-type: none"> • Select Zone Pairs to display the through-firewall rules that are applied to traffic traveling between the selected zones or • Select All rules to display all through-firewall rules configured on the ZyWALL.
#	This is the index number of your firewall rule. It is not associated with a specific rule.
Priority	This is the position of your firewall rule in the global rule list (including all through-ZyWALL and to-ZyWALL rules). The ordering of your rules is important as rules are applied in sequence.
From	This is the zone from which the packets come.
To	This is the zone to which the packets travel.
Schedule	This field tells you the schedule object that the rule uses.
User	This is the user name or user group name to which this firewall rule applies.
Source	This displays the source address object to which this firewall rule applies.

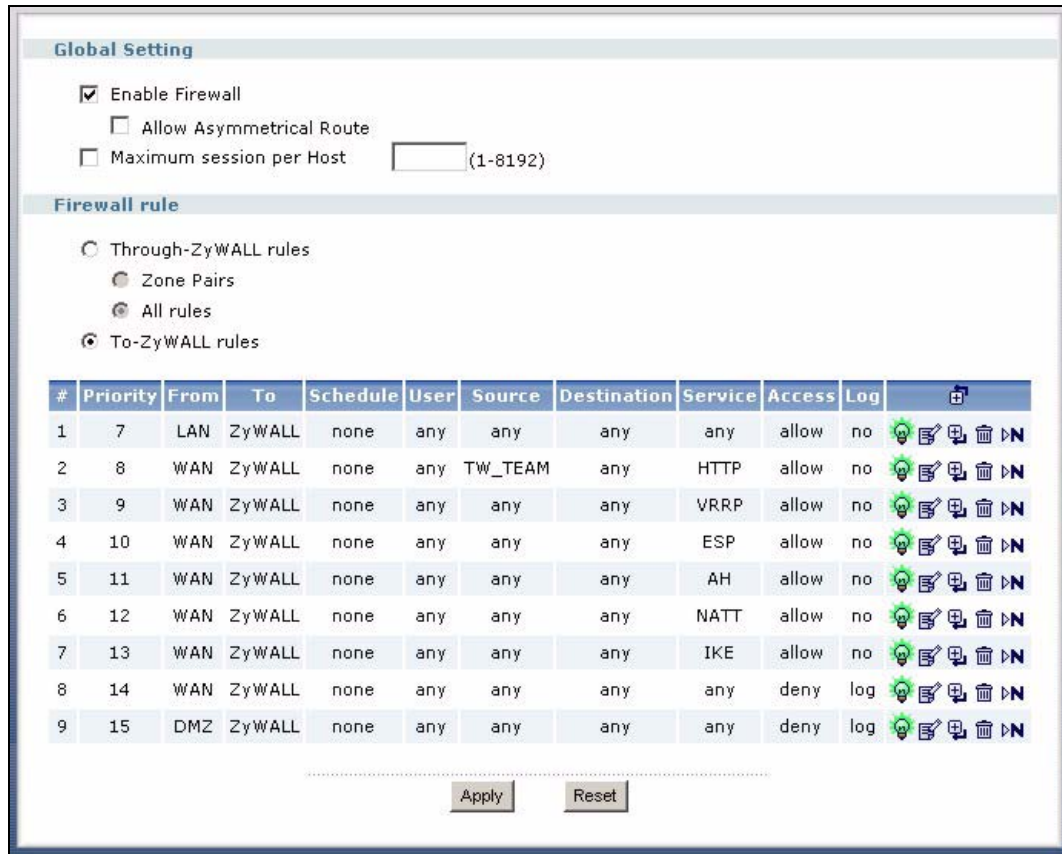
Table 99 Firewall: All Rules (continued)

LABEL	DESCRIPTION
Destination	This displays the destination address object to which this firewall rule applies.
Service	This displays the service object to which this firewall rule applies.
Access	This field displays whether the firewall silently discards packets (deny), discards packets and sends a TCP reset packet to the sender (reject) or permits the passage of packets (allow).
Log	This field shows you whether a log (and alert) is created when packets match this rule or not.
	Click the Add icon in the heading row to add a new first entry.
	This displays whether the rule is enabled or not. Click the Active icon to activate or deactivate the rule.
	Click the Edit icon to go to the screen where you can edit the rule on the ZyWALL.
	Click the Add icon in an entry to add a rule below the current entry.
	Click the Remove icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule. Note that subsequent firewall rules move up by one when you take this action.
	In a numbered list, click the Move to N icon to display a field to type an index number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

19.6.3 To-ZyWALL Rules

Select **To-ZyWALL rules** to view or configure the firewall rules for packets destined for the ZyWALL.

Figure 203 Firewall: To-ZyWALL Rules



The following table describes the labels in this screen.

Table 100 Firewall: To-ZyWALL Rules

LABEL	DESCRIPTION
Global Setting	
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control 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>Note: 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 virtual interfaces to put the ZyWALL and the backup gateway on separate subnets. See Section 19.5 on page 306 for an example.</p>

Table 100 Firewall: To-ZyWALL Rules (continued)







LABEL	DESCRIPTION
Maximum session per host	<p>Use this field to set the highest number of sessions that the ZyWALL will permit a computer with the same IP address to have at one time.</p> <p>When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.</p> <p>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the ZyWALL.</p> <p>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using too many of the available NAT sessions.</p>
Firewall Rule	<p>Select Through-ZyWALL rules if you want to configure the firewall rules for traffic that goes through the ZyWALL. Select To-ZyWALL rules if you want to configure the firewall rules for traffic that is destined for the ZyWALL and allow or disallow a specific computer to manage the ZyWALL.</p> <p>If you select Through-ZyWALL rules, you can either</p> <ul style="list-style-type: none"> • Select Zone Pairs to display the through-firewall rules that are applied to traffic traveling between the selected zones or • Select All rules to display all through-firewall rules configured on the ZyWALL.
#	This is the index number of your firewall rule. It is not associated with a specific rule.
Priority	This is the position of your firewall rule in the global rule list (including all through-ZyWALL and to-ZyWALL rules). The ordering of your rules is important as rules are applied in sequence.
From	This is the zone from which the packets come.
To	This is the zone to which the packets travel.
Schedule	This field tells you the schedule object that the rule uses.
User	This is the user name or user group name to which this firewall rule applies.
Source	This displays the source address object to which this firewall rule applies.
Destination	This displays the destination address object to which this firewall rule applies.
Service	This displays the service object to which this firewall rule applies.
Access	This field displays whether the firewall silently discards packets (deny), discards packets and sends a TCP reset packet to the sender (reject) or permits the passage of packets (allow).
Log	This field shows you whether a log (and alert) is created when packets match this rule or not.
	Click the Add icon in the heading row to add a new first entry.
	This displays whether the rule is enabled or not. Click the Active icon to activate or deactivate the rule.
	Click the Edit icon to go to the screen where you can edit the rule on the ZyWALL.
	Click the Add icon in an entry to add a rule below the current entry.

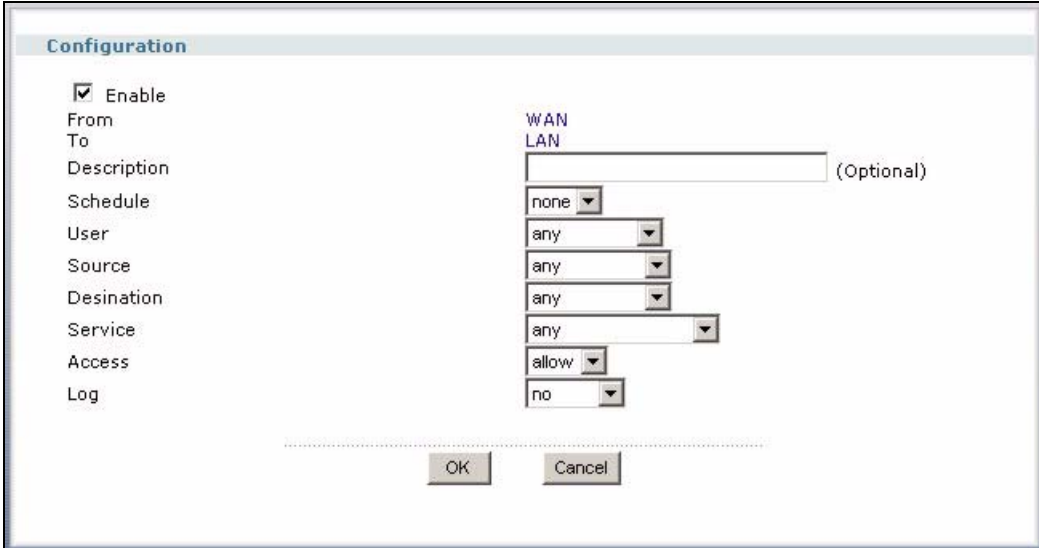
Table 100 Firewall: To-ZyWALL Rules (continued)

LABEL	DESCRIPTION
	Click the Remove icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule. Note that subsequent firewall rules move up by one when you take this action.
	In a numbered list, click the Move to N icon to display a field to type an index number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

19.6.4 Edit a Firewall Rule

In the **Firewall** screen, click the **Edit** or **Add** icon to display the **Firewall Rule Edit** screen and refer to the following table for information on the labels.

Note: For through-ZyWALL rules, select **Zone Pairs** and specify which zones packets come from and travel to in the previous screen; otherwise, you are creating a firewall rule that applies to packets traveling between any two networks.

Figure 204 Firewall Rule Edit


The screenshot shows the 'Firewall Rule Edit' configuration window. The window title is 'Configuration'. On the left side, there is a list of settings with their current values:

- Enable
- From: WAN
- To: LAN
- Description: (Optional)
- Schedule: none
- User: any
- Source: any
- Destination: any
- Service: any
- Access: allow
- Log: no

At the bottom of the window, there are two buttons: 'OK' and 'Cancel'.

The following table describes the labels in this screen.

Table 101 Firewall Rule Edit

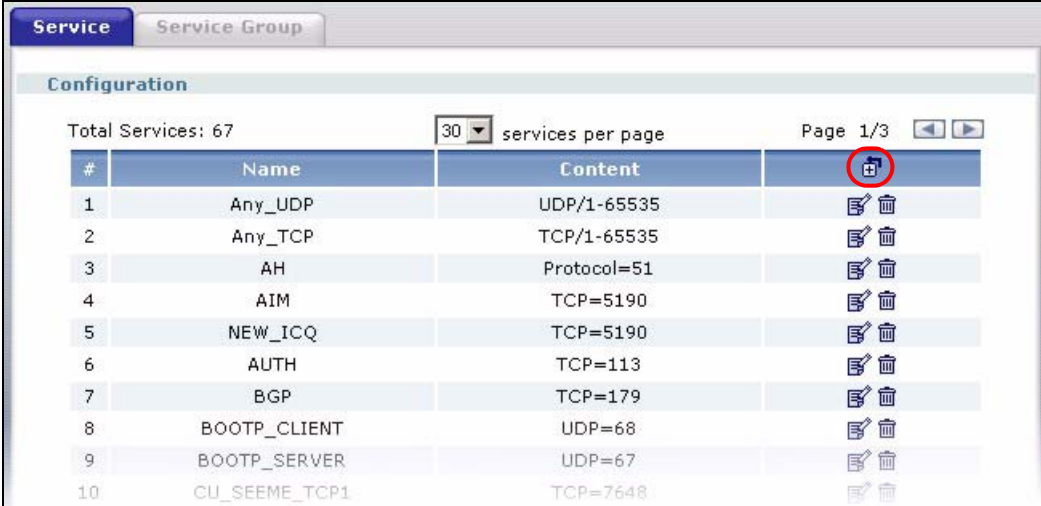
LABEL	DESCRIPTION
Enable	Select this check box to activate the firewall rule.
From To	<p>For through-ZyWALL rules, these are read-only and display the direction of travel of packets to which the rule applies.</p> <p>If you select Through-ZyWALL rules and All rules in the previous screen, these fields display any. That means the firewall rule applies to packets traveling between any two networks.</p> <p>For to-ZyWALL rules, select from which zone the packets are allowed or blocked. any means all interfaces or VPN tunnels.</p> <p>The To field is read-only and displays ZyWALL. It means the rules are only applied to the packets sent to the ZyWALL itself.</p>
Description	Enter a descriptive name of up to 60 printable ASCII characters for the firewall rule. Spaces are allowed.
Schedule	Select a schedule from the drop-down list box to have the rule active at the scheduled times. Otherwise, select none and the rule is always effective.
User	<p>This field is not available when you are configuring a to-ZyWALL rule.</p> <p>Select a user name or user group name from the drop-down list box. The firewall rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out.</p> <p>Otherwise, select any and there is no need for user logging.</p> <p>Note: If you specified a source IP address (group) instead of any in the field below, the user's IP address should be within the IP address range.</p>
Source	Select a source IP address (group) object.
Destination	Select a destination IP address (group) object.
Service	Select a service from the drop-down list box. Please see the chapter about the Object > Service screen for more information on services available.
Access	<p>Use the drop-down list box to select what the firewall is to do with packets that match this rule.</p> <p>Select deny to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select reject to deny the packets and send a TCP reset packet to the sender. Any UDP packets are dropped without sending a response packet.</p> <p>Select allow to permit the passage of the packets.</p>
Log	Select whether to have the ZyWALL generate a log (log), log and alert (log alert) or not (no) when the rule is matched.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.











19.7 Firewall Rule Configuration Example

The following Internet firewall rule example allows a hypothetical MyService from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 (Dest_1) on the LAN. You need to configure the service and address objects before you create a firewall rule.

- 1 In the **Object > Service** screen, click the **Add** icon () to open the **Service Edit** screen.

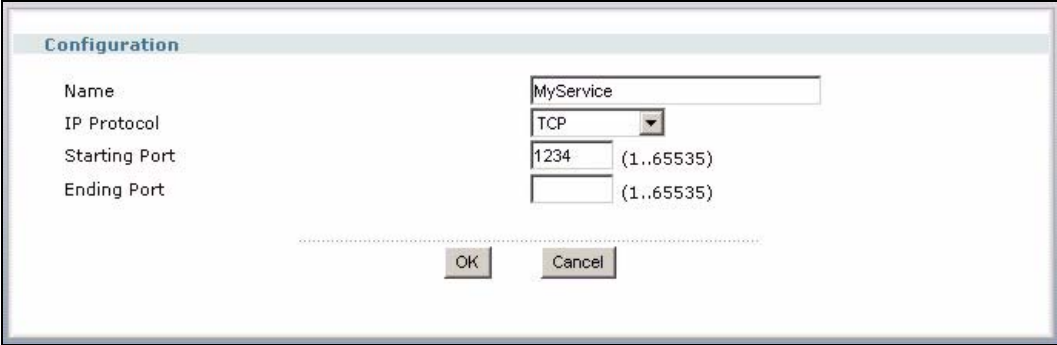
Figure 205 Firewall Example: Object > Service



#	Name	Content	
1	Any_UDP	UDP/1-65535	
2	Any_TCP	TCP/1-65535	
3	AH	Protocol=51	
4	AIM	TCP=5190	
5	NEW_ICQ	TCP=5190	
6	AUTH	TCP=113	
7	BGP	TCP=179	
8	BOOTP_CLIENT	UDP=68	
9	BOOTP_SERVER	UDP=67	
10	CU_SEEME_TCP1	TCP=7648	

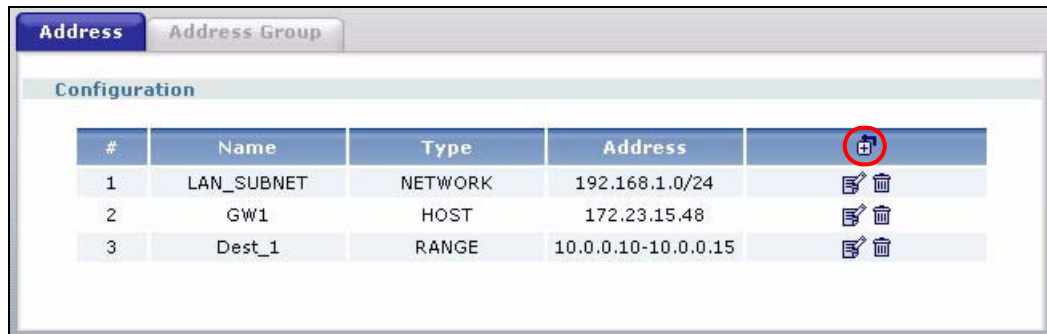
- 2 Configure it as follows and click **OK**.







Figure 206 Firewall Example: Create a Service Object



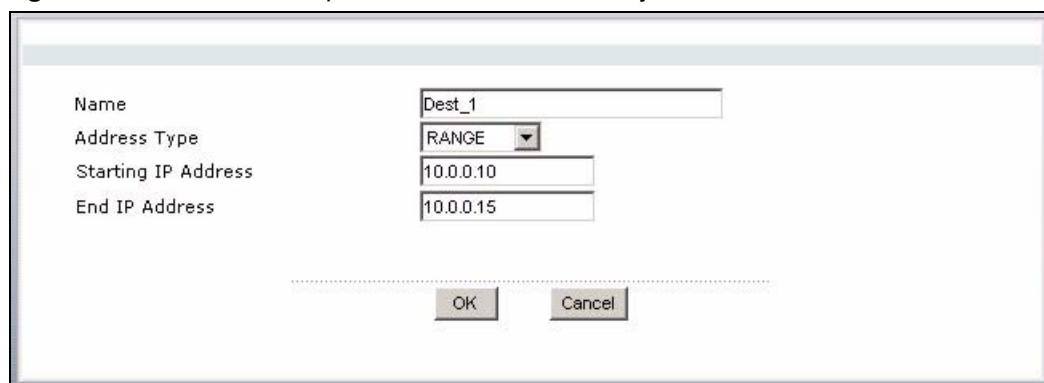
Name	MyService
IP Protocol	TCP
Starting Port	1234 (1..65535)
Ending Port	(1..65535)

- 3 Click **Object > Address** to display the **Address** screen. Click the **Add** icon () to open the **Address Edit** screen.

Figure 207 Firewall Example: Object > Address

#	Name	Type	Address	
1	LAN_SUBNET	NETWORK	192.168.1.0/24	 
2	GW1	HOST	172.23.15.48	 
3	Dest_1	RANGE	10.0.0.10-10.0.0.15	 

4 Configure it as follows and click **OK**.

Figure 208 Firewall Example: Create an Address Object

Name: Dest_1
Address Type: RANGE
Starting IP Address: 10.0.0.10
End IP Address: 10.0.0.15

OK Cancel

5 Click **Configuration > Policy > Firewall**. Select **Through-ZyWALL rules** and **Zone Pairs** and then the **From WAN to LAN** packet direction.


6 In the **Firewall** screen, click the **Add** icon () in the heading row to configure a new first entry or the **Add** icon () in an entry to add a rule below the selected entry.

Figure 209 Firewall Example: Select the Traveling Direction of Traffic

Global Setting

Enable Firewall

Allow Asymmetrical Route

Maximum session per Host (1-8192)

Firewall rule

Through-ZyWALL rules

Zone Pairs

All rules

To-ZyWALL rules

From Zone	To Zone
<input type="radio"/> LAN	<input checked="" type="radio"/> LAN
<input checked="" type="radio"/> WAN	<input type="radio"/> WAN
<input type="radio"/> DMZ	<input type="radio"/> DMZ

#	Priority	Schedule	User	Source	Destination	Service	Access	Log	
1	3	none	any	any	any	any	deny	log	

Apply Reset

7 Enter the name of the firewall rule.

8 Select **Any** in the **Source** drop-down list box, **Dest_1** in the **Destination** drop-down list box and **MyService** in the **Service** drop-down list box to configure it as follows. Click **OK** when you are done.

Figure 210 Firewall Example: Edit a Firewall Rule

Configuration

Enable

From: WAN

To: LAN

Description: Ex-1 (Optional)

Schedule: none

User: any

Source: any

Destination: Dest_1

Service: MyService

Access: allow

Log: no

OK Cancel

Figure 211 Firewall Example: MyService Example Rule Summary

Global Setting

Enable Firewall
 Maximum session per Host (1-8192)

Firewall rule

Through-ZyWALL rules
 Zone Pairs
 All rules
 To-ZyWALL rules

From Zone	To Zone
<input type="radio"/> LAN	<input checked="" type="radio"/> LAN
<input checked="" type="radio"/> WAN	<input type="radio"/> WAN
<input type="radio"/> DMZ	<input type="radio"/> DMZ
<input type="radio"/> Wanda	<input type="radio"/> Wanda

#	Priority	Schedule	User	Source	Destination	Service	Access	Log	
1	3	none	any	any	Dest_1	MyService	allow	no	
2	4	none	any	any	any	any	deny	log	

CHAPTER 20

Application Patrol

This chapter describes how to set up application patrol for the ZyWALL. First, it provides an overview, and, then, it introduces the screens. [See the Application Patrol section](#) in the Configuration Overview chapter for related information on these screens.

20.1 Application Patrol Overview

Application patrol provides a convenient way to manage instant messenger (IM) and peer-to-peer (P2P) application use on the network. It can also be used to manage a few general protocols (for example, http and ftp), as well as the streaming protocol rtsp.

Note: The ZyWALL checks firewall rules before it checks application patrol rules for traffic going through the ZyWALL.

If you want to use a service, make sure both the firewall and application patrol allow the service's packets to go through the ZyWALL.

Application patrol examines every TCP and UDP connection passing through the ZyWALL and identifies what application is using the connection. Then, you can specify, by application, whether or not the ZyWALL continues to route the connection.

20.1.1 Classification of Applications

There are two ways the ZyWALL can identify the application. The first approach is called port-less. In this approach, the ZyWALL looks at the IP payload (OSI level-7) and attempts to match it with known patterns for specific applications. Usually, this occurs at the beginning of a connection, when the payload is more consistent across connections, and the ZyWALL examines several packets to make sure the match is correct.

Note: The ZyWALL lets the first eight packets through the firewall, regardless of the routing policy for the application.

The second approach is called port-base. In this approach, the ZyWALL only uses OSI level-3 information, such as IP address and port, to identify what application is using the connection. This approach is available in case the ZyWALL identifies a lot of "false positives" for a particular application.

20.1.2 Default Action for Each Application

For each application, you specify the action the ZyWALL takes once it identifies one of its connections.

- **Forward** - the ZyWALL routes the packets for this application.
- **Drop** - the ZyWALL does not route the packets for this application, and it does not notify the client of this decision.
- **Reject** - the ZyWALL does not route the packets for this application, and it notifies the client of this decision.

20.1.3 Exceptions to the Default Action

You can also specify exceptions, when the ZyWALL should not follow the default rule for the application. There are two kinds of exceptions, one identified by the original destination port of the connection and one identified by schedule, user, source, and destination information. You can use the first kind to restrict applications to particular ports, and you can use the second kind to define other exceptions.

20.1.4 Bandwidth Management for Applications

If the ZyWALL is supposed to route packets for an application, you can also restrict the bandwidth used by each application. This restriction may be ineffective in certain cases, however, such as using MSN to send files via P2P.

20.1.5 Other Applications

Sometimes, the ZyWALL cannot identify the application. For example, the application might be a new application, or the packets might arrive out of sequence. (The ZyWALL does not reorder packets when identifying the application.) In these cases, you can still provide a default rule for the ZyWALL to follow. In addition, you can use destination port, schedule, user, source, and destination information to create a sequence of specific conditions, similar to the sequence of rules used by firewalls, to specify what the ZyWALL should do more precisely.

20.2 Application Patrol Screens

Use the **Configuration** summary screen to enable and disable application patrol, look at every application the ZyWALL can recognize, and review the settings for each one. It also lets you open the **Configuration Edit** screen, which enables and disables the rules for each application and allows you to specify the default policy and exceptions for each application.

The **Other Protocol** screen controls what the ZyWALL does when it does not recognize the application, and it identifies the conditions that refine this. It also lets you open the **Other Configuration Add/Edit** screen to create new conditions or edit existing ones.

20.3 Configuration Summary

You can use the **Configuration** summary screen to enable and disable application patrol. This screen also lists every application the ZyWALL can recognize, displays the settings for each one, and lets you open the **Configuration Edit** screen to change the settings.

To access this screen, login to the web configurator. When the main screen appears, click **Policy > App. Patrol**. The following screen appears.

Figure 212 Policy > Application Patrol > Configuration

Configuration
Other Protocol

General Setup

Enable Application Patrol

General Protocols

#	Service	Access	Classify	Exception	BWM / kbps	Log	Modify
1	ftp	forward	portless	drop	no	no	
2	smtp	forward	portless	drop	no	no	
3	pop3	forward	portless	drop	no	no	
4	irc	forward	portless	drop	no	no	
5	http	forward	portless	drop	no	no	

Instant Messenger

#	Service	Access	Classify	Exception	BWM / kbps	Log	Modify
1	msn	forward	portless	drop	no	no	
2	aol-icq	forward	portless	drop	no	no	
3	yahoo	forward	portless	drop	no	no	
4	qq	forward	portless	drop	no	no	

Peer to Peer

#	Service	Access	Classify	Exception	BWM / kbps	Log	Modify
1	bittorrent	forward	portless	drop	no	no	
2	eDonkey	forward	portless	drop	no	no	
3	fasttrack	forward	portless	drop	no	no	
4	gnutella	forward	portless	drop	no	no	
5	napster	forward	portless	drop	no	no	
6	h323	forward	portless	drop	no	no	
7	sip	forward	portless	drop	no	no	
8	soulseek	forward	portless	drop	no	no	

Streaming Protocols

#	Service	Access	Classify	Exception	BWM / kbps	Log	Modify
1	rtsp	forward	portless	drop	no	no	

Apply Reset

The following table describes the labels in this screen. See [Section 20.3.1](#) on page 325 for more information as well.

Table 102 Policy > Application Patrol > Configuration

LABEL	DESCRIPTION
Enable Application Patrol	Select this check box to turn on application patrol.
	The applications that the ZyWALL can recognize are divided into four categories: General Protocols , Instant Messenger , Peer to Peer , and Streaming Protocols .
#	This field is a sequential value, and it is not associated with a specific application.

Table 102 Policy > Application Patrol > Configuration (continued)

LABEL	DESCRIPTION
Service	This field displays the name of the application.
Access	This field displays what the ZyWALL does with packets for this application. Choices are: forward , drop , and reject .
Classify	This field displays how the ZyWALL identifies this application. Choices are: portless and portbase .
Exception	This field describes what the ZyWALL does with packets if there are exception policies for this application. If the ZyWALL normally forwards packets for this application, exceptions can either drop or reject them; if the ZyWALL normally drops or rejects packets for this application, exceptions can forward them.
BWM / kbps	This field displays the bandwidth limitation, if any, for this application.
Log	This field displays what kind of record the ZyWALL creates when it identifies this application. Choices are: no , log , and log alert .
Modify	<p>This column provides icons to activate and deactivate each application and to edit the settings for each one.</p> <p>To activate or deactivate patrol for an application, click the Active icon for the corresponding application.</p> <p>To edit the settings for an application, click the Edit icon next to the application. The Configuration Edit screen appears.</p>

20.3.1 Configuration Edit

The **Configuration Edit** screen allows you to edit the settings for each application. To access this screen, go to the **Configuration Summary** screen (see [Section 20.3 on page 323](#)), and click the appropriate **Edit** icon.

Figure 213 Policy > Application Patrol > Configuration > Edit

Service

Enable Service

Service Identification

Name: pop3

Classification: Port-less Port-base

Default Port: 110

Default Policy

Access: Reject

Log: no

Enable Bandwidth Shaping: 1 kbps

Exception Policy

Allow Port: [Empty]

Action: Forward

#	Schedule	User	Source	Destination	Log	
1	none	any	any	any	no	[Add] [Remove] [Next]

OK Cancel

The following table describes the labels in this screen.

Table 103 Policy > Application Patrol > Configuration > Edit

LABEL	DESCRIPTION
Service	
Enable Service	Select this check box to turn on patrol for this application.
Service Identification	
Name	This field displays the name of the application.
Classification	Specify how the ZyWALL should identify this application. Choices are: Port-less - the ZyWALL identifies this application by matching the IP payload with the application's pattern(s). Port-base - the ZyWALL identifies this application by looking at the destination port in the IP header.
Default Port	This field is available if the classification is Port-base . You can view and edit the ports used to identify this application.
Add icon	This field is available if the classification is Port-base . This column provides icons to add and remove port numbers used to identify the application. To add a port number, click the Add icon at the top of the column. Type the destination port number in the new Default Port record. To remove a port number, click the Remove icon next to the port number. The Web configurator confirms that you want to delete the port number before doing so.

Table 103 Policy > Application Patrol > Configuration > Edit (continued)

LABEL	DESCRIPTION
Default Policy	
Access	<p>This field controls what the ZyWALL does with packets for this application. Choices are:</p> <p>Forward - the ZyWALL routes the packets for this application.</p> <p>Drop - the ZyWALL does not route the packets for this application and does not notify the client of its decision.</p> <p>Reject - the ZyWALL does not route the packets for this application and notifies the client of its decision.</p>
Log	<p>This field controls what kind of record the ZyWALL creates when it identifies this application. Choices are:</p> <p>no - the ZyWALL does not record anything</p> <p>log - the ZyWALL creates a record in the log</p> <p>log alert - the ZyWALL creates an alert</p> <p>Please see Chapter 36 on page 525 for more information.</p>
Enable Bandwidth Shaping	<p>Select this check box to tell the ZyWALL to restrict the amount of bandwidth the application can use.</p>
kpbs	<p>This field is only effective when Enable Bandwidth Shaping is checked. Type how much bandwidth, in kilobits per second, this application can use.</p>
Exception Policy	<p>This section controls the conditions that are tested to decide whether or not an exception occurs. Exceptions can occur two ways: by destination port number (if the default policy is Drop or Reject) or by conditions defined by schedule, user, source, and destination. You also use this section to specify what the ZyWALL does when an exception occurs.</p>
Allow Port	<p>This field is available if the Access is Drop or Reject. You can view and edit the ports that create exceptions to the default policy.</p>
Add icon	<p>This field is available if the Access is Drop or Reject. This column provides icons to add and remove port numbers that create exceptions to the default policy.</p> <p>To add a port number, click the Add icon at the top of the column. Type the port number in the new Allow Port record.</p> <p>To remove a port number, click the Remove icon next to the port number. The Web configurator confirms that you want to delete the port number before doing so.</p>
Action	<p>This field controls what action the ZyWALL should take if an exception occurs. If the Access is Drop or Reject, this field displays Forward, the only possible action. If the Access is Forward, select whether you want to Drop or Reject the connection. These actions are the same actions used in the Access field.</p>
#	<p>This field is a sequential value, and it is not associated with a specific condition.</p> <p>Note: The ZyWALL checks conditions in the order they appear in the list. While this sequence does not affect the functionality, you might improve the performance of the ZyWALL by putting more common conditions at the top of the list.</p>
Schedule	<p>Select a schedule that defines when the condition applies. Select none if the condition is effective anytime.</p>
User	<p>Select a user or a group for whom this condition applies. Select any if the condition is effective for every user.</p>
Source	<p>Select a source address or address group for whom this condition applies. Select any if the condition is effective for every source.</p>

Table 103 Policy > Application Patrol > Configuration > Edit (continued)

LABEL	DESCRIPTION
Destination	Select a destination address or address group for whom this condition applies. Select any if the condition is effective for every destination.
Log	Select what kind of record the ZyWALL creates when the condition is satisfied. Choices are: no - the ZyWALL does not record anything log - the ZyWALL creates a record in the log log alert - the ZyWALL creates an alert Please see Chapter 36 on page 525 for more information.
Add icon	This column provides icons to add, move, and remove conditions for the exception. To add a condition, click the Add icon at the top of the column or next to each condition. A new condition appears in the appropriate place in the list. To remove a condition, click on the Remove icon next to the condition. The web configurator confirms that you want to delete the condition before doing so. To move a condition up or down in the list, click on the Move to N icon next to the condition, and type the line number (# field) where you want to move this condition. The # field is updated accordingly.

20.4 Other Protocol Screen

The **Other Protocol** screen controls the default policy for applications; in other words, you can control what the ZyWALL does when it does not recognize the application. This screen also allows you to add, edit, and remove conditions to this default policy.

To access this screen, login to the web configurator. When the main screen appears, click once on **Policy** to open the **Policy** tree, and then click once on **App. Patrol**. Click once on the **Other Protocol** tab. The following screen appears.

Figure 214 Policy > Application Patrol > Other Protocol

The screenshot shows the 'Other Protocol' configuration page. At the top, there are tabs for 'Configuration' and 'Other Protocol'. Below the tabs is a 'Default Rule' section with a table containing 'Default Rule' and 'Access' (set to 'Forward') and 'Log' (set to 'no'). Below this is an 'Other Configuration' section with a table with columns: #, Running Port, Schedule, User, Source, Destination, Protocol, Access, Log, and a plus icon. At the bottom are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen. See [Section 20.4.1 on page 330](#) for more information as well.

Table 104 Policy > Application Patrol > Other Protocol

LABEL	DESCRIPTION
Default Rule	
Access	This field controls what the ZyWALL does with packets when it does not recognize the application. Choices are: Forward - the ZyWALL routes the packets. Drop - the ZyWALL does not route the packets and does not notify the client of its decision. Reject - the ZyWALL does not route the packets and notifies the client of its decision.
Log	This field controls what kind of record the ZyWALL creates when it does not recognize the application. Choices are: no - the ZyWALL does not record anything log - the ZyWALL creates a record in the log log alert - the ZyWALL creates an alert Please see Chapter 36 on page 525 for more information.
Other Configuration	This section displays the conditions that are applied, in sequence, to decide what the appropriate action is when the ZyWALL does not recognize the application.
#	This field is a sequential value, and it is not associated with a specific condition.
Running Port	This field displays the destination port number that applies in this condition. If it is zero, every port number applies.
Schedule	This field displays the schedule that defines when the condition applies.
User	This field displays the user or a group for whom this condition applies.
Source	This field displays the source address or address group for whom this condition applies.
Destination	This field displays the destination address or address group for whom this condition applies.
Protocol	This field displays the protocol for which this condition applies.
Access	This field displays what the ZyWALL does with packets when this condition is satisfied. Choices are: Forward , Drop , and Reject .

Table 104 Policy > Application Patrol > Other Protocol (continued)

LABEL	DESCRIPTION
Log	This field displays what kind of record the ZyWALL creates when the condition is satisfied. Choices are: no , log , and log alert .
Add icon	This column provides icons to add, move, and remove conditions for the exception. To add a condition, click the Add icon at the top of the column or next to each condition. A new condition appears in the appropriate place in the list. To remove a condition, click on the Remove icon next to the condition. The web configurator confirms that you want to delete the condition before doing so. To move a condition up or down in the list, click on the Move to N icon next to the condition, and type the line number (# field) where you want to move this condition. The # field is updated accordingly.

20.4.1 Other Configuration Add/Edit

The **Other Configuration Add/Edit** screen allows you to create a new condition or edit an existing one. To access this screen, go to the **Other Protocol** screen (see [Section 20.4 on page 328](#)), and click either the **Add** icon or an **Edit** icon.

Figure 215 Policy > Application Patrol > Other Protocol > Edit

The following table describes the labels in this screen.

Table 105 Policy > Application Patrol > Other Protocol > Edit

LABEL	DESCRIPTION
Running Port	Type the destination port number that applies in this condition. Type zero, if this condition applies for every port number.
Schedule	Select a schedule that defines when the condition applies. Select none if the condition is effective anytime.
User	Select a user or a group for whom this condition applies. Select any if the condition is effective for every user.
Source	Select a source address or address group for whom this condition applies. Select any if the condition is effective for every source.
Destination	Select a destination address or address group for whom this condition applies. Select any if the condition is effective for every destination.

Table 105 Policy > Application Patrol > Other Protocol > Edit (continued)

LABEL	DESCRIPTION
Protocol	Select the protocol for which this condition applies. Choices are: TCP and UDP .
Access	This field controls what the ZyWALL does with packets when this condition is satisfied. Choices are: Forward - the ZyWALL routes the packets. Drop - the ZyWALL does not route the packets and does not notify the client of its decision. Reject - the ZyWALL does not route the packets and notifies the client of its decision.
Log	Select what kind of record the ZyWALL creates when the condition is satisfied. Choices are: no - the ZyWALL does not record anything log - the ZyWALL creates a record in the log log alert - the ZyWALL creates an alert Please see Chapter 36 on page 525 for more information.

CHAPTER 21

IDP

This chapter introduces IDP (Intrusion, Detection and Prevention), IDP profiles, binding an IDP profile to a zone, custom signatures and updating signatures. [See the IDP section](#) in the Configuration Overview chapter for related information on these screens.

21.1 Introduction to IDP

An IDP system can detect malicious or suspicious packets and respond instantaneously. It can detect:

- Pattern-based attacks
- Anomalies based on violations of protocol standards (RFCs – Requests for Comments)
- Abnormal flows such as port scans.

21.1.1 Host Intrusions

The goal of host-based intrusions is to infiltrate files on an individual computer or server in with the goal of accessing confidential information or destroying information on a computer.

You must install a host IDP directly on the system being protected. It works closely with the operating system, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them.

Disadvantages of host IDPs are that you have to install them on each device (that you want to protect) in your network and due to the necessarily tight integration with the host operating system, future operating system upgrades could cause problems.

21.1.2 Network Intrusions

Network-based intrusions have the goal of bringing down a network or networks by attacking computer(s), switch(es), router(s) or modem(s). If a LAN switch is compromised for example, then the whole LAN is compromised. Host-based intrusions may be used to cause network-based intrusions when the goal of the host virus is to propagate attacks on the network, or attack computer/server operating system vulnerabilities with the goal of bringing down the computer/server. Typical “network-based intrusions” are SQL slammer, Blaster, Nimda MyDoom etc.

21.1.3 IDP on the ZyWALL

IDP on the ZyWALL protects against network-based intrusions. See [Section 21.7.1 on page 339](#) for a list of attacks that the ZyWALL can protect against. You can also create your own custom IDP rules.

21.2 Protected Zones and Profiles

A zone is a combination of ZyWALL interfaces and VPN connections for security. See the zone chapter for details on zones and the interfaces chapter for details on interfaces.

An IDP profile is a set of IDP rules with configured activation, log and action settings. The ZyWALL comes with default profiles that you can bind to zones. For example, bind the default DMZ profile to the (default) DMZ zone.

You can also create your own IDP profiles from base profiles. See [Table 107 on page 337](#) for details on base profiles.

Note: You can only bind one profile to one zone.

IDP applies to outgoing traffic from an interface. To protect your LAN computers for example, first create a zone for LAN computers, assign interfaces to them and then bind an IDP profile to that zone.

21.3 Configuring IDP General

Click **Policy > IDP > General**. Use this screen to bind a profile to a zone.

Note: Traffic anomaly and protocol anomaly detection is free; you do not have to register for IDP service.

You must register in order to use packet inspection signatures. See the **Registration** screen.

Figure 216 Enable IDP Warning



Figure 217 IDP > General

Protected Zone	IDP Profile	Activation
LAN	LAN_IDP	
WAN	none	
DMZ	DMZ_IDP	

Registration Status: **Not Licensed**
Registration Type: **None**

The following table describes the screens in this screen.

Table 106 IDP > General

LABEL	DESCRIPTION
General Setup	
Enable IDP	Select this check box to enable IDP on the ZyWALL. You can enable IDP if IDP service is not registered but only traffic anomaly and protocol anomaly detection applies; packet inspection does not. You must register for IDP service in order to use packet inspection signatures. If you don't have a standard license, you can register for a once-off trial one.
Bindings	
Protected Zone	This field shows the zones on the ZyWALL.
IDP Profile	An IDP profile is a set of IDP rules with configured activation, log and action settings. This field shows which IDP profile is bound to which zone. It displays none if a profile is not bound to a zone. To bind a different profile to a zone, click the icon next to the profile name to display a pop-up dialog box. You create IDP profiles in the Policy > IDP > Profile screen.
Activation	Click the Active icon to enable or disable IDP on a zone.
Registration Status	You need to create an account at myZyXEL.com, register your ZyWALL and then subscribe for IDP in order to be able to download new packet inspection signatures from myZyXEL.com. There's an initial free trial period for IDP after which you must pay to subscribe to the service. See the Registration chapter for details.
Registration Status	Licensed, Not Licensed or Expired indicates whether you have subscribed for IDP services or not or your registration has expired.
Registration Type	This field shows Trial, Standard or None depending on whether you subscribed to the IDP trial, bought an iCard for IDP service or neither.

21.4 Introducing IDP Profiles

An IDP profile is a set of packet inspection signatures, traffic anomaly rules and protocol anomaly rules.

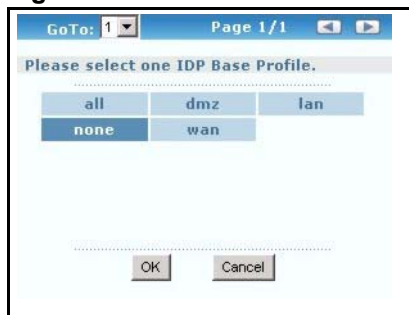
- Packet inspection signatures examine packet content for malicious data. Packet inspection applies to OSI (Open System Interconnection) layer-4 to layer-7 contents. You need to subscribe for IDP service in order to be able to download new signatures.
- Traffic anomaly rules look for abnormal behavior or events such as port scanning, sweeping or network flooding. It operates at OSI layer-2 and layer-3. Traffic anomaly rules may be updated when you upload new firmware.
- Protocol anomaly rules check for protocol compliance against the relevant RFC (Request For Comments). Protocol anomaly detection includes HTTP Inspection, TCP Decoder, UDP Decoder and ICMP Decoder. Protocol anomaly rules may be updated when you upload new firmware.

Anomaly detection is in general effective against abnormal behaviour while packet inspection signatures are created for known attacks.

21.4.1 Base Profiles

The ZyWALL comes with several base profiles. You use base profiles to create new profiles.

Figure 218 Base Profiles



These are the default base profiles at the time of writing.

Table 107 Base Profiles

BASE PROFILE	DESCRIPTION
dmz	This profile is most suitable for networks containing your servers. Signatures for common services such as DNS, FTP, HTTP, ICMP, IMAP, MISC, NETBIOS, POP3, RPC, RSERVICE, SMTP, SNMP, SQL, TELNET, Oracle, MySQL are enabled. Signatures with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Signatures with a low or medium severity level (two or three) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low severity level (one) are disabled.
wan	Signatures for all services are enabled. Signatures with a medium, high or severe severity level (greater than two) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low or low severity level (less than or equal to two) are disabled.
lan	This profile is most suitable for common LAN network services. Signatures for common services such as DNS, FTP, HTTP, ICMP, IM, IMAP, MISC, NETBIOS, P2P, POP3, RPC, RSERVICE, SMTP, SNMP, SQL, TELNET, TFTP, MySQL are enabled. Signatures with a high or severe severity level (greater than three) generate logs (not log alerts) and cause packets that trigger them to be dropped. Signatures with a low or medium severity level (two or three) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low severity level (one) are disabled.
all	All signatures are enabled. Signatures with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Signatures with a very low, low or medium severity level (less than or equal to three) generate logs (not log alerts) and no action is taken on packets that trigger them.
none	All signatures are disabled. No logs are generated nor actions are taken.

21.5 Profile Summary Screen

Select **Policy > IDP > Profile**. Use this screen to:

- Add a new profile
- Edit an existing profile
- Delete an existing profile

Figure 219 Policy > IDP > Profile



The following table describes the fields in this screen.

Table 108 Policy > IDP > Profile

LABEL	DESCRIPTION
Name	This is the name of the profile you created.
Base Profile	This is the base profile from which the profile was created.
(Icons)	Click the 'add' icon in the column header to create a new profile. A pop-up screen displays requiring you to choose a base profile from which to create the new profile. Click an edit icon to edit an existing profile. Click a remove icon to delete an existing profile.

21.6 Creating New Profiles

You may want to create a new profile if not all signatures in a base profile are applicable to your network. In this case you should disable non-applicable signatures so as to improve ZyWALL IDP processing efficiency.

You may also find that certain signatures or rules are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the ZyWALL. As each network is different, false positives and false negatives are common on initial IDP deployment.

You could create a new 'monitor profile' that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'inline profile' whereby you configure appropriate actions to be taken when a packet matches a signature or rule.

21.6.1 Procedure To Create a New Profile

To create a new profile:

- 1 Click the 'add' icon in the **Policy > IDP > Profile** screen to display a pop-up screen allowing you to choose a base profile.
- 2 Select a base profile (see [Table 107 on page 337](#)) and then click **OK** to go to the profile details screen.
- 3 Type a new profile name

- 4 Enable or disable individual signature and or rules
- 5 Edit the default log options and actions.

21.7 Profiles: Packet Inspection

Select **Policy > IDP > Profile** and then add a new or edit an existing profile select. Packet inspection (group view) is the first screen in the profile.

Packet inspection signatures examine the contents of a packet for malicious data. It operates at layer-4 to layer-7.

21.7.1 Policy Types

This section describes IDP policy types, also known as attack types, as categorized in the ZyWALL. You may refer to these types when categorizing your own custom rules.

Table 109 Policy Types

POLICY TYPE	DESCRIPTION
P2P	Peer-to-peer (P2P) is where computing devices link directly to each other and can directly initiate communication with each other; they do not need an intermediary. A device can be both the client and the server. In the ZyWALL, P2P refers to peer-to-peer applications such as e-Mule, e-Donkey, BitTorrent, iMesh, etc.
IM	IM (Instant Messaging) refers to chat applications. Chat is real-time, text-based communication between two or more users via networks-connected computers. After you enter a chat (or chat room), any room member can type a message that will appear on the monitors of all the other participants.
SPAM	Spam is unsolicited "junk" e-mail sent to large numbers of people to promote products or services.
DoS/DDoS	The goal of Denial of Service (DoS) attacks is not to steal information, but to disable a device or network on the Internet. A distributed denial-of-service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
Scan	A scan describes the action of searching a network for an exposed service. An attack may then occur once a vulnerability has been found. Scans occur on several network levels. A network scan occurs at layer-3. For example, an attacker looks for network devices such as a router or server running in an IP network. A scan on a protocol is commonly referred to as a layer-4 scan. For example, once an attacker has found a live end system, he looks for open ports. A scan on a service is commonly referred to a layer-7 scan. For example, once an attacker has found an open port, say port 80 on a server, he determines that it is a HTTP service run by some web server application. He then uses a web vulnerability scanner (for example, Nikto) to look for documented vulnerabilities.

Table 109 Policy Types (continued)

POLICY TYPE	DESCRIPTION
Buffer Overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The excess information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Intruders could run codes in the overflow buffer region to obtain control of the system, install a backdoor or use the victim to launch attacks on other devices.
Virus/Worm	A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a program that is designed to copy itself from one computer to another on a network. A worm's uncontrolled replication consumes system resources, thus slowing or stopping other tasks.
Backdoor/Trojan	A backdoor (also called a trapdoor) is hidden software or a hardware mechanism that can be triggered to gain access to a program, online service or an entire computer system. A Trojan horse is a harmful program that is hidden inside apparently harmless programs or data. Although a virus, a worm and a Trojan are different types of attacks, they can be blended into one attack. For example, W32/Blaster and W32/Sasser are blended attacks that feature a combination of a worm and a Trojan.
Access Control	Access control refers to procedures and controls that limit or detect access. Access control attacks try to bypass validation checks in order to access network resources such as servers, directories, and files.
Web Attack	Web attacks refer to attacks on web servers such as IIS (Internet Information Services).

21.7.2 IDP Service Groups

An IDP service group is a set of related packet inspection signatures.

Table 110 IDP Service Groups

WEB_PHP	WEB_MISC	WEB_IIS	WEB_FRONTPAGE
WEB_CGI	WEB_ATTACKS	TFTP	TELNET
SQL	SNMP	SMTP	RSERVICES
RPC	POP3	POP2	P2P
ORACLE	NNTP	NETBIOS	MYSQL
MISC_EXPLOIT	MISC_DDOS	MISC_BACKDOOR	MISC
IMAP	IM	ICMP	FTP
FINGER	DNS		

The following figure shows the WEB_PHP service group that contains signatures related to attacks on web servers using PHP exploits. PHP (PHP: Hypertext Preprocessor) is a server-side HTML embedded scripting language that allows web developers to build dynamic websites.

Logs and actions applied to a service group apply to all signatures within that group. If you select **original setting** for service group logs and/or actions, all signatures within that group are returned to their last-saved settings.

Figure 220 IDP Service Groups

The screenshot shows the configuration interface for IDP Service Groups. The 'Profile' tab is selected, and the 'Packet Inspection' sub-tab is active. The 'Name' field contains 'LAN_IDP'. The 'Signature Group' section shows a table with columns for Service, Activation, Log, and Action. The 'WEB_PHP' service group is highlighted, and its 'Log' and 'Action' dropdowns are set to 'original setting'.

Service	Activation	Log	Action
WEB_PHP		original setting	original setting
WEB-PHP admin.php access		log	none
WEB-PHP admin.php file upload attempt		log alert	drop
WEB-PHP Advanced Poll admin_comment.php access		log	none
WEB-PHP Advanced Poll admin_edit.php access		log	none
WEB-PHP Advanced Poll admin_embed.php access		log	none
WEB-PHP Advanced Poll admin_help.php access		log	none
WEB-PHP Advanced Poll admin_license.php access		log	none

21.7.3 Profile > Packet Inspection > Group View Screen


Figure 221 Policy > IDP > Profile > Packet Inspection_Group View

General **Profile** Custom Signatures Update

Packet Inspection Traffic Anomaly Protocol Anomaly

Name: LAN_IDP Switch to query view

Signature Group

Service ▲	Activation	Log	Action			
⊕ WEB_PHP		original setting ▼	original setting ▼			
⊕ WEB_MISC		original setting ▼	original setting ▼			
⊕ WEB_IIS		original setting ▼	original setting ▼			
⊕ WEB_FRONTPAGE		original setting ▼	original setting ▼			
⊕ WEB_CGI		original setting ▼	original setting ▼			
⊕ WEB_ATTACKS		original setting ▼	original setting ▼			
⊕ TFTP		original setting ▼	original setting ▼			
⊕ TELNET		original setting ▼	original setting ▼			
⊕ SQL		original setting ▼	original setting ▼			
⊕ SNMP		original setting ▼	original setting ▼			
⊕ SMTP		original setting ▼	original setting ▼			
⊕ RPC		original setting ▼	original setting ▼			
⊕ POP3		original setting ▼	original setting ▼			
⊕ POP2		no ▼	none ▼			
⊕ P2P		original setting ▼	original setting ▼			
⊕ ORACLE		no ▼	none ▼			
⊕ NNTP		no ▼	none ▼			
⊕ NETBIOS		original setting ▼	original setting ▼			
⊕ MYSQL		original setting ▼	original setting ▼			
⊕ MISC_EXPLOIT		original setting ▼	original setting ▼			
⊕ MISC_DDOS		original setting ▼	original setting ▼			
⊕ MISC_BACKDOOR		original setting ▼	original setting ▼			
⊕ MISC		original setting ▼	original setting ▼			
⊕ IMAP		original setting ▼	original setting ▼			
⊖ IM		original setting ▼	original setting ▼			
Message ▲	SID	Severity	Policy Type	Activation	Log	Action
CHAT AIM receive message	8000659	low	IM		log ▼	none ▼
CHAT ICQ access	8004032	verylow	IM		no ▼	none ▼
CHAT ICQ forced user addition	8000857	medium	IM		log ▼	none ▼
CHAT MSN login attempt	8001036	low	IM		log ▼	none ▼
CHAT MSN message	8004031	verylow	IM		no ▼	none ▼
CHAT MSN outbound file transfer rejected	8001033	high	IM		log alert ▼	drop ▼
CHAT MSN outbound file transfer request	8001030	low	IM		log ▼	none ▼
CHAT MSN user search	8001035	low	IM		log ▼	none ▼
⊕ ICMP					original setting ▼	none ▼
⊕ FTP					original setting ▼	original setting ▼
⊕ FINGER					no ▼	none ▼
⊕ DNS					original setting ▼	original setting ▼

OK Cancel Save

The following table describes the fields in this screen.

Table 111 Policy > IDP > Profile > Packet Inspection_Group View

LABEL	DESCRIPTION
Name	<p>This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names:</p> <p>MyProfile mYProfile Mymy12_3-4</p> <p>These are invalid profile names:</p> <p>1mYProfile My Profile MyProfile? Whatalongprofilename123456789012</p>
Switch to query view	<p>Click this button to go to a screen where you can search for signatures by criteria such as name, ID, severity, attack type, vulnerable attack platforms, service category, log options or actions.</p>
Service	<p>Click the + sign next to a service group to expand it. A service group is a group of related IDP signatures.</p>
Message	<p>This is the name of the signature.</p>
SID	<p>This is the signature ID (identification) number that uniquely identifies a ZyWALL signature.</p>
Severity	<p>These are the severities as defined in the ZyWALL. The number in brackets is the number you use if using commands.</p> <p>Severe (5): These denote attacks that try to run arbitrary code or gain system privileges.</p> <p>High (4): These denote known serious vulnerabilities or attacks that are probably not false alarms.</p> <p>Medium (3): These denote medium threats, access control attacks or attacks that could be false alarms.</p> <p>Low (2): These denote mild threats or attacks that could be false alarms.</p> <p>Very Low (1): These denote possible attacks caused by traffic such as Ping, trace route, ICMP queries etc.</p>
Policy Type	<p>This is the attack type as defined on the ZyWALL. See Table 109 on page 339 for a description of each type.</p>
Activation	<p>Click the icon to enable or disable a signature or group of signatures.</p>
Log	<p>These are the log options:</p> <p>original setting: Select this option to return each log option within a service group to its previously saved configuration.</p> <p>no: Select this option on an individual signature or a complete service group to have the ZyWALL create no log when a packet matches a signature(s).</p> <p>log: Select this option on an individual signature or a complete service group to have the ZyWALL create a log when a packet matches a signature(s).</p> <p>log alert: An alert is an e-mailed log for more serious events that may need more immediate attention. Select this option to have the ZyWALL send an alert when a packet matches a signature(s).</p>

Table 111 Policy > IDP > Profile > Packet Inspection_Group View (continued)

LABEL	DESCRIPTION
Action	<p>Select what action the ZyWALL should take when a packet matches a signature here.</p> <p>original setting: Select this action to return each signature in a service group to its previously saved configuration.</p> <p>none: Select this action on an individual signature or a complete service group to have the ZyWALL take no action when a packet matches the signature(s).</p> <p>drop: Select this action on an individual signature or a complete service group to have the ZyWALL silently drop a packet that matches the signature(s). Neither sender nor receiver are notified.</p> <p>reject-sender: Select this action on an individual signature or a complete service group to have the ZyWALL send a reset to the sender when a packet matches the signature. If it is a TCP attack packet, the ZyWALL will send a packet with a 'RST' flag. If it is an ICMP or UDP attack packet, the ZyWALL will send an ICMP unreachable packet.</p> <p>reject-receiver: Select this action on an individual signature or a complete service group to have the ZyWALL send a reset to the receiver when a packet matches the signature. If it is a TCP attack packet, the ZyWALL will send a packet with an 'RST' flag. If it is an ICMP or UDP attack packet, the ZyWALL will do nothing.</p> <p>reject-both: Select this action on an individual signature or a complete service group to have the ZyWALL send a reset to both the sender and receiver when a packet matches the signature. If it is a TCP attack packet, the ZyWALL will send a packet with a 'RST' flag to the receiver and sender. If it is an ICMP or UDP attack packet, the ZyWALL will send an ICMP unreachable packet.</p>
OK	A profile consists of three separate screens. If you want to configure just one screen for an IDP profile, click OK to save your settings to the ZyWALL, complete the profile and return to the profile summary page.
Cancel	Click Cancel to return to the profile summary page without saving any changes.
Save	If you want to configure more than one screen for an IDP profile, click Save to save the configuration to the ZyWALL, but remain in the same page. You may then go to another profile screen (tab) in order to complete the profile. Click OK in the final profile screen to complete the profile.

21.7.4 Profile > Packet Inspection > Query View Screen

Click **Switch to query view** in the screen as shown in [Figure 221 on page 342](#) to go to a signature query screen. In the query view screen, you can search for signatures by criteria such as name, ID, severity, attack type, vulnerable attack platforms, service category, log options or actions.

Figure 222 Policy > IDP > Profile > Packet Inspection_Query View

The following table describes the fields in this screen.

Table 112 Policy > IDP > Profile > Packet Inspection_Query View

LABEL	DESCRIPTION
Name	This is the name of the profile that you created in the IDP > Profiles > Packet Inspection group view screen.
Switch to group view	Click this button to go to the IDP profile group view screen where IDP signatures are grouped by service and you can configure activation, logs and/or actions.
Query Signatures	Select the criteria on which to perform the search.
Search all custom signatures	Select this check box to search for signatures you created or imported in the Custom Signature screen. You can search by name or ID. If the name and ID fields are left blank, then all custom signatures are displayed.
Name	Type the name or part of the name of the signature(s) you want to find.
Signature ID (SID)	Type the ID or part of the ID of the signature(s) you want to find.
Severity	Search for signatures by severity level(s) (see Table 111 on page 343). Hold down the [Ctrl] key if you want to make multiple selections.
Attack Type	Search for signatures by attack type(s) (see Table 109 on page 339). Attack types are known as policy types in the group view screen. Hold down the [Ctrl] key if you want to make multiple selections.

Table 112 Policy > IDP > Profile > Packet Inspection_Query View (continued)

LABEL	DESCRIPTION
Platform	Search for signatures created to prevent intrusions targeting specific operating system(s). Hold down the [Ctrl] key if you want to make multiple selections.
Service	Search for signatures by IDP service group(s). See Table 110 on page 340 for group details. Hold down the [Ctrl] key if you want to make multiple selections.
Activation	Search for enabled and/or disabled signatures here.
Log	Search for signatures by log option here. See Table 111 on page 343 for option details.
Actions	Search for signatures by the response the ZyWALL takes when a packet matches a signature. See Table 111 on page 343 for action details. Hold down the [Ctrl] key if you want to make multiple selections.
Search	Click this button to begin the search. The results display at the bottom of the screen. Results may be spread over several pages depending on how broad the search criteria selected were. The tighter the criteria selected, the fewer the signatures returned.
Query Result	The results are displayed in a table showing the SID, Name, Severity, Attack Type, Platform, Service, Activation, Log, and Action criteria as selected in the search. Click the SID column header to sort search results by signature ID.
Total IDP:	This displays the total number of signatures found in your search.
IDP per page	Select the number of signatures you want to appear per page here.
Page:1/1<-->	Navigate between pages of signatures found here.
OK	Click OK to save your settings to the ZyWALL, complete the profile and return to the profile summary page.
Cancel	Click Cancel to return to the profile summary page without saving any changes.
Save	Click Save to save the configuration to the ZyWALL, but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click OK in the final profile screen to complete the profile.

21.7.5 Query Example

This example shows a search with these criteria:

- Severity: severe and high
- Attack Type: DDoS
- Platform: Windows 2000 and Windows XP computers
- Service: Any
- Actions: Any

Figure 223 Query Example Search Criteria

Attributes, hold "Ctrl" to make multiple selection on items in the list.

Severity: Very-Low, Low, Medium, High, Severe

Attack Type: Any, Access-Control, Backdoor/Trojan, Buffer-Overflow, DDoS

Platform: Any, All, Win95/98, WinNT, WinXP/2000

Service: Any, DNS, FINGER, FTP, MYSQL

Configured options

Activation: any Log: any

Actions, hold "Ctrl" to make multiple selection on items in the list.

Any, none, drop, reject-sender, reject-receiver

Search

Figure 224 Query Example Search Results

Query Result

Total IDP: 27 30 IDP per page Page:1/1

SID	Name	Severity	Attack Type	Platform	Service	Activation	Log	Action
658	SMTP e...	high	DDOS	Win95/...	SMTP	⚡	no	none
529	NETBIO...	high	DDOS	Win95/...	NETBIOS	⚡	no	none
3638	WEB-CG...	high	DDOS	Win95/...	WEB_CGI	⚡	no	none
3159	NETBIO...	high	DDOS	Win95/...	NETBIOS	⚡	no	none
3158	NETBIO...	high	DDOS	Win95/...	NETBIOS	⚡	no	none
3150	WEB-II...	high	DDOS	Win95/...	WEB_IIS	⚡	no	none
3129	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3128	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3127	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3126	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3125	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3124	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3123	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3122	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3121	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3122	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3121	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3120	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3119	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3118	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3117	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3116	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3115	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
3114	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
2252	NETBIO...	high	DDOS	WinNT ...	NETBIOS	⚡	no	none
2004	MS-SQL...	severe	DDOS	WinNT ...	SQL	⚡	no	none
1920	FTP SI...	high	DDOS	Win95/...	FTP	⚡	no	none
1538	NNTP A...	high	DDOS	Win95/...	NNTP	⚡	no	none
1283	WEB-II...	high	DDOS	Win95/...	WEB_IIS	⚡	no	none

OK Cancel Save

21.8 Profiles: Traffic Anomaly

The traffic anomaly screen is the second screen in an IDP profile. Traffic anomaly detection looks for abnormal behavior such as scan or flooding attempts. Select **Policy > IDP > Profile > Traffic Anomaly**. If you made changes to other screens belonging to this profile, make sure you have clicked **OK** or **Save** to save the changes before selecting the **Traffic Anomaly** tab.

21.8.1 Port Scanning

An attacker scans device(s) to determine what types of network protocols or services a device supports. One of the most common port scanning tools in use today is Nmap.

Many connection attempts to different ports (services) may indicate a port scan. These are some port scan types:

- TCP Portscan
- UDP Portscan
- IP Portscan

An IP port scan searches not only for TCP, UDP and ICMP protocols in use by the remote computer, but also additional IP protocols such as EGP (Exterior Gateway Protocol) or IGP (Interior Gateway Protocol). Determining these additional protocols can help reveal if the destination device is a workstation, a printer, or a router.

21.8.1.1 Decoy Port Scans

Decoy port scans are scans where the attacker has spoofed the source address. These are some decoy scan types:

- TCP Decoy Portscan
- UDP Decoy Portscan
- IP Decoy Portscan

21.8.1.2 Distributed Port Scans

Distributed port scans are many-to-one port scans. Distributed port scans occur when multiple hosts query one host for open services. This may be used to evade intrusion detection. These are distributed port scan types:

- TCP Distributed Portscan
- UDP Distributed Portscan
- IP Distributed Portscan

21.8.1.3 Port Sweeps

Many different connection attempts to the same port (service) may indicate a port sweep, that is, they are one-to-many port scans. One host scans a single port on multiple hosts. This may occur when a new exploit comes out and the attacker is looking for a specific service. These are some port sweep types:

- TCP Portsweep
- UDP Portsweep
- IP Portsweep
- ICMP Portsweep

21.8.1.4 Filtered Port Scans

A filtered port scan may indicate that there were no network errors (ICMP unreachable or TCP RSTs) or responses on closed ports have been suppressed. Active network devices, such as NAT routers, may trigger these alerts if they send out many connection attempts within a very small amount of time. These are some filtered port scan examples.

- TCP Filtered Portscan
- TCP Filtered Decoy Portscan
- TCP Filtered Portsweep
- ICMP Filtered Portsweep
- IP Filtered Distributed Portscan
- UDP Filtered Portscan
- UDP Filtered Decoy Portscan
- UDP Filtered Portsweep
- TCP Filtered Distributed Portscan
- IP Filtered Portscan
- IP Filtered Decoy Portscan
- IP Filtered Portsweep
- UDP Filtered Distributed Portscan

21.8.2 Flood Detection

Flood attacks saturate a network with useless data, use up all available bandwidth, and therefore make communications in the network impossible.

21.8.2.1 ICMP Flood Attack

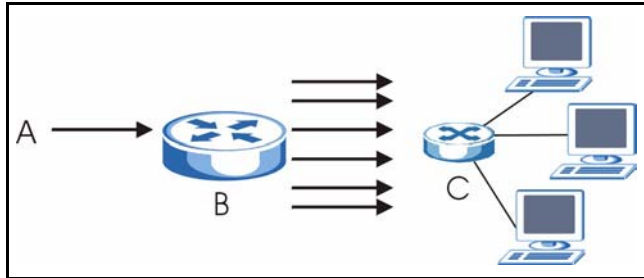
An ICMP flood is broadcasting many pings or UDP packets so that so much data is sent to the system, that it slows it down or locks it up.

21.8.2.2 Smurf

A smurf attacker (A) floods a router (B) with Internet Control Message Protocol (ICMP) echo request packets (pings) with the destination IP address of each packet as the broadcast address of the network. The router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic.

If an attacker (A) spoofs the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only saturate the receiving network (B), but the network of the spoofed source IP address (C).

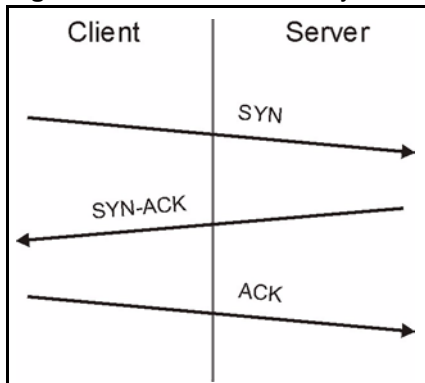
Figure 225 Smurf Attack



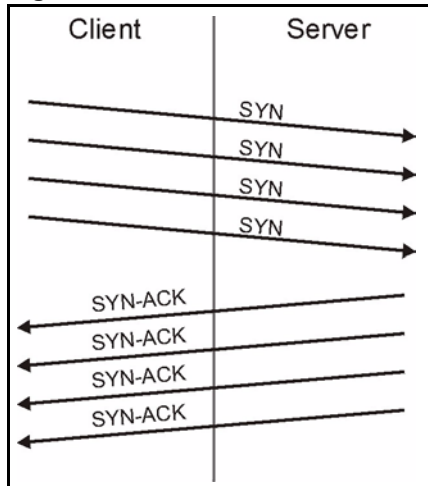
21.8.2.3 TCP SYN Flood Attack

Usually a client starts a session by sending a SYN (synchronize) packet to a server. The receiver returns 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 226 TCP Three-Way Handshake



A SYN flood attack is when an attacker sends a series of SYN packets. Each packet causes the receiver to reply with a SYN-ACK response. The receiver then waits for the ACK that follows the SYN-ACK, and stores all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are only moved off the queue when an ACK comes back or when an internal timer ends the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for other users.

Figure 227 SYN Flood

21.8.2.4 LAND Attack

In a LAND attack, hackers flood SYN packets into a network with a spoofed source IP address of the network itself. This makes it appear as if the computers in the network sent the packets to themselves, so the network is unavailable while they try to respond to themselves.

21.8.2.5 UDP Flood Attack

UDP is a connection-less protocol and it does not require any connection setup procedure to transfer data. A UDP flood attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down.

21.8.3 Profile > Traffic Anomaly Screen

Figure 228 Profiles: Traffic Anomaly

General
Profile
Custom Signatures
Update

Packet Inspection
Traffic Anomaly
Protocol Anomaly

Name

Scan Detection

Sensetivity medium

Name ▲	Activation	Log	Action
		log ▼	
(open port) Open Port		log ▼	none
(portscan) IP Decoy Protocol Scan		log ▼	none
(portscan) IP Distributed Protocol Scan		log ▼	none
(portscan) IP Filtered Decoy Protocol Scan		log ▼	none
(portscan) IP Filtered Distributed Protocol Scan		log ▼	none
(portscan) IP Filtered Protocol Scan		log ▼	none
(portscan) IP Protocol Scan		log ▼	none
(portscan) TCP Decoy Portscan		log ▼	none
(portscan) TCP Distributed Portscan		log ▼	none
(portscan) TCP Filtered Decoy Portscan		log ▼	none
(portscan) TCP Filtered Distributed Portscan		log ▼	none
(portscan) TCP Filtered Portscan		log ▼	none
(portscan) TCP Portscan		log ▼	none
(portscan) UDP Decoy Portscan		log ▼	none
(portscan) UDP Distributed Portscan		log ▼	none
(portscan) UDP Filtered Decoy Portscan		log ▼	none
(portscan) UDP Filtered Distributed Portscan		log ▼	none
(portscan) UDP Filtered Portscan		log ▼	none
(portscan) UDP Portscan		log ▼	none
(sweep) ICMP Filtered Sweep		log ▼	none
(sweep) ICMP Sweep		log ▼	none
(sweep) IP Filtered Protocol Sweep		log ▼	none
(sweep) IP Protocol Sweep		log ▼	none
(sweep) TCP Filtered Port Sweep		log ▼	none
(sweep) TCP Port Sweep		log ▼	none
(sweep) TCP Port Sweep		log ▼	none
(sweep) UDP Filtered Port Sweep		log ▼	none
(sweep) UDP Port Sweep		log ▼	none

Flood Detection

Sensetivity medium

Name ▲	Activation	Log	Action
		log ▼	
(flood) ICMP Flood		log ▼	none
(flood) IP Flood		log ▼	none
(flood) TCP Flood		log ▼	none
(flood) UDP Flood		log ▼	none

OK
Cancel
Save

The following table describes the fields in this screen.

Table 113 IDP > Profile > Traffic Anomaly

LABEL	DESCRIPTION
Name	<p>This is the name of the IDP profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names:</p> <p>MyProfile mYProfile Mymy12_3-4</p> <p>These are invalid profile names:</p> <p>1mYProfile My Profile MyProfile? Whatalongprofilename123456789012</p>
Scan/Flood Detection	<p>If you're uncertain of how to edit individual anomaly rules, then just decrease or increase traffic/protocol anomaly sensitivity.</p>
Name	<p>This is the name of the traffic anomaly rule. Click the Name column heading to sort in ascending or descending order according to the rule name.</p>
Sensitivity	<p>Select a sensitivity level so as to reduce false positives in your network. If you choose low sensitivity, then scan/flood thresholds and sample times are set low, so you will have fewer logs and false positives; however some traffic anomaly attacks may not be detected.</p> <p>If you choose high sensitivity, then scan/flood thresholds and sample times are set high, so most traffic anomaly attacks will be detected; however you will have more logs and false positives.</p>
Activation	<p>Click the icon to enable or disable a rule or group of rules.</p>
Log	<p>Select the log option here. See Table 111 on page 343 for option details.</p>
Action	<p>Action defines what the ZyWALL should do when a packet matches a rule. See Table 111 on page 343 for action details.</p> <p>Note: At the time of writing, these actions are not configurable for traffic anomaly rules.</p>
OK	<p>Click OK to save your settings to the ZyWALL, complete the profile and return to the profile summary page.</p>
Cancel	<p>Click Cancel to return to the profile summary page without saving any changes.</p>
Save	<p>Click Save to save the configuration to the ZyWALL but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click OK in the final profile screen to complete the profile.</p>

21.9 Profiles: Protocol Anomaly

Protocol anomaly is the third screen in an IDP profile. Protocol anomaly (PA) rules check for protocol compliance against the relevant RFC (Request for Comments).

Protocol anomaly detection includes HTTP Inspection, TCP Decoder, UDP Decoder and ICMP Decoder where each category reflects the packet type inspected.

Protocol anomaly rules may be updated when you upload new firmware.

21.9.1 HTTP Inspection and TCP/UDP/ICMP Decoders

The following table gives some information on the HTTP inspection, TCP decoder, UDP decoder and ICMP decoder ZyWALL protocol anomaly rules.

Table 114 HTTP Inspection and TCP/UDP/ICMP Decoders

LABEL	DESCRIPTION
HTTP Inspection	
APACHE-WHITESPACE ATTACK	This rule deals with non-RFC standard of tab for a space delimiter. Apache uses this, so if you have an Apache server, you need to enable this option.
ASCII-ENCODING ATTACK	This rule can detect attacks where malicious attackers use ASCII-encoding to encode attack strings. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server.
BARE-BYTE-UNICODE-ENCODING ATTACK	Bare byte encoding uses non-ASCII characters as valid values in decoding UTF-8 values. This is NOT in the HTTP standard, as all non-ASCII values have to be encoded with a %. Bare byte encoding allows the user to emulate an IIS server and interpret non-standard encodings correctly.
BASE36-ENCODING ATTACK	This is a rule to decode base36-encoded characters. This rule can detect attacks where malicious attackers use base36-encoding to encode attack strings. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server.
DIRECTORY-TRAVERSAL ATTACK	This rule normalizes directory traversals and self-referential directories. So, "/abc/this_is_not_a_real_dir/./xyz" get normalized to "/abc/xyz". Also, "/abc/./xyz" gets normalized to "/abc/xyz". If a user wants to configure an alert, then specify "yes", otherwise "no". This alert may give false positives since some web sites refer to files using directory traversals.
DOUBLE-ENCODING ATTACK	This rule is IIS specific. IIS does two passes through the request URI, doing decodes in each one. In the first pass, IIS encoding (UTF-8 unicode, ASCII, bare byte, and %u) is done. In the second pass ASCII, bare byte, and %u encodings are done.
IIS-BACKSLASH-EVASION ATTACK	This is an IIS emulation rule that normalizes backslashes to slashes. Therefore, a request-URI of "/abc\xyz" gets normalized to "/abc/xyz".
IIS-UNICODE-CODEPOINT-ENCODING ATTACK	This rule can detect attacks which send attack strings containing non-ASCII characters encoded by IIS Unicode. IIS Unicode encoding references the unicode.map file. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server.
MULTI-SLASH-ENCODING ATTACK	This rule normalizes multiple slashes in a row, so something like: "abc////////xyz" get normalized to "abc/xyz".
NON-RFC-DEFINED-CHAR ATTACK	This rule lets you receive a log or alert if certain non-RFC characters are used in a request URI. For instance, you may want to know if there are NULL bytes in the request-URI.
NON-RFC-HTTP-DELIMITER ATTACK	This is when a newline "\n" character is detected as a delimiter. This is non-standard but is accepted by both Apache and IIS web servers.

Table 114 HTTP Inspection and TCP/UDP/ICMP Decoders (continued)

LABEL	DESCRIPTION
OVERSIZE-CHUNK-ENCODING ATTACK	This rule is an anomaly detector for abnormally large chunk sizes. This picks up the apache chunk encoding exploits and may also be triggered on HTTP tunneling that uses chunk encoding.
OVERSIZE-REQUEST-URI-DIRECTORY ATTACK	This rule takes a non-zero positive integer as an argument. The argument specifies the max character directory length for URL directory. If a URL directory is larger than this argument size, an alert is generated. A good argument value is 300 characters. This should limit the alerts to IDS evasion type attacks, like whisker.
SELF-DIRECTORY-TRAVERSAL ATTACK	This rule normalizes self-referential directories. So, "/abc/.xyz" gets normalized to "/abc/xyz".
U-ENCODING ATTACK	This rule emulates the IIS %u encoding scheme. The %u encoding scheme starts with a %u followed by 4 characters, like %uXXXX. The XXXX is a hex encoded value that correlates to an IIS unicode codepoint. This is an ASCII value. An ASCII character is encoded like, %u002f = /, %u002e = ., etc.
UTF-8-ENCODING ATTACK	The UTF-8 decode rule decodes standard UTF-8 unicode sequences that are in the URI. This abides by the unicode standard and only uses % encoding. Apache uses this standard, so for any Apache servers, make sure you have this option turned on. When this rule is enabled, ASCII decoding is also enabled to enforce correct functioning.
WEBROOT-DIRECTORY-TRAVERSAL ATTACK	This is when a directory traversal traverses past the web server root directory. This generates much fewer false positives than the directory option, because it doesn't alert on directory traversals that stay within the web server directory structure. It only alerts when the directory traversals go past the web server root directory, which is associated with certain web attacks.
TCP Decoder	
BAD-LENGTH-OPTIONS ATTACK	This is when a TCP packet is sent where the TCP option length field is not the same as what it actually is or is 0. This may cause some applications to crash.
EXPERIMENTAL-OPTIONS ATTACK	This is when a TCP packet is sent which contains non-RFC-complaint options. This may cause some applications to crash.
OBSOLETE-OPTIONS ATTACK	This is when a TCP packet is sent which contains obsolete RFC options.
OVERSIZE-OFFSET ATTACK	This is when a TCP packet is sent where the TCP data offset is larger than the payload.
TRUNCATED-OPTIONS ATTACK	This is when a TCP packet is sent which doesn't have enough data to read. This could mean the packet was truncated.
TTCP-DETECTED ATTACK	T/TCP provides a way of bypassing the standard three-way handshake found in TCP, thus speeding up transactions. However, this could lead to unauthorized access to the system by spoofing connections.
UNDERSIZE-LEN ATTACK	This is when a TCP packet is sent which has a TCP datagram length of less than 20 bytes. This may cause some applications to crash.
UNDERSIZE-OFFSET ATTACK	This is when a TCP packet is sent which has a TCP header length of less than 20 bytes. This may cause some applications to crash.
UDP Decoder	

Table 114 HTTP Inspection and TCP/UDP/ICMP Decoders (continued)

LABEL	DESCRIPTION
OVERSIZE-LEN ATTACK	This is when a UDP packet is sent which has a UDP length field of greater than the actual packet length. This may cause some applications to crash.
TRUNCATED-HEADER ATTACK	This is when a UDP packet is sent which has a UDP datagram length of less than the UDP header length. This may cause some applications to crash.
UNDERSIZE-LEN ATTACK	This is when a UDP packet is sent which has a UDP length field of less than 8 bytes. This may cause some applications to crash.
ICMP Decoder	
TRUNCATED-ADDRESS-HEADER ATTACK	This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP address header length. This may cause some applications to crash.
TRUNCATED-HEADER ATTACK	This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP header length. This may cause some applications to crash.
TRUNCATED-TIMESTAMP-HEADER ATTACK	This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP Time Stamp header length. This may cause some applications to crash.

21.9.2 Protocol Anomaly Configuration

Select **Policy > IDP > Profile > Protocol Anomaly**. If you made changes to other screens belonging to this profile, make sure you have clicked **OK** or **Save** to save the changes before selecting the **Protocol Anomaly** tab.

Figure 229 Profiles: Protocol Anomaly

General **Profile** Custom Signatures Update

Packet Inspection Traffic Anomaly **Protocol Anomaly**

Name LAN_IDP

HTTP Inspection

Name ▲	Activation	Log	Action
(http_inspect) APACHE-WHITESPACE ATTACK		log	none
(http_inspect) ASCII-ENCODING ATTACK		log	none
(http_inspect) BARE-BYTE-UNICODING-ENCODING ATTACK		log	none
(http_inspect) BASE36-ENCODING ATTACK		log	none
(http_inspect) DIRECTORY-TRAVERSAL ATTACK		log	none
(http_inspect) DOUBLE-ENCODING ATTACK		log	none
(http_inspect) IIS-BACKSLASH-EVASION ATTACK		log	none
(http_inspect) IIS-UNICODE-CODEPOINT-ENCODING ATTACK		log	none
(http_inspect) MULTI-SLASH-ENCODING ATTACK		log	none
(http_inspect) NON-RFC-DEFINED-CHAR ATTACK		log	none
(http_inspect) NON-RFC-HTTP-DELIMITER ATTACK		log	none
(http_inspect) OVERSIZE-CHUNK-ENCODING ATTACK		log	none
(http_inspect) OVERSIZE-REQUEST-URI-DIRECTORY ATTACK		log	none
(http_inspect) SELF-DIRECTORY-TRAVERSAL ATTACK		log	none
(http_inspect) U-ENCODING ATTACK		log	none
(http_inspect) UTF-8-ENCODING ATTACK		log	none
(http_inspect) WEBROOT-DIRECTORY-TRAVERSAL ATTACK		log	none

TCP Decoder

Name ▲	Activation	Log	Action
(tcp_decoder) BAD-LENGTH-OPTIONS ATTACK		log	none
(tcp_decoder) EXPERIMENTAL-OPTIONS ATTACK		log	none
(tcp_decoder) OBSOLETE-OPTIONS ATTACK		log	none
(tcp_decoder) OVERSIZE-OFFSET ATTACK		log	none
(tcp_decoder) TRUNCATED-OPTIONS ATTACK		log	none
(tcp_decoder) TTCP-DETECTED ATTACK		log	none
(tcp_decoder) UNDERSIZE-LEN ATTACK		log	none
(tcp_decoder) UNDERSIZE-OFFSET ATTACK		log	none

UDP Decoder

Name ▲	Activation	Log	Action
(udp_decoder) OVERSIZE-LEN ATTACK		log	none
(udp_decoder) TRUNCATED-HEADER ATTACK		log	none
(udp_decoder) UNDERSIZE-LEN ATTACK		log	none

ICMP Decoder

Name ▲	Activation	Log	Action
(icmp_decoder) TRUNCATED-ADDRESS-HEADER ATTACK		log	none
(icmp_decoder) TRUNCATED-HEADER ATTACK		log	none
(icmp_decoder) TRUNCATED-TIMESTAMP-HEADER ATTACK		log	none

OK Cancel Save

The following table describes the fields in this screen.

Table 115 IDP > Profile > Protocol Anomaly

LABEL	DESCRIPTION
Name	This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: MyProfile mYProfile Mymy12_3-4 These are invalid profile names: 1mYProfile My Profile MyProfile? Whatalongprofilename123456789012
HTTP Inspection/TCP Decoder/UDP Decoder/ICMP Decoder	
Name	This is the name of the protocol anomaly rule. Click the Name column heading to sort in ascending or descending order according to the protocol anomaly rule name.
Activation	Click the icon to enable or disable a rule or group of rules.
Log	Select the log option here. See Table 111 on page 343 for option details.
Action	Select what the ZyWALL should do when a packet matches a rule. See Table 111 on page 343 for action details.
OK	Click OK to save your settings to the ZyWALL, complete the profile and return to the profile summary page.
Cancel	Click Cancel to return to the profile summary page without saving any changes.
Save	Click Save to save the configuration to the ZyWALL but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click OK in the final profile screen to complete the profile.

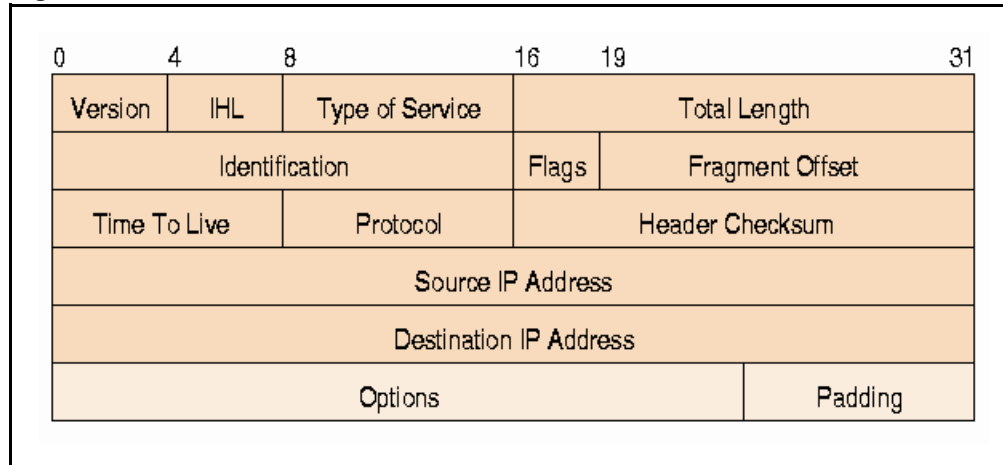
21.10 Introducing IDP Custom Signatures

Create custom signatures for new attacks or attacks peculiar to your network. Custom signatures can also be saved to/from your computer so as to share with others.

You need some knowledge of packet headers and attack types to create your own custom signatures.

21.10.1 IP Packet Header

These are the fields in an Internet Protocol (IP) version 4 packet header.

Figure 230 IP v4 Packet Headers

The header fields are discussed below:

Table 116 IP v4 Packet Headers

HEADER	DESCRIPTION
Version	The value 4 indicates IP version 4.
IHL	IP Header Length is the number of 32 bit words forming the total length of the header (usually five).
Type of Service	The Type of Service, (also known as Differentiated Services Code Point (DSCP)) is usually set to 0, but may indicate particular quality of service needs from the network.
Total Length	This is the size of the datagram in bytes. It is the combined length of the header and the data.
Identification	This is a 16-bit number, which together with the source address, uniquely identifies this packet. It is used during reassembly of fragmented datagrams.
Flags	Flags are used to control whether routers are allowed to fragment a packet and to indicate the parts of a packet to the receiver.
Fragment Offset	This is a byte count from the start of the original sent packet.
Time To Live	This is a counter that decrements every time it passes through a router. When it reaches zero, the datagram is discarded. It is used to prevent accidental routing loops.
Protocol	The protocol indicates the type of transport packet being carried, for example, 1 = ICMP; 2= IGMP; 6 = TCP; 17= UDP.
Header Checksum	This is used to detect processing errors introduced into the packet inside a router or bridge where the packet is not protected by a link layer cyclic redundancy check. Packets with an invalid checksum are discarded by all nodes in an IP network.
Source IP Address	This is the IP address of the original sender of the packet.
Destination IP Address	This is the IP address of the final destination of the packet.

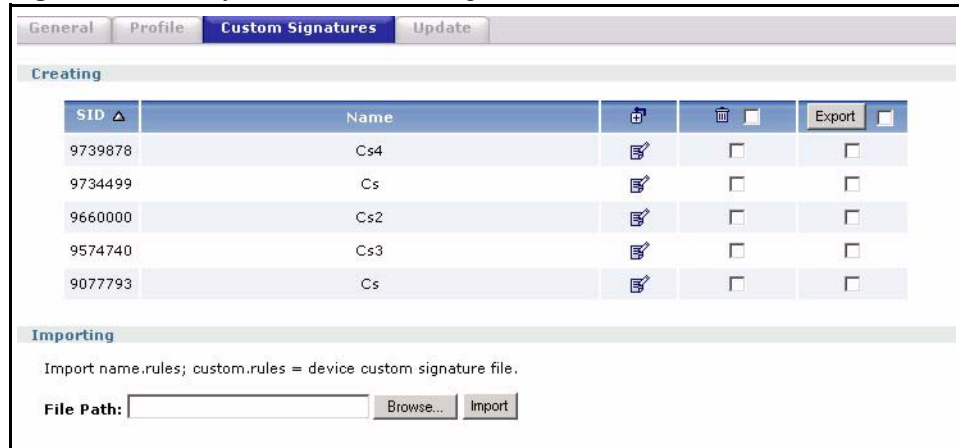
Table 116 IP v4 Packet Headers (continued)

HEADER	DESCRIPTION
Options	IP options is a variable-length list of IP options for a datagram that define IP Security Option , IP Stream Identifier , (security and handling restrictions for the military), Record Route (have each router record its IP address), Loose Source Routing (specifies a list of IP addresses that must be traversed by the datagram), Strict Source Routing (specifies a list of IP addresses that must ONLY be traversed by the datagram), Timestamp (have each router record its IP address and time), End of IP List and No IP Options .
Padding	Padding is used as a filler to ensure that the IP packet is a multiple of 32 bits.

21.11 Configuring Custom Signatures

Select **Policy > IDP > Custom Signatures**. The first screen shows a summary of all custom signatures created. Click the **SID** or **Name** heading to sort. Click the add icon to create a new signature or click the edit icon to edit an existing signature. You can delete signatures here or save them to your computer.

Note: The ZyWALL checks all signatures and continues searching even after a match is found. If two or more rules have conflicting actions for the same packet, then the ZYWALL applies the more restrictive action (**reject-both**, **reject-receiver** or **reject-sender**, **drop**, **none** in this order). If a packet matches a rule for **reject-receiver** and it also matches a rule for **reject-sender**, then the ZyWALL will **reject-both**.

Figure 231 Policy > IDP > Custom Signatures

The following table describes the fields in this screen.

Table 117 Policy > IDP > Custom Signatures

LABEL	DESCRIPTION
Creating	Use this part of the screen to create, edit, delete or export (save to your computer) custom signatures.
SID	SID is the signature ID that uniquely identifies a signature. Click the SID header to sort signatures in ascending or descending order. It is automatically created when you click the add icon to create a new signature. You can edit the ID, but it cannot already exist and it must be in the 9000000 to 9999999 range.
Name	This is the name of your custom signature. Duplicate names can exist, but it is advisable to use unique signature names that give some hint as to intent of the signature and the type of attack it is supposed to prevent.
Add/Edit 	Click the add icon to create a new signature or click the edit icon to edit an existing signature.
Delete 	Use this column to delete signatures. Select (or clear) the check box in the header column to select (or clear) all check boxes in that column. You can also select (or clear) individual signatures within the column. When you are certain that you have only selected signatures that you want to delete, click the remove icon. Click OK in the confirm delete signature dialog box to delete the selected signature(s).
Export 	Use this column to save signatures to your computer. Select (or clear) the check box in the header column to select (or clear) all check boxes in that column. You can also select (or clear) individual signatures within the column. When you are certain that you have only selected signatures that you want to save, click Export . Click Save in the file download dialog box and then select a location and name for the file. Custom signatures must end with the 'rules' file name extension, for example, MySig.rules.

Table 117 Policy > IDP > Custom Signatures (continued)

LABEL	DESCRIPTION
Importing	Use this part of the screen to import custom signatures (previously saved to your computer) to the ZyWALL. Note: The name of the complete custom signature file on the ZyWALL is 'custom.rules'. If you import a file named 'custom.rules', then all custom signatures on the ZyWALL are overwritten with the new file. If this is not your intention, make sure that the files you import are not named 'custom.rules'.
File Path	Type the file path and name of the custom signature file you want to import in the text box (or click Browse to find it on your computer) and then click Import to transfer the file to the ZyWALL. New signatures then display in the ZyWALL IDP > Custom Signatures screen.

21.11.1 Creating or Editing a Custom Signature

Click the add icon to create a new signature or click the edit icon to edit an existing signature in the screen as shown in [Figure 231 on page 361](#).

A packet must match all items you configure in this screen before it matches the signature. The more specific your signature (including packet contents), then the fewer false positives the signature will trigger.

Try to write signatures that target a vulnerability, for example a certain type of traffic on certain operating systems, instead of a specific exploit.

Figure 232 Policy > IDP > Custom Signatures > Add/Edit

Name	Example		
Signature ID	9525484		
Information			
Severity	[Dropdown]		
Platform	<input type="checkbox"/> All <input type="checkbox"/> WinXP/2000 <input type="checkbox"/> Solaris <input type="checkbox"/> Network-Device	<input type="checkbox"/> Win95/98 <input type="checkbox"/> Linux <input type="checkbox"/> SGI	<input type="checkbox"/> WinNT <input type="checkbox"/> FreeBSD <input type="checkbox"/> Other-Unix
Service	[Dropdown]		
Policy Type	[Dropdown]		
Frequency			
<input type="checkbox"/> Threshold	[0] Packet(s)/	[0] Second(s)	
Header Options			
Network Protocol	IPv4		
<input type="checkbox"/> Type of Service	Equal [0]		
<input type="checkbox"/> Identification	[0]		
<input type="checkbox"/> Fragmentation	<input type="checkbox"/> Reserved Bit <input type="checkbox"/> Don't Fragment <input type="checkbox"/> More Fragment		
<input type="checkbox"/> Fragment Offset	Equal [0]		
<input type="checkbox"/> Time to Live	Equal [0]		
<input type="checkbox"/> IP Options	Any [Dropdown]		
<input type="checkbox"/> Same IP			
Transport Protocol	TCP [Dropdown]		
<input type="checkbox"/> Port	Source Port [0]	Destination Port [0]	
<input checked="" type="checkbox"/> Flow	To Client [Dropdown]	Established [Dropdown] No Stream [Dropdown]	
<input type="checkbox"/> Flags	<input type="checkbox"/> SYN <input type="checkbox"/> FIN <input type="checkbox"/> RST <input type="checkbox"/> PSH <input type="checkbox"/> ACK <input type="checkbox"/> URG <input type="checkbox"/> Reserved 1 (MSB) <input type="checkbox"/> Reserved 2		
<input type="checkbox"/> Sequence Number	[0]		
<input type="checkbox"/> Ack Number	[0]		
<input type="checkbox"/> Window Size	Equal [0]		
Payload Options			
<input type="checkbox"/> Payload Size	Equal [0]	Byte(s)	
Patterns			
<input checked="" type="checkbox"/> Offset	Relative to start of payload [23]		[Add]
Content	Add content [Text Box]		[Add] [Delete]
	<input checked="" type="checkbox"/> Case-insensitive <input checked="" type="checkbox"/> Decode as URI		
<input checked="" type="checkbox"/> Offset	Relative to start of payload [58]		[Add]
Content	Add content [Text Box]		[Add] [Delete]
	<input checked="" type="checkbox"/> Case-insensitive <input checked="" type="checkbox"/> Decode as URI		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

The following table describes the fields in this screen.

Table 118 Policy > IDP > Custom Signatures > Add/Edit

LABEL	DESCRIPTION
Name	Type the name of your custom signature. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. Duplicate names can exist but it is advisable to use unique signature names that give some hint as to intent of the signature and the type of attack it is supposed to prevent. Refer to (but do not copy) the packet inspection signature names for hints on creating a naming convention.
Signature ID	A signature ID is automatically created when you click the add icon to create a new signature. You can edit the ID to create a new one (in the 9000000 to 9999999 range), but you cannot use one that already exists. You may want to do that if you want to order custom signatures by SID.
Information	Use the following fields to set general information about the signature as denoted below.
Severity	The severity level denotes how serious the intrusion is. Categorize the seriousness of the intrusion here. See Table 111 on page 343 as a reference.
Platform	Some intrusions target specific operating systems only. Select the operating systems that the intrusion targets, that is, the operating systems you want to protect from this intrusion. SGI refers to Silicon Graphics Incorporated, who manufactures multi-user Unix workstations that run the IRIX operating system (SGI's version of UNIX). A router is an example of a network device.
Service	Select the IDP service group that the intrusion exploits or targets. See Table 110 on page 340 for a list of IDP service groups. The custom signature then appears in that group in the IDP > Profile > Packet Inspection screen
Policy Type	Categorize the type of intrusion here. See Table 109 on page 339 as a reference.
Frequency	Recurring packets of the same type may indicate an attack. Use the following field to indicate how many packets per how many seconds constitute an intrusion
Threshold	Select Threshold and then type how many packets (that meet the criteria in this signature) per how many seconds constitute an intrusion.
Header Options	
Network Protocol	Configure signatures for IP version 4.
Type Of Service	Type of service in an IP header is used to specify levels of speed and/or reliability. Some intrusions use an invalid Type Of Service number. Select the check box, then select Equal or Not-Equal and then type in a number.
Identification	The identification field in a datagram uniquely identifies the datagram. If a datagram is fragmented, it contains a value that identifies the datagram to which the fragment belongs. Some intrusions use an invalid Identification number. Select the check box and then type in the invalid number that the intrusion uses.
Fragmentation	A fragmentation flag identifies whether the IP datagram should be fragmented, not fragmented or is a reserved bit. Some intrusions can be identified by this flag. Select the check box and then select the flag that the intrusion uses.
Fragmentation Offset	When an IP datagram is fragmented, it is reassembled at the final destination. The fragmentation offset identifies where the fragment belongs in a set of fragments. Some intrusions use an invalid Fragmentation Offset number. Select the check box, select Equal , Smaller or Greater and then type in a number

Table 118 Policy > IDP > Custom Signatures > Add/Edit (continued)

LABEL	DESCRIPTION
Time to Live	Time to Live is a counter that decrements every time it passes through a router. When it reaches zero, the datagram is discarded. Usually it's used to set an upper limit on the number of routers a datagram can pass through. Some intrusions can be identified by the number in this field. Select the check box, select Equal , Smaller or Greater and then type in a number.
IP Options	IP options is a variable-length list of IP options for a datagram that define IP Security Option , IP Stream Identifier , (security and handling restrictions for the military), Record Route (have each router record its IP address), Loose Source Routing (specifies a list of IP addresses that must be traversed by the datagram), Strict Source Routing (specifies a list of IP addresses that must ONLY be traversed by the datagram), Timestamp (have each router record its IP address and time), End of IP List and No IP Options . IP Options can help identify some intrusions. Select the check box, then select an item from the list box that the intrusion uses
Same IP	Select the check box for the signature to check for packets that have the same source and destination IP addresses.
Transport Protocol	The following fields vary depending on whether you choose TCP , UDP or ICMP .
Transport Protocol: TCP	
Port	Select the check box and then enter the source and destination TCP port numbers that will trigger this signature.
Flow	<p>If selected, the signature only applies to certain directions of the traffic flow and only to clients or servers. Select Flow and then select the identifying options.</p> <p>Established: The signature only checks for established TCP connections</p> <p>Stateless: The signature is triggered regardless of the state of the stream processor (this is useful for packets that are designed to cause devices to crash)</p> <p>To Client: The signature only checks for server responses from A to B.</p> <p>To Server: The signature only checks for client requests from B to A.</p> <p>From Client: The signature only checks for client requests from B to A.</p> <p>From Servers: The signature only checks for server responses from A to B.</p> <p>No Stream: The signature does not check rebuilt stream packets.</p> <p>Only Stream: The signature only checks rebuilt stream packets.</p>
Flags	Select what TCP flag bits the signature should check.
Sequence Number	Use this field to check for a specific TCP sequence number.
Ack Number	Use this field to check for a specific TCP acknowledgement number.
Window Size	Use this field to check for a specific TCP window size.
Transport Protocol: UDP	
Port	Select the check box and then enter the source and destination UDP port numbers that will trigger this signature.
Transport Protocol: ICMP	
Type	Use this field to check for a specific ICMP type value.
Code	Use this field to check for a specific ICMP code value.

Table 118 Policy > IDP > Custom Signatures > Add/Edit (continued)

LABEL	DESCRIPTION
ID	Use this field to check for a specific ICMP ID value. This is useful for covert channel programs that use static ICMP fields when they communicate.
Sequence Number	Use this field to check for a specific ICMP sequence number. This is useful for covert channel programs that use static ICMP fields when they communicate.
Payload Options	The longer a payload option is, the more exact the match, the faster the signature processing. Therefore, if possible, it is recommended to have at least one payload option in your signature.
Payload Size	This field may be used to check for abnormally sized packets or for detecting buffer overflows. Select the check box, then select Equal , Smaller or Greater and then type the payload size. Stream rebuilt packets are not checked regardless of the size of the payload.
Offset	This field specifies where to start searching for a pattern within a packet. For example, an offset of 5 would start looking for the specified pattern after the first five bytes of the payload.
Content	Type the content that the signature should search for in the packet payload. Hexadecimal code entered between pipes is converted to ASCII. For example, you could represent the ampersand as either <code>&</code> or <code> 26 </code> (26 is the hexadecimal code for the ampersand).
Case-insensitive	Select this check box if content casing does NOT matter.
Decode as URI	A Uniform Resource Identifier (URI) is a string of characters for identifying an abstract or physical resource (RFC 2396). A resource can be anything that has identity, for example, an electronic document, an image, a service ("today's weather report for Taiwan"), a collection of other resources. An identifier is an object that can act as a reference to something that has identity. Example URIs are: <code>ftp://ftp.is.co.za/rfc/rfc1808.txt</code> ; ftp scheme for File Transfer Protocol services <code>http://www.math.uio.no/faq/compression-faq/part1.html</code> ; http scheme for Hypertext Transfer Protocol services <code>mailto:mduerst@ifi.unizh.ch</code> ; mailto scheme for electronic mail addresses <code>telnet://melvyl.ucop.edu/</code> ; telnet scheme for interactive services via the TELNET Protocol Select this check box for the signature to search for normalized URI fields. This means that if you are writing signatures that includes normalized content, such as <code>%2</code> for directory traversals, these signatures will not be triggered because the content is normalized out of the URI buffer. For example, the URI: <code>/scripts/..%c0%af../winnt/system32/cmd.exe?/c+ver</code> will get normalized into: <code>/winnt/system32/cmd.exe?/c+ver</code>
OK	Click this button to save your changes to the ZyWALL and return to the summary screen.
Cancel	Click this button to return to the summary screen without saving any changes.

21.11.2 Custom Signature Example

Before creating a custom signature, you must first clearly understand the vulnerability.

21.11.2.1 Understand the Vulnerability

Check the ZyWALL logs when the attack occurs. Use web sites such as Google and security focus to get as much information about the attack as you can. The more specific your signature, the less chance it will cause false positives.

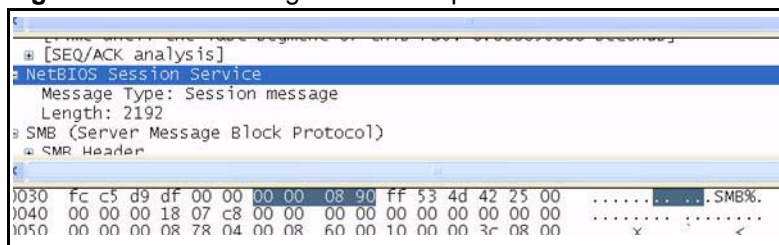
As an example, say you want to create a signature for the ‘Microsoft Windows Plug-and-Play Service Remote Overflow (MS-05-39)’ attack. Search the Security Focus web site and you will find it uses the NetBIOS service in established TCP connections to a server using port 445.

21.11.2.2 Analyze Packets

Then use a packet sniffer such as TCPdump or Ethereal to investigate some more.

From the NetBIOS header you see that the first byte ‘00’ defines the message type. The next three bytes represent the length of data, so you can ignore it. Therefore enter `|00|` as the first pattern.

Figure 233 Custom Signature Example Pattern 1



Next, check the content of the SMB header. Add `|FF|SMB%` and ‘TransactionNmPipe’ to the signature as the next patterns.

Figure 236 Example Custom Signature

Name	MS0539	
Signature ID	9914437	
Information		
Severity	high	
Platform	<input type="checkbox"/> All <input type="checkbox"/> Win95/98 <input type="checkbox"/> WinNT <input checked="" type="checkbox"/> WinXP/2000 <input type="checkbox"/> Linux <input type="checkbox"/> FreeBSD <input type="checkbox"/> Solaris <input type="checkbox"/> SGI <input type="checkbox"/> Other-Unix <input type="checkbox"/> Network-Device	
Service	NETBIOS	
Policy Type	BufferOverflow	
Frequency		
<input type="checkbox"/> Threshold	Packet(s) / Second(s)	
Header Options		
Network Protocol	IPv4	
<input type="checkbox"/> Type of Service	Equal	
<input type="checkbox"/> Identification		
<input type="checkbox"/> Fragmentation	<input type="checkbox"/> Reserved Bit <input type="checkbox"/> Don't Fragment <input type="checkbox"/> More Fragment	
<input type="checkbox"/> Fragment Offset	Equal	
<input type="checkbox"/> Time to Live	Equal	
<input type="checkbox"/> IP Options	Any	
<input type="checkbox"/> Same IP		
Transport Protocol	TCP	
<input checked="" type="checkbox"/> Port	Source Port 0	Destination Port 445
<input checked="" type="checkbox"/> Flow	Established	To Server Only Stream
<input type="checkbox"/> Flags	<input type="checkbox"/> SYN <input type="checkbox"/> FIN <input type="checkbox"/> RST <input type="checkbox"/> PSH <input type="checkbox"/> ACK <input type="checkbox"/> URG <input type="checkbox"/> Reserved 1 (MSB) <input type="checkbox"/> Reserved 2	
<input type="checkbox"/> Sequence Number		
<input type="checkbox"/> Ack Number		
<input type="checkbox"/> Window Size	Equal	
Payload Options		
<input type="checkbox"/> Payload Size	Equal Byte(s)	
Patterns		
<input checked="" type="checkbox"/> Offset	Relative to start of payload 0	
Content	000	
<input checked="" type="checkbox"/> Offset	Relative to end of last match 3	
Content	FFSMB%	
<input checked="" type="checkbox"/> Offset	Relative to end of last match 56	
Content	8000	
<input checked="" type="checkbox"/> Offset	Relative to start of payload 58	
Content	5C 00P00000P000E00 5C 00 00 00	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

21.11.3 Applying Custom Signatures

After you create your custom signature, it becomes available in the IDP service group category in the **IDP > Profile > Packet Inspection** screen. Custom signatures have an SID from 9000000 to 9999999.

You can activate the signature, configure what action to take when a packet matches it and if it should generate a log or alert in a profile. Then bind the profile to a zone.

Figure 237 Example: Custom Signature in IDP Profile

Message	SID	Severity	Policy Type	Alert	Action	Log
RPC				original setting	none	
POP3				original setting	none	
POP2				log	none	
P2P				original setting	none	
ORACLE				log	none	
NNTP				log	none	
NETBIOS				original setting	none	
MS0539	9914437	High	BufferOverflow	log	none	
NETBIOS DCERPC CoGetInstanceFromFile little endian overflow attempt	3158	high	DDOS	log	none	
NETBIOS DCERPC CoGetInstanceFromFile overflow attempt	3159	high	DDOS	log	none	
NETBIOS DCERPC DIRECT veritas alter context attempt	3697	low	AccessControl	no	none	
NETBIOS DCERPC DIRECT veritas bind attempt	3698	low	AccessControl	no	none	
NETBIOS DCERPC DIRECT veritas little endian alter context attempt	3699	low	AccessControl	no	none	
NETBIOS DCERPC DIRECT veritas little endian bind attempt	3700	low	AccessControl	no	none	

21.11.4 Verifying Custom Signatures

You should configure the signature to create a log when an ‘attack packet’ matches the signature. (You may also want to configure an alert if the attack is more serious and needs more immediate attention.) After you apply the signature to a zone, you can see if it works by checking the logs (**Maintenance > Logs > View Log**).

All IDP signatures come under the **IDP** category. The **Priority** column shows **warn** for signatures that are configured to generate a log only. It shows **critical** for signatures that are configured to generate a log and alert. **count** is the number of attacks that occurred at that time. The **Note** column displays **ACCESS FORWARD** when no action is configured for the signature. It displays **ACCESS DENIED** if you configure the signature action to drop the packet. The destination port is the service port (NetBIOS in this case) that the attack tries to exploit.

Figure 238 Custom Signature Log

#	Time	Priority	Category	Message	Source	Destination	Note
1	2006-05-08 03:49:03	warn	IDP	[type=Sig(648)] SHELLCODE x86 NOOP, Action: No Action	10.10.10.1:1246	192.168.199.96:445	ACCESS FORWARD
2	2006-05-08 03:49:03	warn	IDP	[type=Sig(9914437)] ms0539, Action: No Action [count=10]	10.10.10.1:1246	192.168.199.96:445	ACCESS FORWARD

21.11.5 Snort Signatures

You may want to refer to open source Snort signatures when creating custom ZyWALL ones. Most Snort rules are written in a single line. Snort rules are divided into two logical sections, the rule header and the rule options as shown in the following example:

```
alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 a5|";
msg:"moundt access");
```

The text up to the first parenthesis is the rule header and the section enclosed in parenthesis contains the rule options. The words before the colons in the rule options section are the option keywords.

The rule header contains the rule's:

- Action
- Protocol
- Source and destination IP addresses and netmasks
- Source and destination ports information.

The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken.

These are some equivalent Snort terms in the ZyWALL.

Table 119 ZyWALL - Snort Equivalent Terms

ZYWALL TERM	SNORT EQUIVALENT TERM
Type Of Service	tos
Identification	id
Fragmentation	fragbits
Fragmentation Offset	fragoffset
Time to Live	ttl
IP Options	ipopts

Table 119 ZyWALL - Snort Equivalent Terms (continued)

ZYWALL TERM	SNORT EQUIVALENT TERM
Same IP	sameip
Transport Protocol	
Transport Protocol: TCP	
Port	(In Snort rule header)
Flow	flow
Flags	flags
Sequence Number	seq
Ack Number	ack
Window Size	window
Transport Protocol: UDP	(In Snort rule header)
Port	(In Snort rule header)
Transport Protocol: ICMP	
Type	itype
Code	icode
ID	icmp_id
Sequence Number	icmp_seq
Payload Options	(Snort rule options)
Payload Size	dsize
Offset (relative to start of payload)	offset
Relative to end of last match	distance
Content	content
Case-insensitive	nocase
Decode as URI	uricontent

Note: Not all Snort functionality is supported in the ZyWALL.

21.12 Updating IDP Signatures

The ZyWALL comes with IDP signatures and anomaly rules. These are continually updated as new attack types evolve. New signatures can be downloaded to the ZyWALL periodically if you have subscribed for IDP service.

You need to create an account at myZyXEL.com, register your ZyWALL and then subscribe for IDP service in order to be able to download new packet inspection signatures from myZyXEL.com (see the **Registration** screen). Use the **Update** screen to schedule or immediately download IDP signatures.

See the **IDP > General > Update** to display the following screen.

Figure 239 IDP Update

The following table describes the fields in this screen.

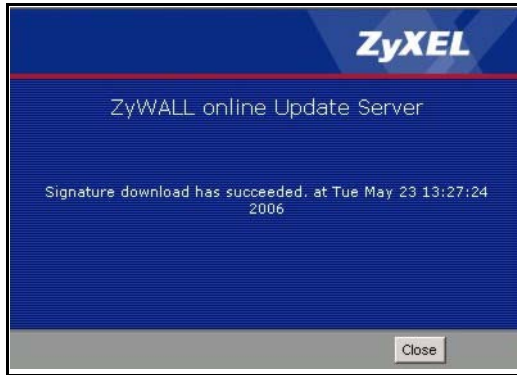
Table 120 IDP Update

LABEL	DESCRIPTION
Signature Information	The following fields display information on the current signature set that the ZyWALL is using.
Current Version	This field displays the IDP signature and anomaly rule set version number. This number increments as the set is enhanced.
Signature Number	This field displays the number of IDP signatures in this set. This number usually increments as the set is enhanced. Older signatures and rules may be removed if they are no longer applicable or have been supplanted by newer ones.
Released Date	This field displays the date and time the set was released.
Remote Update	Use these fields to have the ZyWALL check for new IDP signatures at myZyXEL.com. If new signatures are found, they are then downloaded to the ZyWALL.
Update Now	Click this button to have the ZyWALL check for new IDP signatures immediately. If there are new ones, the ZyWALL will then download them.
Auto Update	Select this check box to have the ZyWALL automatically check for new IDP signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.
Hourly	Select this option to have the ZyWALL check for new IDP signatures every hour.
Daily	Select this option to have the ZyWALL check for new IDP signatures everyday at the specified time. The time format is the 24 hour clock, so '23' means 11PM for example.
Weekly	Select this option to have the ZyWALL check for new IDP signatures once a week on the day and at the time specified.
Apply	Click this button to save your changes to the ZyWALL.
Reset	Click this button to return the screen to its last-saved settings.

Figure 240 Downloading IDP Signatures



Figure 241 Successful IDP Signature Download



CHAPTER 22

Content Filtering Screens

This chapter covers how to use the content filtering feature to control web access. [See the Content Filter section](#) in the Configuration Overview chapter for related information on these screens.

22.1 Content Filtering Overview

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. It can also block access to specific categories of web site content. You can create different content filtering policies for different addresses, schedules, users or groups and content filtering profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

22.1.1 Content Filtering Policies

A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filtering profile.
- Use address and/or user/group objects to define to whose web access to apply the content filtering profile.
- Apply a content filtering profile that you have custom-tailored.

22.1.2 Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

22.1.2.1 Category-based Blocking

The ZyWALL can block access to particular categories of web site content, such as pornography or racial intolerance.

22.1.2.2 Restrict Web Features

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

22.1.2.3 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 particular keywords.

22.1.3 Content Filtering Configuration Guidelines

You must configure an address object, a schedule object and a filtering profile before you can set up a content filtering policy. When the ZyWALL receives an HTTP request, the content filter searches for a policy that matches the source address and time (schedule). The content filter checks the policies in order (based on the policy numbers). When a matching policy is found, the content filter allows or blocks the request depending on the settings of the filtering profile specified by the policy. Some requests may not match any policy. The ZyWALL allows the request if the default policy is not set to block. The ZyWALL blocks the request if the default policy is set to block.

22.2 Content Filter General Screen

Click **Configuration > Policy > Content Filter > General** to open the **Content Filter General** screen. Use this screen to enable content filtering, view and order your list of content filtering policies, create a denial of access message or specify a redirect URL and check your external web filtering service registration status.

Figure 242 Configuration > Policy > Content Filter > General

The following table describes the labels in this screen.

Table 121 Configuration > Policy > Content Filter > General

LABEL	DESCRIPTION
General Setup	
Enable Content Filter	Select this check box to enable the content filter.
Block web access when no policy is applied	Select this check box to stop users from accessing the Internet by default when their attempted access does not match a content filtering policy.
Policies	This is a list of the configured content filtering policies.
#	This column lists the index numbers of the content filtering policies.
Address	A content filtering policy applies to web access from the IP addresses listed here. any means the content filtering policy applies to all of the web access requests that the ZyWALL receives from any IP address.
Schedule	This column displays the name of the schedule for each content filtering policy. You can define different policies for different time periods. none means the content filtering policy applies all of the time.
User	This column displays the individual or group to which this policy applies. any means the content filtering policy applies to all of the web access requests that the ZyWALL receives from any user.
Filtering Profile	This column displays the name of the content filtering profile that each content filtering policy uses. The content filtering profile defines to which web services, web sites or web site categories access is to be allowed or denied.

Table 121 Configuration > Policy > Content Filter > General (continued)

LABEL	DESCRIPTION
Add	<p>Click the Add icon at the top of the column to create a new content filtering policy at the top of the list.</p> <p>The Active icon shows the entry is enabled. Click this icon to disable the entry.</p> <p>The Inactive icon shows the entry is disabled. Click this icon to enable the entry.</p> <p>Click the Edit icon to go to a screen where you can change the configuration settings of an entry.</p> <p>Click the Remove icon to delete an entry from the list.</p> <p>Click the Move icon, type a number in the move entry dialog box and press [ENTER] to move the entry to the numbered location.</p> <p>Click a content filtering policy's Add icon to create a new content filtering policy above the current line. All other entries below the new entry are pushed down.</p> <p>The ordering of the content filtering policies is important as they are used in the order they are listed. The ZyWALL checks requests for Web sessions against the list of content filtering policies (starting from the first in the list). The ZyWALL's content filtering feature blocks or allows the Web session according to the first matching content filtering policy and does not check any other content filtering policies. The ZyWALL does not perform content filtering on Web session requests that do not match any of the content filtering policies.</p>
Denied Access Message	<p>Enter a message to be displayed when content filtering blocks access to a web page. Use up to 255 characters (0-9a-zA-Z;/?:@&=+\$\._!~*()%). For example, "Access to this web page is not allowed. Please contact the network administrator".</p>
Redirect URL	<p>Enter the URL of the web page to which you want to send users when their web access is blocked by content filtering. The web page you specify here opens in a new frame below the denied access message.</p> <p>Use "http://" followed by up to 255 characters (0-9a-zA-Z;/?:@&=+\$\._!~*()%). For example, http://192.168.1.17/blocked access.</p>
Registration Status	<p>This read-only field displays the status of your content-filtering database service registration.</p> <p>Not Licensed displays if you have not successfully registered and activated the service.</p> <p>Expired displays if your subscription to the service has expired.</p> <p>Licensed displays if you have successfully registered the ZyWALL and activated the service.</p> <p>Note: After you register for content filtering, you can see Section 22.6 on page 382 for how to use the Test Against Web Filtering Server button. When content filtering is active, you should see the web page's category. The query fails if content filtering is not active.</p> <p>You can view content filtering reports after you register the ZyWALL and activate the subscription service in the Registration screen (see Chapter 23 on page 395).</p>

Table 121 Configuration > Policy > Content Filter > General (continued)

LABEL	DESCRIPTION
Registration Type	<p>This read-only field displays what kind of service registration you have for the content-filtering database.</p> <p>Not Licensed displays if you have not successfully registered and activated the service.</p> <p>Standard displays if you have successfully registered the ZyWALL and activated the service.</p> <p>Trial displays if you have successfully registered the ZyWALL and activated the trial service subscription.</p>
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

22.3 Content Filter Policy Screen

Click **Configuration > Policy > Content Filter > General > Add** to open the **Content Filter Policy** screen. Use this screen to configure a content filtering policy. A content filtering policy defines which content filter profile should be applied, when it should be applied, and to whose web access it should be applied.

Figure 243 Configuration > Policy > Content Filter > General > Add I

The screenshot shows a dialog box titled "Configuration". It contains four rows, each with a label on the left and a dropdown menu on the right. The labels and their corresponding dropdown values are: "Schedule" with "Workday", "Address" with "Marketing", "Filtering Profile" with "Workday", and "User / Group" with "ANY". Below these fields are two buttons: "OK" and "Cancel".

The following table describes the labels in this screen.

Table 122 Configuration > Policy > Content Filter > General > Add

LABEL	DESCRIPTION
Schedule	Select a schedule to define when to apply this content filtering policy. You can define different policies for different time periods. For example, you could have one policy that blocks access to certain categories of web sites during working hours and another policy that allows access to certain categories after the work day is over. Use the Object > Schedule screens to configure schedules. Select NONE to have the content filtering policy apply all of the time.
Address	Select the address or address group for which you want to use this policy. Select ANY to have the content filtering policy apply to all of the web access requests that the ZyWALL receives from any IP address.
Filtering Profile	Use the drop-down list box to select the content filtering profile that you want to use for this policy. The content filtering profile defines to which web services, web sites or web site categories access is to be allowed or denied. Use the content filtering Filtering Profiles screens to configure the profiles.
User/Group	Use the drop-down list box to select the individual or group for which you want to use this policy. Use the User/Group screens to configure the lists of individuals and groups. Select ANY to have the content filtering policy apply to all of the web access requests that the ZyWALL receives from any user.
OK	Click OK to save your changes back to the ZyWALL.
Cancel	Click Cancel to begin configuring this screen afresh.

22.4 Content Filtering Profile Screen

Click **Configuration > Policy > Content Filter > Filtering Profile** to open the **Filtering Profile** screen. A content filtering profile defines to which web services, web sites or web site categories access is to be allowed or denied.

Figure 244 Configuration > Policy > Content Filter > Filtering Profile

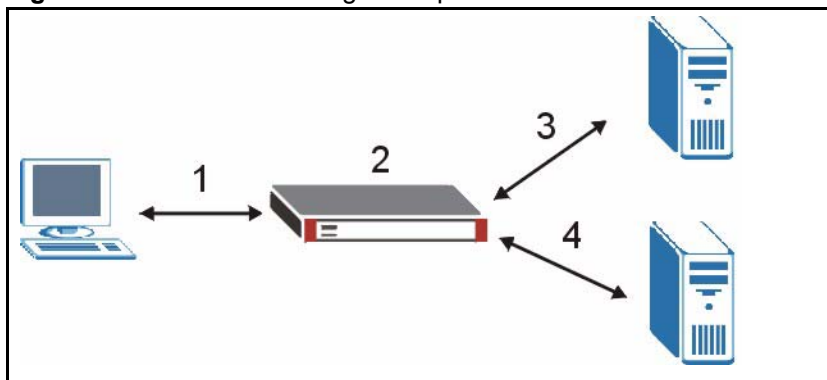
The following table describes the labels in this screen.

Table 123 Configuration > Policy > Content Filter > Filtering Profile

LABEL	DESCRIPTION
#	This column lists the index numbers of the content filtering profiles.
Filtering Profile Name	This column lists the names of the content filtering profiles.
Add	Click the Add icon at the top of the column to create a new content filtering profile at the end of the list. Click a content filtering policy's Add icon at the to create a new content filtering policy below the current line. All other entries below the new entry are pushed down.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

22.5 External Web Filtering Service

When you register for and enable the external web filtering service, 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 245 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 22.9 on page 391](#)). 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 queries the external content filtering database and simultaneously sends the request to the web server.
- 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 based on the settings in the content filtering profile. The web site's address and category are then stored in the ZyWALL's content filtering cache.

22.6 Content Filter Categories Screen

Click **Configuration > Policy > Content Filtering > Filtering Profile > Add** to open the **Categories** screen. Use this screen to enable 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 8 on page 163](#)) 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 23 on page 395](#) for details).

- 1 Log into myZyXEL.com and click your device's link to open it's **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 251 on page 397](#)). Type your myZyXEL.com account password in the **Password** field. Click **Submit**.

Figure 246 Configuration > Policy > Content Filtering > Filtering Profile > Add

The screenshot shows the 'Filtering Profile' configuration window. It has three tabs: 'General', 'Filtering Profile' (selected), and 'Cache'. Under 'Filtering Profile', there are two sub-tabs: 'Categories' and 'Customization'. The 'Name' field contains 'Art'. The 'Auto Web Category Setup' section shows 'External Web Filtering Service Status: Licensed' and 'Enable External Web Filtering Service' checked. Action options for 'Matched Web Pages', 'Unrated Web Pages', and 'When Web Filtering Server Is Unavailable' are all set to 'Block'. The 'Content Filter Service Unavailable Timeout' is set to 10 seconds. The 'Select Categories' section has 'Arts/Entertainment' checked. At the bottom, there is a 'Test Web Site Attribute' section with a text input field and buttons for 'Test Against Local Cache' and 'Test Against Web Filtering Server'. 'OK' and 'Cancel' buttons are at the very bottom.

The following table describes the labels in this screen.

Table 124 Configuration > Policy > Content Filtering > Filtering Profile > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Auto Web Category Setup	
External Web Filtering Service Status	This read-only field displays the status of your external content filtering service registration. Not Licensed displays if you have not successfully registered and activated the service. Expired displays if your subscription to the service has expired. Licensed displays if you have successfully registered the ZyWALL and activated the service.

Table 124 Configuration > Policy > Content Filtering > Filtering Profile > Add (continued)

LABEL	DESCRIPTION
Enable External Web Filtering Service	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 Block 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 Content Filter General screen along with the category of the blocked web page. Select Log to record attempts to access prohibited web pages.
Unrated Web Pages	Select Block to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page. Select Log to record attempts to access web pages that are not categorized.
When Web Filtering Server Is Unavailable	Select Block to block access to any requested web page if the external content filtering database is unavailable. The following are possible causes: There is no response from the external content filtering server within the time period specified in the Content Filter Server Unavailable Timeout field. The ZyWALL is not able to resolve the domain name of the external content filtering database. 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"). Select Log to record attempts to access web pages that occur when the external content filtering database is unavailable.
Content Filter Service Unavailable Timeout	Specify a number of seconds (1 to 60) 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 Block When Content Filter Server Is Unavailable field. This setting applies to all of your content filtering profiles.
Select Categories	
Select All Categories	Select this check box to restrict access to all site categories listed below.
Clear All Categories	Select this check box to clear the selected categories below.
Adult/Mature Content	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.
Pornography	Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
Sex Education	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.

Table 124 Configuration > Policy > Content Filtering > Filtering Profile > Add (continued)

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

Table 124 Configuration > Policy > Content Filtering > Filtering Profile > Add (continued)

LABEL	DESCRIPTION
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.
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.

Table 124 Configuration > Policy > Content Filtering > Filtering Profile > Add (continued)

LABEL	DESCRIPTION
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.
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.

Table 124 Configuration > Policy > Content Filtering > Filtering Profile > Add (continued)

LABEL	DESCRIPTION
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.
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 Advanced to see an expanded list of categories, or click Basic to see a smaller list.
Test Web Site Attribute	
Test if Web site is blocked	You can check which category a web page belongs to. Enter a web site URL in the text box.
Test Against Local Cache	Click this button to see the category recorded in the ZyWALL's content filtering database for the web page you specified (if the database has an entry for it).
Test Against Web Filtering Server	Click this button to see the category recorded in the external content filter server's database for the web page you specified.
OK	Click OK to save your changes back to the ZyWALL.
Cancel	Click Cancel to exit this screen without saving your changes.

22.7 Content Filter Customization Screen

Click **Configuration > Policy > Content Filtering > Filtering Profiles > Customization** to open the **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 247 Configuration > Policy > Content Filtering > Filtering Profiles > Customization

The following table describes the labels in this screen.

Table 125 Configuration > Policy > Content Filtering > Filtering Profiles > Customization

LABEL	DESCRIPTION
Filtering Profile Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Customization Setup	
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.

Table 125 Configuration > Policy > Content Filtering > Filtering Profiles > Customization

LABEL	DESCRIPTION
Allow Web traffic for trusted web sites only	When this box is selected, the ZyWALL blocks Web access to sites that are not on the Trusted Web Sites list. If they are chosen carefully, this is the most effective way to block objectionable material.
Restricted 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.
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.
Allow 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 Trusted Web Sites 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 256 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. Use up to 63 characters (0-9a-z-). The casing does not matter.
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 Trusted Web Site List , 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 256 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 also blocked. For example, entering “bad-site.com” also blocks “www.bad-site.com”, “partner.bad-site.com”, “press.bad-site.com”, etc. Use up to 63 characters (0-9a-z-). The casing does not matter.
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 Forbidden Web Site List , and then click this button to delete it from that list.

Table 125 Configuration > Policy > Content Filtering > Filtering Profiles > Customization

LABEL	DESCRIPTION
Blocked URL Keywords	This section allows you to block Web sites with URLs that contain certain keywords in the domain name or IP address. You can enter up to 256 keywords.
Add Blocked Keyword	Enter a keyword or a numerical IP address to block. You can also enter a numerical IP address. Use up to 63 case-insensitive characters (0-9a-zA-Z;/?:@&+\$. _!~*()% ,). For example enter Bad_Site to block access to any web page that includes the exact phrase Bad_Site. This does not block access to web pages that only include part of the phrase (such as Bad for example).
Blocked URL Keywords	This list displays the keywords already added.
Add	Click this button when you have finished adding the key words field above.
Delete	Select a keyword from the Keyword List , and then click this button to delete it from that list.
OK	Click OK to save your changes back to the ZyWALL.
Cancel	Click Cancel to exit this screen without saving your changes.

22.8 Keyword Blocking URL Checking

The ZyWALL checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is [news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php).

Since the ZyWALL checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the ZyWALL would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path ([news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php)) but it would not find "tw/news".

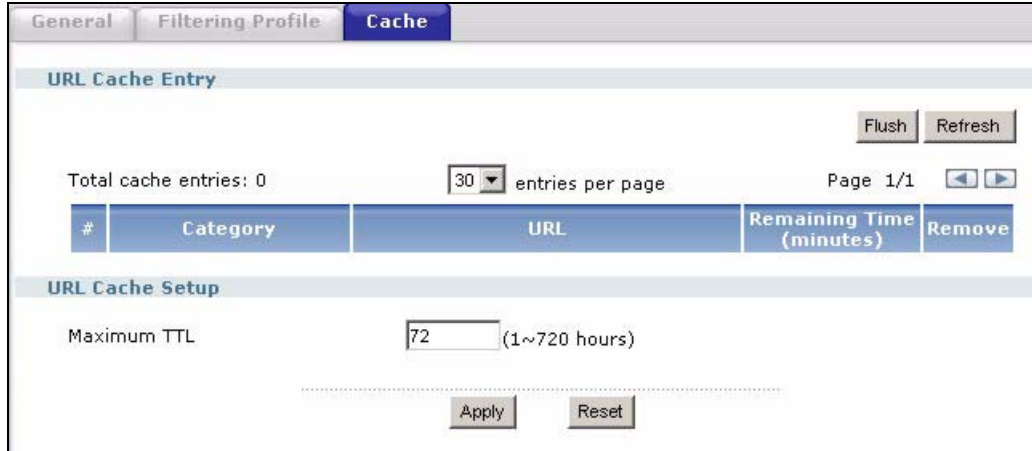
22.9 Content Filter Cache Screen

Click **Configuration > Policy > 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 23.2 on page 400](#) for how to submit a web site that has been incorrectly categorized.

Figure 248 Configuration > Policy > Content Filter > Cache



The following table describes the labels in this screen.

Table 126 Configuration > Policy > Content Filter > Cache

LABEL	DESCRIPTION
URL Cache Entry	
Flush	Click this button to clear all web site addresses from the cache manually.
Refresh	Click this button to reload the list of content filter cache entries.
Total cache entries	This is the number of web site addresses in the content filter cache.
Page	This shows which page number of entries is being displayed and the total number of pages. Click the left or right arrow button to go to the previous or next page.
#	This is the index number of a categorized web site address record.
Category	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.
Remaining Time (minutes)	This is the number of minutes left before the URL entry is discarded from the cache.
Remove	Click the delete icon to remove the URL entry from the cache.
Flush	
Refresh	Click this button to reload the cache.
URL Cache Setup	

Table 126 Configuration > Policy > Content Filter > Cache (continued)

LABEL	DESCRIPTION
Maximum TTL	Type the maximum time to live (TTL) (1 to 720 hours). This sets how long the ZyWALL is to keep an entry in the URL cache before discarding it. The external content filtering database frequently adds previously uncategorized web sites and sometimes changes a web site's category. Setting this limit higher will speed up the processing of web access requests but will also make it take longer for the ZyWALL to reflect changes in the external content filtering database.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 23

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 8 on page 163](#) on how to create a myZyXEL.com account, register your device and activate the subscription services using the **REGISTRATION** screens.

23.1 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).

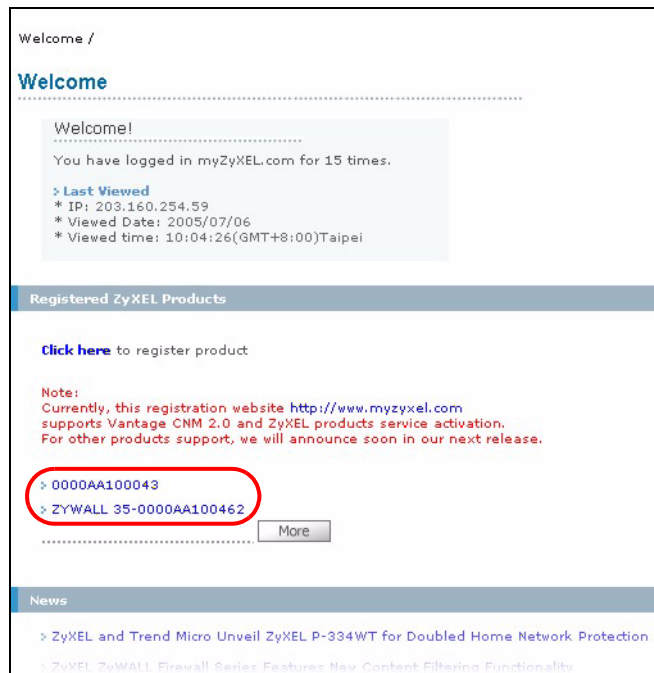
- 1 Go to <http://www.myZyXEL.com>.
- 2 Fill in your myZyXEL.com account information and click **Submit**.

Figure 249 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 251 on page 397](#)).

Figure 250 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 251 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 251 on page 397). Type your myZyXEL.com account password in the **Password** field.

6 Click **Submit**.

Figure 252 Blue Coat: Login

ZyXEL Powered By **Blue Coat** Technical Support

System Login

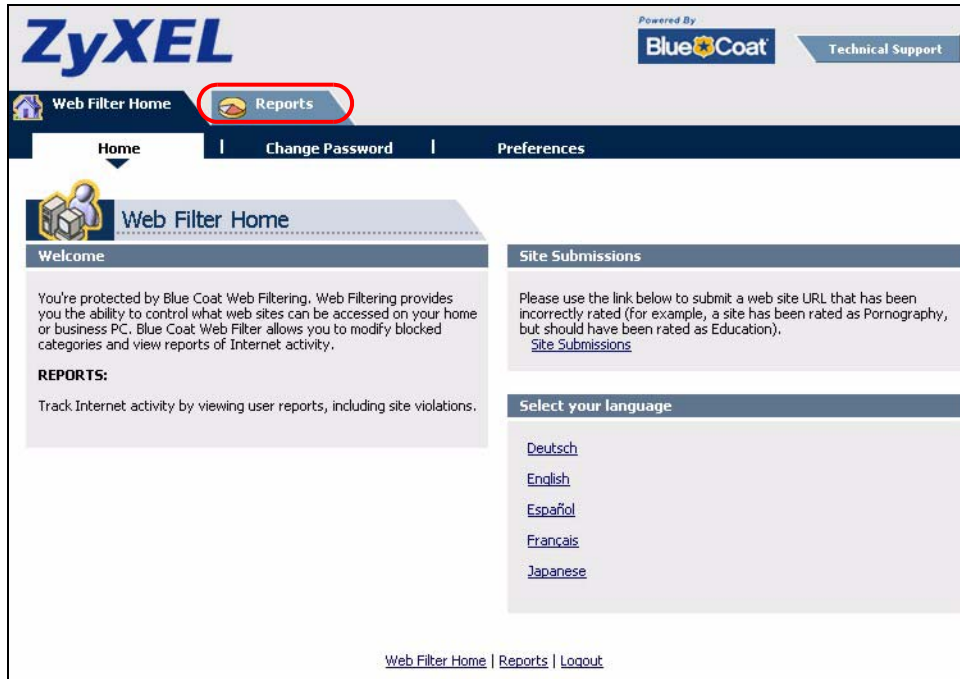
Welcome to your Blue Coat Web Filter Administration site. Please login using your Username and Password.

Name

Password

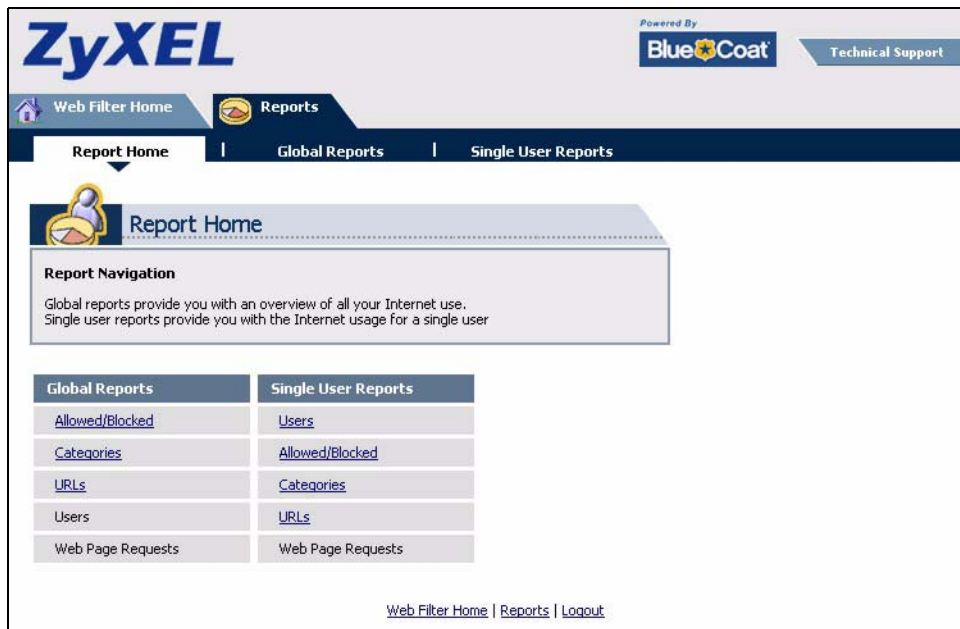
7 In the **Web Filter Home** screen, click the **Reports** tab.

Figure 253 Blue Coat Content Filtering Reports Main Screen



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

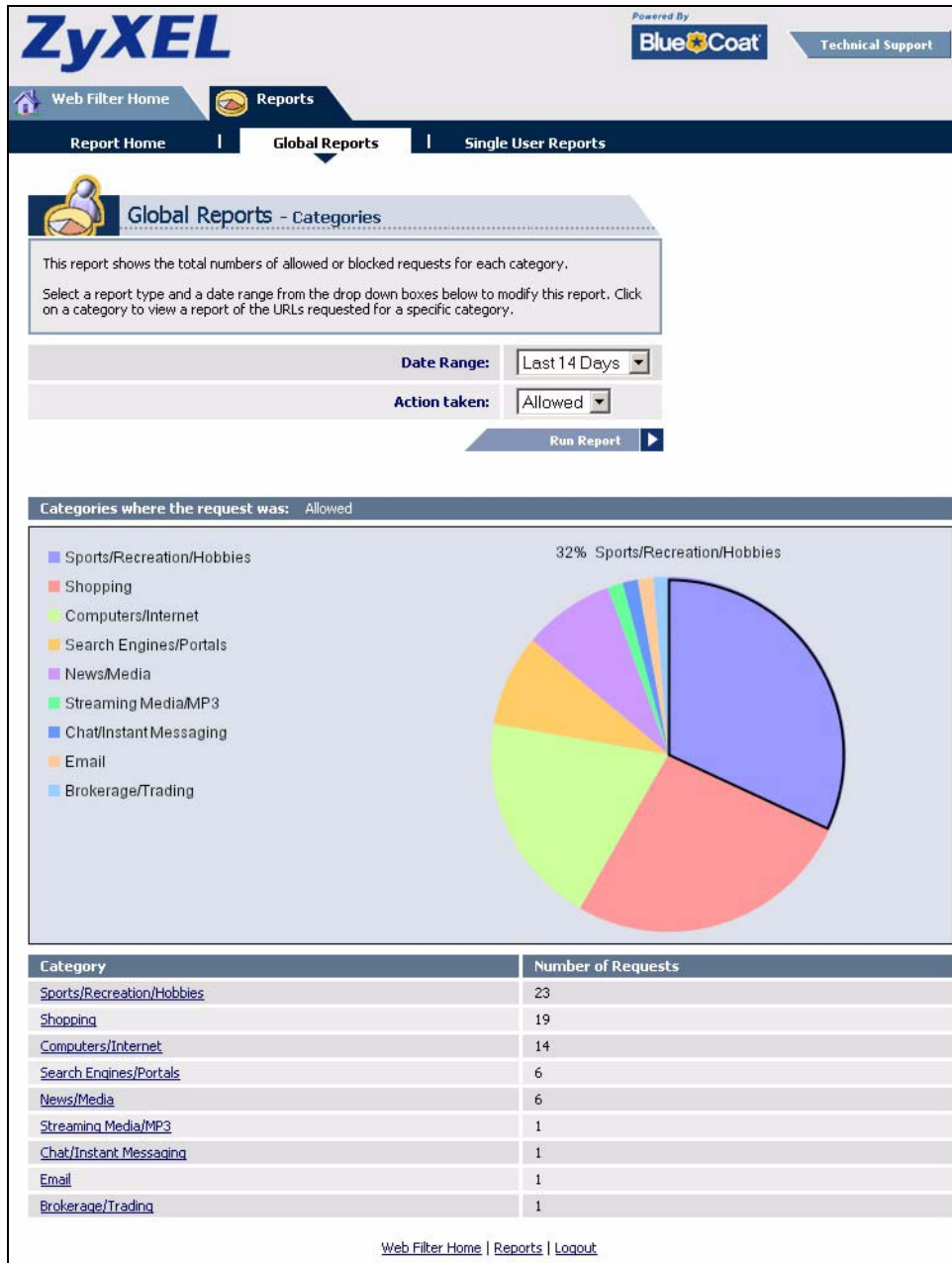
Figure 254 Blue Coat: Report Home



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 255 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 256 Requested URLs Example

Global Reports - URLs

This report displays allowed or blocked URLs requested within a specific category. Click on a URL to view the users that requested that URL.

Date Range: Last 14 Days

Action taken: Allowed

Category: Sports/Recreation/Hobbies

Run Report

URLs Requested for category: Sports/Recreation/Hobbies

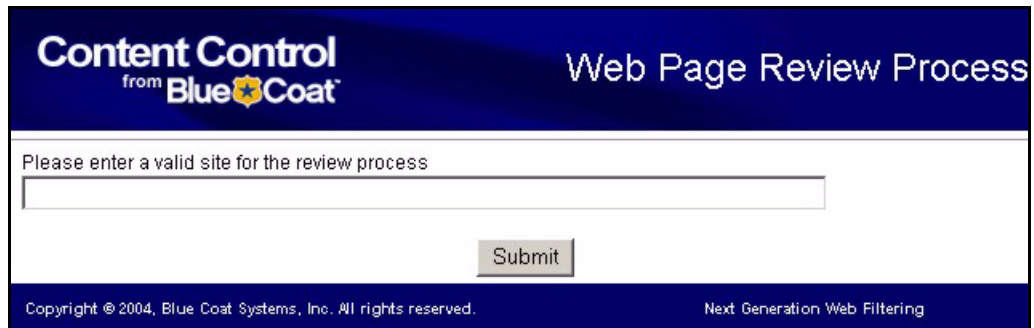
Item #	URL	Number of Requests	Open Web Page
1	adsatt.espn.go.com/insertfiles/javascript/flash.js	1	
2	sports.espn.go.com/crossdomain.xml	1	
3	sports.espn.go.com/sports/tvlistings/fp/headerData	1	
4	espn.go.com/Adserver?CallDown&AdTypes=MotionLogo;	1	
5	espn.go.com/myespn/login3.html	1	
6	broadband.espn.go.com/EBB2/popup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

Web Filter Home | Reports | Logout

23.2 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 23.1 on page 395](#)).
- 2 In the **Web Filter Home** screen (see [Figure 253 on page 398](#)), click **Site Submissions** to open the **Web Page Review Process** screen shown next.

Figure 257 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 24

Virtual Servers

This chapter describes how to set up, manage, and remove virtual servers. First, it provides an overview of virtual servers, and, then, it introduces the virtual server screens and commands. [See the Virtual Server \(Port Forwarding\) section](#) in the Configuration Overview chapter for related information on these screens.

24.1 Virtual Server Overview

Virtual server is also known as port forwarding or port translation.

Virtual servers are computers on a private network behind the ZyWALL that you want to make available outside the private network. If the ZyWALL has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

In the ZyWALL, you set up a virtual server for each forwarding rule. The first part of the virtual server defines the conditions required to forward the packet.

- **Original IP** - the original destination address; it can be an Ethernet, VLAN, bridge, or PPPoE/PPTP interface; a specific IP address; or a HOST address object. (See [Chapter 28 on page 437](#).)
- **Protocol Type** - the protocol [TCP, UDP, or both (**Any**)] used by the service requesting the connection.
- **Original Port(s)** - the original destination port or range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service.

The second part of the virtual server controls where the packet is forwarded if the conditions are satisfied.

- **Mapped IP** - the translated destination address.
- **Mapped Port(s)** - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

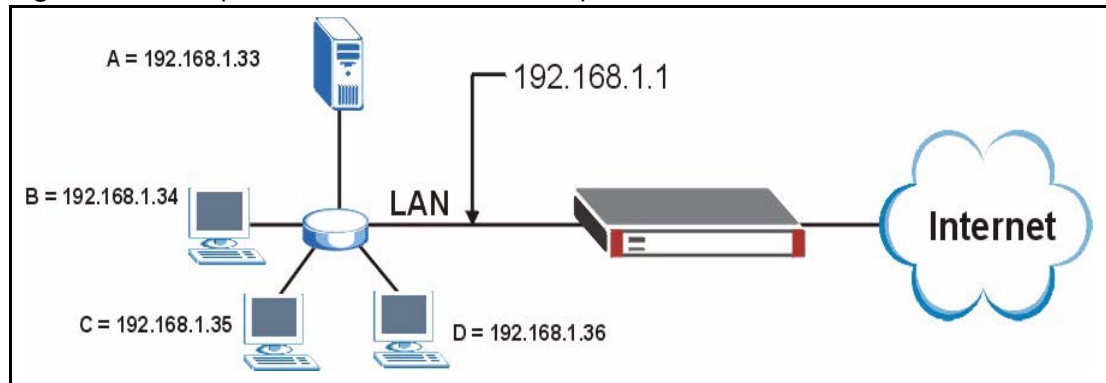
The ZyWALL checks virtual servers before it applies to-ZyWALL firewall rules, so to-ZyWALL firewall rules do not apply to traffic that is forwarded by virtual servers. The ZyWALL still checks regular (through-ZyWALL) firewall rules according to the source IP address and mapped IP address.

Some common port numbers are listed in [Appendix B on page 547](#).

24.2 Virtual Server 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 258 Multiple Servers Behind NAT Example



24.3 Virtual Server Screens




The **Virtual Server** summary screen provides a summary of all virtual servers and their configuration, and the **Virtual Server Add/Edit** screen lets you configure a virtual server.

24.4 Virtual Server Summary Screen

The **Virtual Server** summary screen provides a summary of all virtual servers and their configuration. In addition, this screen allows you to create new virtual servers and edit and delete existing virtual servers.

To access this screen, login to the web configurator. When the main screen appears, click **Policy > Virtual Server**. The following screen appears, providing a summary of the existing virtual servers.

Figure 259 Policy > Virtual Server

Virtual Server								
#	Name	Interface	Original IP	Mapped IP	Protocol	Original Port	Mapped Port	
1	mail_forward	ge4	any	192.168.5.1	any	25	25	  

The following table describes the labels in this screen. See [Section 24.4.1 on page 405](#) below for more information as well.

Table 127 Policy > Virtual Server

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific virtual server.
Name	This field displays the name of the virtual server.
Interface	This field displays the interface on which packets for the virtual server were received.
Original IP	This field displays the original destination IP address (or address object) of packets for the virtual server. It displays any if there is no restriction on the original destination IP address.
Mapped IP	This field displays the new destination IP address for the packet.
Protocol	This field displays the service used by the packets for this virtual server. It displays any if there is no restriction on the services.
Original Port	This field displays the original destination port(s) of packets for the virtual server. This field is blank if there is no restriction on the original destination port.
Mapped Port	This field displays the new destination port(s) for the packet. This field is blank if there is no restriction on the original destination port.
Add icon	<p>This column provides icons to add, edit, and remove virtual servers. In addition, you can activate and deactivate virtual servers.</p> <p>To add a virtual server, click the Add icon at the top of the column. The Virtual Server Add/Edit screen appears.</p> <p>To activate / deactivate a virtual server, click the Active icon next to the virtual server.</p> <p>To edit a virtual server, click the Edit icon next to the virtual server. The Virtual Server Add/Edit screen appears.</p> <p>To delete a virtual server, click on the Remove icon next to the virtual server. The web configurator confirms that you want to delete it before doing so.</p>

24.4.1 Virtual Server Add/Edit

The **Virtual Server Add/Edit** screen lets you create new virtual servers and edit existing ones. To open this window, open the **Virtual Server** summary screen. (See [Section 24.4 on page 404](#).) Then, click on an **Add** icon or **Edit** icon to open the following screen.

Figure 260 Policy > Virtual Server > Edit

The following table describes the labels in this screen.

Table 128 Policy > Virtual Server > Edit

LABEL	DESCRIPTION
Name	Type in the name of the virtual server. The name is used to refer to the virtual server. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Interface	Select the interface on which packets for the virtual server must be received.
Original IP	Use the drop-down list box to indicate which destination IP address this virtual server supports. Choices are: Any - this virtual server supports the IP address of the selected interface. User Defined - this virtual server supports a specific IP address, specified in the User Defined field. HOST address - the drop-down box lists all the HOST address objects in the ZyWALL. If you select one of them, this virtual server supports the IP address specified by the address object.
User Defined	This field is available if Original IP is User Defined . Type the destination IP address that this virtual server supports.
Mapped IP	Type the translated destination IP address, if this virtual server forwards the packet.
Mapping Type	Use the drop-down list box to select how many original destination ports this virtual server supports for the selected destination IP address (Original IP). Choices are: Any - this virtual server supports all the destination ports. Port - this virtual server supports one destination port. Ports - this virtual server supports a range of destination ports.
Protocol Type	This field is available if Mapping Type is Port or Ports . Select the protocol supported by this virtual server. Choices are TCP , UDP , or Any .
Original Port	This field is available if Mapping Type is Port . Enter the original destination port this virtual server supports.
Mapped Port	This field is available if Mapping Type is Port . Enter the translated destination port if this virtual server forwards the packet.
Original Start Port	This field is available if Mapping Type is Ports . Enter the beginning of the range of original destination ports this virtual server supports.

Table 128 Policy > Virtual Server > Edit (continued)

LABEL	DESCRIPTION
Original End Port	This field is available if Mapping Type is Ports . Enter the end of the range of original destination ports this virtual server supports.
Mapped Start Port	This field is available if Mapping Type is Ports . Enter the beginning of the range of translated destination ports if this virtual server forwards the packet.
Mapped End Port	This field is available if Mapping Type is Ports . Enter the end of the range of translated destination ports if this virtual server forwards the packet.
OK	Click OK to save your changes back to the ZyWALL.
Cancel	Click Cancel to return to the Virtual Server summary screen without creating the virtual server (if it is new) or saving any changes (if it already exists).

CHAPTER 25

HTTP Redirect

This chapter shows you how to configure HTTP redirection on your ZyWALL. [See the HTTP Redirect section](#) in the Configuration Overview chapter for related information on these screens.

25.1 HTTP Redirect Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the ZyWALL) to a web proxy server.

25.1.1 Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a firewall or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

A client connects to a web proxy server each time he/she wants to access the Internet. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

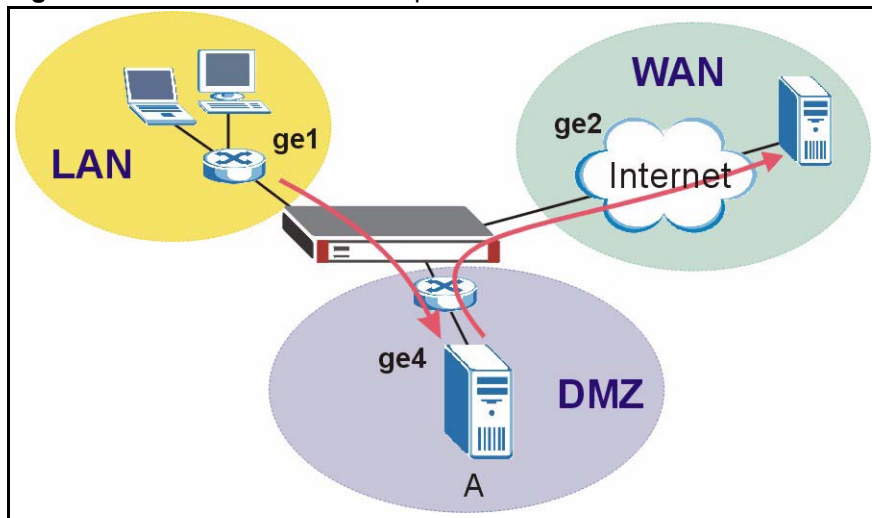
25.2 HTTP Redirect, Firewall and Policy Route

With HTTP redirect, the relevant packet flow for HTTP traffic is:

- 1 Firewall
- 2 Application Patrol
- 3 HTTP Redirect
- 4 Policy Route

Even if you set a policy route to the same incoming interface and service as a HTTP redirect rule, the ZyWALL checks the HTTP redirect rules first and forwards HTTP traffic to a proxy server if matched. You need to make sure there is no firewall rule(s) blocking the HTTP requests from the client to the proxy server.

You also need to manually configure a policy route to forward the HTTP traffic from the proxy server to the Internet.

Figure 261 HTTP Redirect Example

In the example, proxy server **A** is connected to **ge4** in the DMZ zone. When a client connected to **ge1** wants to open a web page, its HTTP request is redirected to proxy server **A** first. If proxy server **A** cannot find the web page in its cache, a policy route allows it to access the Internet to get them from a server. Proxy server **A** then forwards the response to the client.

To make this example work, make sure you have the following settings.

For HTTP traffic between **ge1** and **ge4**:

- a from LAN to WAN through-ZyWALL rule (default) to allow HTTP request from **ge1** to **ge4**. Responses to this request are allowed automatically.
- a application patrol rule to allow HTTP traffic between **ge1** and **ge4**.
- a HTTP redirect rule to forward HTTP traffic from **ge1** to proxy server **A**.

For HTTP traffic between **ge4** and **ge2**:





- a from DMZ to WAN through-ZyWALL rule (default) to allow HTTP request from **ge4** to **ge2**. Responses to this request are allowed automatically.
- a application patrol rule to allow HTTP traffic between **ge4** and **ge2**.
- a policy route to forward HTTP traffic from proxy server **A** to the Internet.

25.3 Configuring HTTP Redirect

To configure redirection of a HTTP request to a proxy server, click **Configuration > Policy > HTTP Redirect**. This screen displays the summary of the HTTP redirect rules.






Note: You can configure up to one HTTP redirect rule for each (incoming) interface.

Figure 262 HTTP Redirect

Configuration				
Name	interface	Proxy Server	Port	
example	ge2	172.20.1.23	80	   

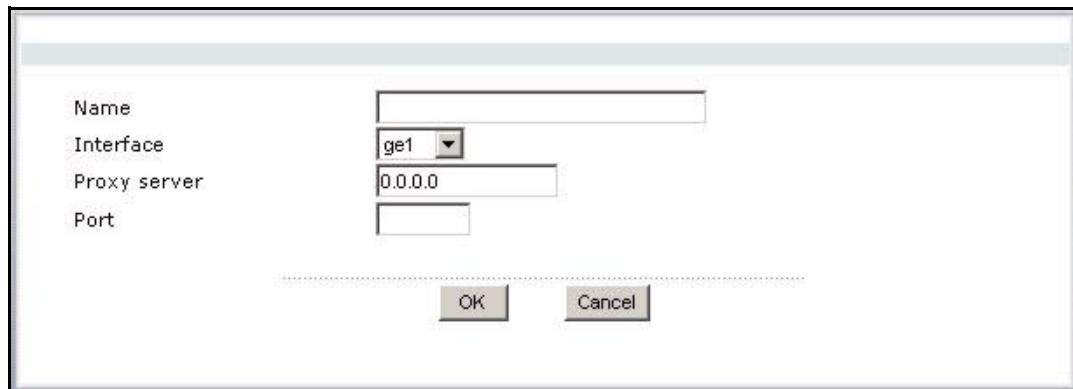
The following table describes the labels in this screen.

Table 129 HTTP Redirect

LABEL	DESCRIPTION
Name	This is the descriptive name (up to 31 printable characters) of a rule.
Interface	This is the interface on which the request must be received.
Proxy Server	This is the IP address of the proxy server.
Port	This is the service port number used by the proxy server.
	Click the Add icon in the heading row to add a new entry.
 	This displays whether the rule is enabled or not. Click the Active icon to activate or deactivate the rule.
	Click the Edit icon to go to the screen where you can edit the rule on the ZyWALL.
	Click the Remove icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule.

25.4 HTTP Redirect Edit

Click **Configuration > Policy > HTTP Redirect** to open the **HTTP Redirect** screen. Then click the **Add** or **Edit** icon to open the **HTTP Redirect Edit** screen where you can configure the rule.

Figure 263 HTTP Redirect Edit

The screenshot shows a web-based configuration interface for editing an HTTP Redirect rule. It features four input fields: a text box for 'Name', a dropdown menu for 'Interface' currently set to 'ge1', a text box for 'Proxy server' containing '0.0.0.0', and an empty text box for 'Port'. At the bottom, there are 'OK' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 130 HTTP Redirect Edit

LABEL	DESCRIPTION
Name	Enter a name to identify this rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Interface	Select the interface on which the HTTP request must be received for the ZyWALL to forward it to the specified proxy server.
Proxy Server	Enter the IP address of the proxy server.
Port	Enter the port number that the proxy server uses.
OK	Click OK to save your changes back to the ZyWALL.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 26

VoIP Pass Through

This chapter covers how to use the ZyWALL's VoIP pass through feature to allow SIP and H.323 VoIP applications to pass through the ZyWALL. See the [VoIP PassThru](#) section in the Configuration Overview chapter for related information on these screens.

26.1 VoIP Pass Through and the ZyWALL

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's NAT.

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 VoIP traffic's data stream. When a device behind the ZyWALL uses an application for which the ZyWALL has VoIP pass through 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 allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

The ZyWALL only needs to use VoIP pass through for traffic that goes through the ZyWALL's NAT. The firewall allows related sessions for VoIP applications that register with a server. The firewall allows or blocks peer to peer VoIP traffic based on the firewall rules.

You do not need to use STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) for VoIP devices behind the ZyWALL when you enable the SIP ALG.

26.1.1 Application Layer Gateway (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 of the ZyWALL's NAT mapping types.

26.1.2 ALG and Trunks

If you send your VoIP traffic through an interface trunk and all of the interfaces are set to active, you can configure routing policies to specify which interface the VoIP traffic uses.

You could also have a trunk with one interface set to active and a second interface set to passive. The ZyWALL does not automatically change the VoIP connection to the second (passive) interface when the active interface's connection goes down. When the active interface's connection fails, the VoIP client needs to re-register through the second interface (that was set to passive) in order to make or receive VoIP calls through that interface. VoIP clients usually re-register automatically at set intervals or the users can manually force them to re-register.

26.1.3 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.

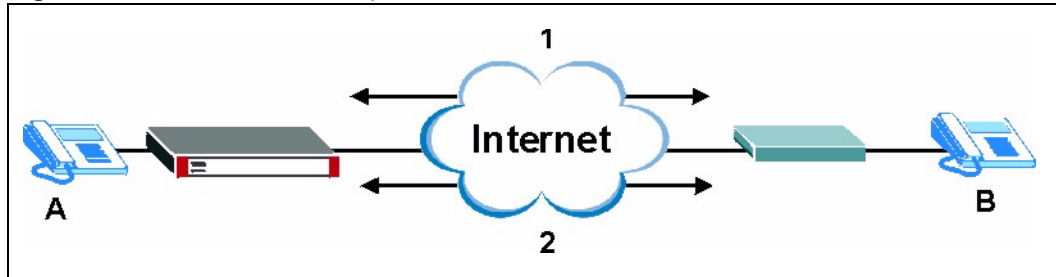
26.1.4 RTP

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.

26.1.4.1 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.
- 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.

The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

Figure 264 H.323 ALG Example

26.1.5 SIP

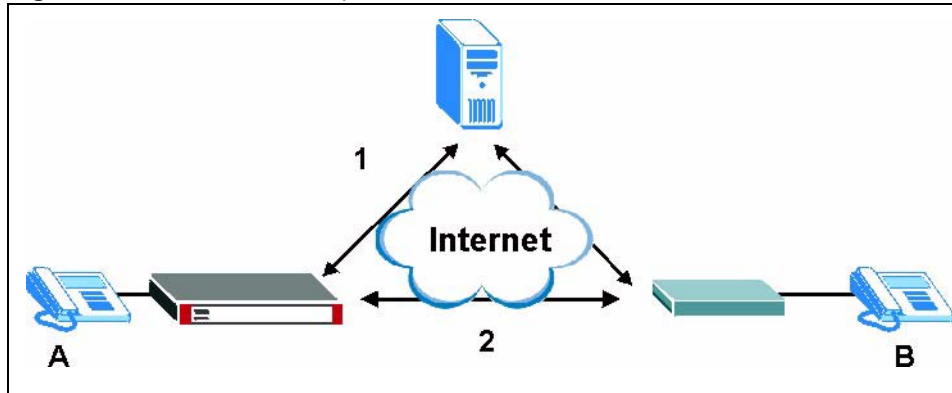
The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

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.

26.1.5.1 SIP ALG Details

- SIP clients can be connected to the LAN or DMZ. A SIP server must be on the WAN.
- Using the SIP ALG allows you to use bandwidth management on SIP traffic.
- The SIP ALG handles SIP calls that go through NAT or that the ZyWALL routes. You can also make other SIP calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The SIP ALG supports peer-to-peer SIP calls. The firewall (by default) allows peer to peer calls from the LAN zone to go to the WAN zone and blocks peer to peer calls from the WAN zone to the LAN zone.
- 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 (1) and audio (2) sessions between SIP clients A and B and the SIP server.

Figure 265 SIP ALG Example

26.1.5.2 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, the ZyWALL SIP ALG deletes the signaling session after the timeout period.

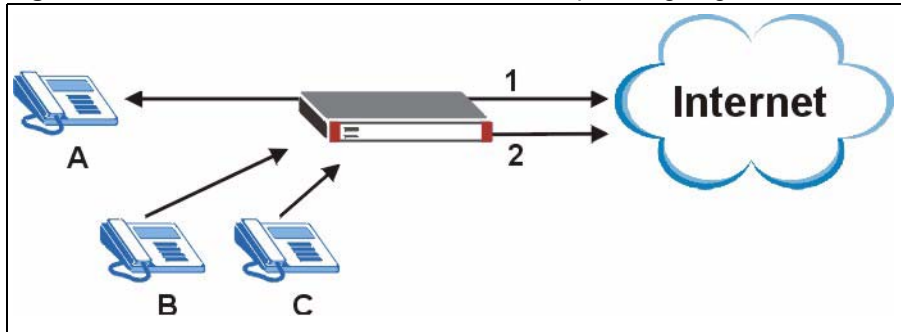
26.2 Peer-to-Peer Calls and the ZyWALL

The ZyWALL ALG can allow peer-to-peer VoIP calls for both H.323 and SIP. You must configure the firewall and virtual server (port forwarding) to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN (or DMZ).

26.2.1 VoIP Calls from the WAN with Multiple Outgoing Calls

When you configure the firewall and virtual server (port forwarding) to allow calls from the WAN to a specific IP address on the LAN, you can also use policy routing to have H.323 (or SIP) calls from other LAN or DMZ IP addresses go out through a different WAN IP address. The policy routing lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

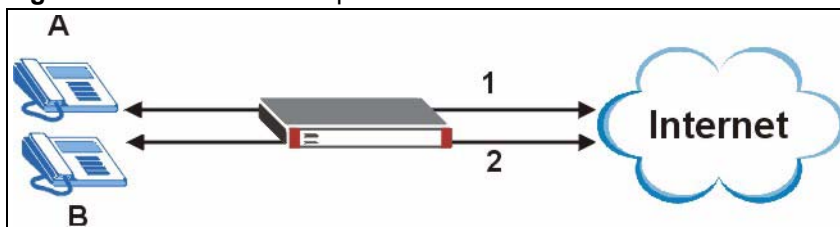
For example, you configure the firewall and virtual server to allow LAN IP address **A** to receive calls from the Internet through WAN IP address **1**. You also use a policy route to have LAN IP address **A** make calls out through WAN IP address **1**. Configure another policy route to have H.323 (or SIP) calls from LAN IP addresses **B** and **C** go out through WAN IP address **2**. Even though only LAN IP address **A** can receive incoming calls from the Internet, LAN IP addresses **B** and **C** can still make calls out to the Internet.

Figure 266 VoIP Calls from the WAN with Multiple Outgoing Calls

26.2.2 VoIP with Multiple WAN IP Addresses

With multiple WAN IP addresses on the ZyWALL, you can configure different firewall and virtual server (port forwarding) rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN (or DMZ). Use policy routing to have the H.323 (or SIP) calls from each of those LAN or DMZ IP addresses go out through the same WAN IP address that calls come in on. The policy routing lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure firewall and virtual server rules to allow LAN IP address **A** to receive calls through public WAN IP address **1**. You configure different firewall and port forwarding rules to allow LAN IP address **B** to receive calls through public WAN IP address **2**. You configure corresponding policy routes to have calls from LAN IP address **A** go out through WAN IP address **1** and calls from LAN IP address **B** go out through WAN IP address **2**.

Figure 267 VoIP with Multiple WAN IP Addresses

26.3 VoIP PassThru Screen

Click **Configuration > Policy > VoIP Passthru** to open the **VoIP PassThru** screen. Use this screen to turn ALGs for SIP and H.323 off or on and configure detailed SIP ALG settings.

Note: You must enable the SIP or H.323 ALG in order to perform bandwidth management on that service's traffic.

Figure 268 Policy > VoIP Passthru

The following table describes the labels in this screen.

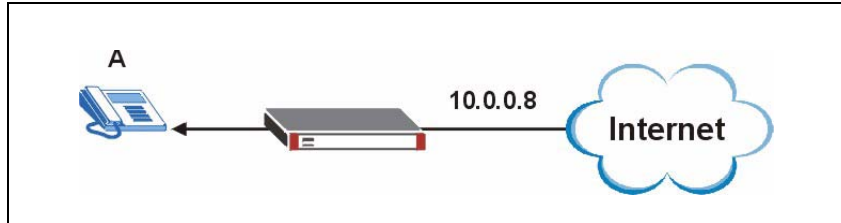
Table 131 Policy > VoIP Passthru

LABEL	DESCRIPTION
Enable SIP Transformations	SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol. Turn on the SIP ALG to allow SIP sessions to pass through the ZyWALL. Using the SIP ALG allows you to use bandwidth management on SIP traffic.
SIP Media inactivity time out	Use this field to set how many seconds (1~86400) the ZyWALL will allow a SIP session to remain idle (without voice traffic) before dropping it. If no voice packets go through the SIP ALG before the timeout period expires, the ZyWALL deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.
SIP Signaling inactivity time out	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, the ZyWALL deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (1~86400).
Additional SIP Signaling port (UDP) for transformations	The ZyWALL’s SIP ALG operates on UDP port 5060 traffic by default. If you are using SIP on another port number, enter the port number here.
Enable H.323 transformations	H.323 is a protocol used for audio communications over networks. Select this check box to turn on the H.323 ALG to allow H.323 sessions to pass through the ZyWALL. Using the H.323 ALG allows you to use bandwidth management on H.323 traffic.
Apply	Click Apply to save your changes back to the ZyWALL.
Cancel	Click Cancel to begin configuring this screen afresh.

26.4 WAN to LAN SIP Peer-to-peer Calls Example

This example shows how to configure firewall and virtual server (port forwarding) rules to allow H.323 calls to come in through WAN IP address 10.0.0.8 to computer A at IP address 192.168.1.56 on the LAN.

Figure 269 WAN to LAN H.323 Peer-to-peer Calls Example



Configure the virtual server policy first to forward H.323 (TCP port 1720) traffic received on the ZyWALL's 10.0.0.8 WAN IP address to LAN IP address 192.168.1.56.

- 1 Click **Policy > Virtual Server > Add**.
- 2 Configure the screen as follows and click **OK**.

Figure 270 Policy > Virtual Server > Add

The screenshot shows a configuration window with the following fields and values:

Name	WAN-LAN_H323
Interface	ge2
Original IP	User Defined
User Defined	10.0.0.8 (IP Address)
Mapped IP	192.168.1.56
Mapping Type	Port
Protocol Type	TCP
Original Port	1720
Mapped Port	1720

At the bottom of the window, there are two buttons: **OK** and **Cancel**.

Configure an address object for the ZyWALL's 10.0.0.8 WAN IP address.

- 3 Click **Object > Address > Add**.
- 4 Configure the screen as follows and click **OK**.

Figure 271 Object > Address > Add

Name: WAN_IP-for-H323
 Address Type: HOST
 IP Address: 10.0.0.8

OK Cancel

Now configure a firewall rule to allow H.323 (TCP port 1720) traffic received on the WAN_IP-for-H323 IP address to go to LAN IP address 192.168.1.56.

- 5** Click **Policy > Firewall**. In **From Zone**, select **WAN**; in **To Zone**, select **LAN**.
- 6** The default rule for WAN-to-LAN traffic drops all traffic. You want to allow SIP access through IP address 10.0.0.8, so add a rule before the default rule. Click the **Add** icon at the top of the column.

Figure 272 Policy > Firewall > WAN to LAN

Global Setting

Enable Firewall
 Allow Asymmetrical Route
 Maximum session per Host: (1-8192)

Firewall rule

Through-ZyWALL rules
 Zone Pairs
 All rules
 To-ZyWALL rules

From Zone		To Zone	
<input type="radio"/> LAN	<input checked="" type="radio"/> WAN	<input checked="" type="radio"/> LAN	<input type="radio"/> WAN
<input type="radio"/> DMZ		<input type="radio"/> DMZ	

#	Priority	Schedule	User	Source	Destination	Service	Access	Log	
1	4	none	any	any	any	any	deny	log	<input checked="" type="checkbox"/>

Apply Reset

- 7** Configure the screen as follows and click **OK**.

Figure 273 Policy > Firewall > WAN > LAN > Add

Configuration

<input checked="" type="checkbox"/> Enable	
From	WAN
To	LAN
Description	WAN-to-LAN_H323 (Optional)
Schedule	none
User	any
Source	any
Destination	WAN_IP-for-H323
Service	H323
Access	allow
Log	no

OK Cancel

CHAPTER 27

User/Group

This chapter describes how to set up user accounts, user groups, and user settings for the ZyWALL. You can also set up rules that control when users have to log in to the ZyWALL before the ZyWALL routes traffic for them. See the [User/Group](#) section in the Configuration Overview chapter for related information on these screens.

27.1 User Account Overview

A user account defines the privileges of a user logged into the ZyWALL. User accounts are used in firewall rules and application patrol, in addition to controlling access to configuration and services in the ZyWALL.

27.1.1 User Types

There are the types of user accounts the ZyWALL uses.

Table 132 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
Admin	Change ZyWALL configuration (web, CLI)	WWW, TELNET, SSH, FTP
Limited-Admin	Look at ZyWALL configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
Access Users		
User	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
Guest	Access network services	WWW
Ext-User	External User Account	WWW

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See [Chapter 32 on page 465](#) for more information about authentication methods.)

27.1.2 Ext-User Accounts

Set up an **Ext-User** account if the user is authenticated by an external server and you want to set up specific policies for this user in the ZyWALL. If you do not want to set up policies for this user, you do not have to set up an **Ext-User** account.

Ext-User users should be authenticated by an external server, such as LDAP or RADIUS. If the ZyWALL tries to use the local database to authenticate an **Ext-User**, the authentication attempt always fails. (This is related to AAA servers and authentication methods, which are discussed in [Chapter 31 on page 455](#) and [Chapter 32 on page 465](#), respectively.)

Note: If the ZyWALL tries to authenticate an **Ext-User** using the local database, the attempt always fails.

Once an **Ext-User** user has been authenticated, the ZyWALL tries to get the user type (see [Table 132 on page 423](#)) from the external server. If the external server does not have the information, the ZyWALL sets the user type for this session to **User**.

For the rest of the user attributes, such as reauthentication time, the ZyWALL checks the following places, in order.

- 1 User account in the remote server.
- 2 User account (Ext-User) in the ZyWALL.
- 3 Default user account for LDAP users (**ldap-users**) or RADIUS users (**radius-users**) in the ZyWALL.

See [Section 27.1.2.1 on page 424](#) for a list of attributes and how to set up the attributes in an external server.

27.1.2.1 Setting up User Attributes in an External Server

To set up user attributes, such as reauthentication time, in LDAP or RADIUS servers, use the following keywords in the user configuration file.

Table 133 LDAP/RADIUS: Keywords for User Attributes

KEYWORD	CORRESPONDING ATTRIBUTE IN WEB CONFIGURATOR
type	User Type. Possible Values: admin, limited-admin, user, guest.
leaseTime	Lease Time. Possible Values: 1-1440 (minutes).
reauthTime	Reauthentication Time. Possible Values: 1-1440 (minutes).

The following examples show you how you might set up user attributes in LDAP and RADIUS servers.

Figure 274 LDAP Example: Keywords for User Attributes

```
type: admin
leaseTime: 99
reauthTime: 199
```


Figure 275 RADIUS Example: Keywords for User Attributes

```
type=user; leaseTime=222; reauthTime=222
```

27.1.2.2 Creating a Large Number of Ext-User Accounts

If you plan to create a large number of **Ext-User** accounts, you might use CLI commands, instead of the web configurator, to create the accounts. Extract the user names from the LDAP or RADIUS server, and create a shell script that creates the user accounts. See [Chapter 9 on page 167](#) for more information about shell scripts.

27.1.3 User Groups

Use user groups when you want to create the same rule for several user accounts, instead of creating separate rules for each one. User groups may consist of user accounts or other user groups, but you cannot put access users and admin users in the same user group.

Note: You cannot put access users and admin users in the same user group.

In addition, you cannot put the default **admin** account into any user group.

Note: You cannot put the default **admin** account into any user group.

The sequence of members in a user group is not important.

27.1.4 Access Users and the ZyWALL

By default, access users do not have to log in to the ZyWALL to use the network services it provides. The ZyWALL automatically routes packets for everyone. In this case, the ZyWALL does not enforce any user-aware policies, but you can still set up policies based on IP address or other criteria.

If you want to enforce user-aware policies, access users must log in to the ZyWALL first. In this case, they should go to the appropriate IP address (or domain name, if you set up DNS) to log in to the ZyWALL. (See [Section 27.5 on page 434](#).) You can provide an incentive to do this by preventing access users from using network services until they log in.

27.1.5 Force User Authentication Policy

Instead of making users to go to the **Login** screen manually, you can configure the ZyWALL to display the **Login** screen automatically whenever it routes HTTP traffic for anyone who has not logged in yet. Then, the ZyWALL can enforce user-aware policies.

Note: This works with HTTP traffic only. The ZyWALL does not force users to log in before it routes other kinds of traffic.

The ZyWALL does not automatically route the request that prompted the login, however, so users have to make this request again.

27.2 User Summary

The **User** screen provides a summary of all user accounts. To access this screen, login to the web configurator, and click **User/Group**.

Figure 276 User/Group

#	User Name	Description	Icons
1	admin	Administration account	[Add] [Edit] [Remove]
2	ldap-users	External LDAP Users	[Add] [Edit] [Remove]
3	radius-users	External RADIUS Users	[Add] [Edit] [Remove]
4	tester	Admin config Read-Only	[Add] [Edit] [Remove]
5	andrew	Local User	[Add] [Edit] [Remove]

The following table describes the labels in this screen.

Table 134 User/Group

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific user.
User Name	This field displays the user name of each user.
Description	This field displays the description for each user.
Add icon	This column provides icons to add, edit, and remove users. To add a user, click the Add icon at the top of the column. The User Add/Edit screen appears. To edit a user, click the Edit icon next to the user. The User Add/Edit screen appears. To delete a user, click the Remove icon next to the user. The web configurator confirms that you want to delete the user before doing so.

27.2.1 User Add/Edit

The **User Add/Edit** screen allows you to create a new user account or edit an existing one. To access this screen, go to the **User** screen (see [Section 27.2 on page 426](#)), and click either the **Add** icon or an **Edit** icon.

Figure 277 User/Group > User > Edit

The following table describes the labels in this screen.

Table 135 User/Group > User > Edit

LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved. See Section 27.2.1.1 on page 428 .
User Type	Select what type of user this is. Choices are: <ul style="list-style-type: none"> • Admin - this user can look at and change the configuration of the ZyWALL • Limited-Admin - this user can look at the configuration of the ZyWALL but not to change it • User - this user has access to the ZyWALL's services but cannot look at the configuration • Guest - this user has access to the ZyWALL's services but cannot look at the configuration • Ext-User - this user account is maintained in a remote server, such as RADIUS or LDAP. See Section 27.1.2 on page 423 for more information about this type.
Password	Select this if this user account requires a password. If it does, enter the password in the field on the right. The password can consist of 4 - 30 alphanumeric characters.
Retype	This field is only available if Password is checked. Enter the password again.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.
Lease Time	Enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the web configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 27.4 on page 431), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	Type the number of minutes this user can be logged into the ZyWALL in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike lease time , the user has no opportunity to renew the session without logging out.

27.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]
- - [dashes]

The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not 'bob'.
- User names have to be different than user group names.
- Reserved user names are listed in the following table.




Table 136 Reserved User Names

- | | | | | |
|--------------|------------------|---------|------------|----------|
| • adm | • admin | • any | • bin | • daemon |
| • debug | • devicehaecived | • ftp | • games | • halt |
| • ldap-users | • lp | • mail | • news | • nobody |
| • operator | • radius-users | • root | • shutdown | • sshd |
| • sync | • uucp | • zyxel | | |

27.3 Group Summary

User groups consist of access users and other user groups. You cannot put admin users in user groups. The **Group** screen provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. To access this screen, login to the web configurator, and click **User/Group > Group**.

Figure 278 User/Group > Group

#	Group Name	Description	Member	Add icon
1	EndUsers		tester	  

The following table describes the labels in this screen. See [Section 27.3.1 on page 429](#) for more information as well.

Table 137 User/Group > Group

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific user group.
Group Name	This field displays the name of each user group.
Description	This field displays the description for each user group.
Member	This field lists the members in the user group. Each member is separated by a comma.
Add icon	This column provides icons to add, edit, and remove user groups. To add a user group, click the Add icon at the top of the column. The Group Add/Edit screen appears. To edit a user group, click the Edit icon next to the user group. The Group Add/Edit screen appears. To delete a user group, click the Remove icon next to the user group. The web configurator confirms that you want to delete the user group before doing so. If you delete the group, you do not delete the users in the group.

27.3.1 Group Add/Edit


The **Group Add/Edit** screen allows you to create a new user group or edit an existing one. To access this screen, go to the **Group** screen (see [Section 27.3 on page 428](#)), and click either the **Add** icon or an **Edit** icon.

Figure 279 User/Group > Group > Edit



The following table describes the labels in this screen.

Table 138 User/Group > Group > Edit

LABEL	DESCRIPTION
Name	Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names.
Description	Enter the description of the user group, if any. You can use up to 60 characters, punctuation marks, and spaces.
#	This field is a sequential value, and it is not associated with a specific member in the user group. The sequence of members in the user group is not important.
Member	<p>This field displays the name of each member in the user group. The word in front of the name indicates whether this member is a user or user group.</p> <p>User - this member is a user.</p> <p>Group - this member is another user group.</p> <p>Click the Popup icon to change this member in the group. The following screen appears.</p> <p>Figure 280 User/Group > Group > Edit > Member</p> 
Add icon	<p>This column provides icons to add members to and remove members from the user group.</p> <p>To add a member to the user group, click the Add icon at the top of the column to add the new member at the beginning of the list, or click the Add icon next to an existing member to add the new member after the existing one. The web configurator chooses a new member alphabetically. You can use the Popup icon next to the new member to change this.</p> <p>To remove a member from the user group, click the Remove icon next to the member. The web configurator confirms that you want to remove the member.</p>

27.4 Setting Screen

The **Setting** screen controls default settings, login settings, lockout settings, and other user settings for the ZyWALL. You can also use this screen to specify when users must log in to the ZyWALL before it routes traffic for them.

To access this screen, login to the web configurator, and click **User/Group > Setting**.

Figure 281 User/Group > Setting

The screenshot shows the 'Setting' screen for a user. It is organized into several sections:

- User Default Setting:** Includes 'User Type' (dropdown menu set to 'User'), 'Lease Time' (input field '1440', range '0-1440 minutes, 0 is unlimited'), and 'Reauthentication Time' (input field '1440', range '0-1440 minutes, 0 is unlimited').
- User Logon Setting:** Includes two checkboxes: 'Limit the number of simultaneous logons for administration account' and 'Limit the number of simultaneous logons for access account'. Each has an associated 'Maximum number per...' input field set to '1' with a range of '(1-1024)'. Both checkboxes are currently unchecked.
- User Lockout Setting:** Includes a checkbox 'Enable logon retry limit' (unchecked). Below it are 'Maximum retry count' (input field '5', range '1-99') and 'Lockout period' (input field '30', range '1-65535 minutes').
- User Miscellaneous Settings:** Includes two checkboxes: 'Allow renewing lease time automatically' (unchecked) and 'Enable user idle detection' (unchecked). Below the second checkbox is 'User idle timeout' (input field '3', range '1-60 minutes').
- Force User Authentication Policy:** Shows 'Total Policy: 1' and a 'Policy per page' dropdown set to '30'. It includes a table with the following data:

#	Schedule	Source	Destination	Authenticate	
1	none	VPN_REMOTE_SUBNET	any	force	

At the bottom of the screen are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 139 User/Group > Setting

LABEL	DESCRIPTION
User Default Setting	
User Type	Select the default user type when you create a new user account. You can still change the user type for each user account.

Table 139 User/Group > Setting (continued)

LABEL	DESCRIPTION
Lease Time	Select the default lease time when you create a new user account. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. You can still change the lease time for each user account.
Reauthentication Time	Select the default reauthentication time when you create a new user account. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. You can still change the reauthentication time for each user account.
User Logon Setting	
Limit ... for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when Limit ... for administration account is checked. Type the maximum number of simultaneous logins by each admin user. The number must be between 1 and 1024.
Limit ... for access account	Select this check box if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can login as many times as they want as long as they use different IP addresses.
Maximum number per access account	This field is effective when Limit ... for access account is checked. Type the maximum number of simultaneous logins by each access user. The number must be between 1 and 1024.
User Lockout Setting	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when Enable logon retry limit is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified lockout period . The number must be between 1 and 99.
Lockout period	This field is effective when Enable logon retry limit is checked. Type the number of minutes the user must wait to try to login again, if logon retry limit is enabled and the maximum retry count is reached. This number must be between 1 and 65,535 (about 45.5 days).
User Miscellaneous Setting	
Allow renewing lease time ...	Select this check box if access users can renew lease time automatically, as well as manually, simply by checking the Update lease time automatically check box on their screen.
Enable user idle detection	This is applicable for access users. Select this check box if you want the ZyWALL to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The ZyWALL automatically logs out the access user once the User idle timeout has been reached.
User idle timeout	This is applicable for access users. This field is effective when Enable user idle detection is checked. Type the number of minutes each access user can be logged in and idle before the ZyWALL automatically logs out the access user.

Table 139 User/Group > Setting (continued)

LABEL	DESCRIPTION
Force User Authentication Policy	Use this section to specify when users must log in to the ZyWALL before the ZyWALL routes HTTP traffic for them. Once users have logged in, the ZyWALL can enforce user-aware policies.s This section displays the conditions that are applied, in sequence, to decide what the appropriate action is. By default, users do not have to log in to the ZyWALL.
#	This field is a sequential value, and it is not associated with a specific condition.
Schedule	This field displays the schedule object that specifies when this condition applies. It displays none if this condition always applies.
Source	This field displays the source address object of traffic to which this condition applies. It displays any if this condition applies to traffic from all source addresses.
Destination	This field displays the destination address object of traffic to which this condition applies. It displays any if this condition applies to traffic from all destination addresses.
Authenticate	This field displays whether users must log in (force) or whether users do not have to log in (skip) when this condition is checked and satisfied.
Add icon	This column provides icons to add, edit, move, and remove conditions. It also provides icons to activate and deactivate conditions. To add a condition, click the Add icon at the top of the column or next to each condition. If you click the one at the top of the column, the new condition is first in the list. If you click the one next to a condition, the new condition appears right below this condition. To edit a condition, click the Edit icon at the top of the column or next to each condition. The Force User Authentication Policy Add/Edit screen appears. To remove a condition, click on the Remove icon next to the condition. The web configurator confirms that you want to delete the condition before doing so. To move a condition up or down in the list, click on the Move to N icon next to the condition, and type the line number (# field) where you want to move this condition. The # field is updated accordingly. To activate or deactivate

27.4.1 Force User Authentication Policy Add/Edit

Use this screen to specify a condition when users must log in or do not have to log in to the ZyWALL before their HTTP traffic can pass through the ZyWALL.

Figure 282 User/Group > Setting > Force User Authentication Policy > add/edit

The following table describes the labels in this screen.

Table 140 User/Group > Setting > Force User Authentication Policy > add/edit

LABEL	DESCRIPTION
Enable	Select this if you want this condition to be active.
Description	Enter a description for this condition. It can be up to 60 printable ASCII characters long.
Authentication	Select whether users must log in (force) or whether users do not have to log in (skip) when this condition is checked and satisfied.
Source Address	Select the source address of traffic to which this condition applies. Select any if this condition applies to traffic from all source addresses.
Destination Address	Select the destination address of traffic to which this condition applies. Select any if this condition applies to traffic from all destination addresses.
Schedule	Select the schedule object that specifies when this condition applies. Select none if this condition always applies.
OK	Select this to save your changes and return to the previous screen.
Cancel	Select this to return to the previous screen without saving any changes.

27.5 Web Configurator for Non-Admin Users

Access users cannot use the Web configurator to browse the configuration of the ZyWALL. Instead, when access users log in to the ZyWALL (forced in the screen as shown in [Figure 281 on page 431](#) or otherwise), the following screen appears.

Figure 283 Web Configurator for Non-Admin Users

The following table describes the labels in this screen.

Table 141 Web Configurator for Non-Admin Users

LABEL	DESCRIPTION
User-defined lease time (max ... minutes)	Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified.
Renew	Access users can click this button to reset the lease time, the amount of time remaining before the ZyWALL automatically logs them out. The ZyWALL sets this amount of time according to the <ul style="list-style-type: none"> • User-defined lease time field in this screen • Lease time field in the User Add/Edit screen (see Section 27.2.1 on page 426) • Lease time field in the Setting screen (see Section 27.4 on page 431)
Updating lease time automatically	This box appears if you checked the Allow renewing lease time automatically box in the Setting screen. (See Section 27.4 on page 431 .) Access users can select this check box to reset the lease time automatically 30 seconds before it expires. Otherwise, access users have to click the Renew button to reset the lease time.
Remaining time before lease timeout	This field displays the amount of lease time that remains, though the user might be able to reset it.
Remaining time before auth. timeout	This field displays the amount of time that remains before the ZyWALL automatically logs the access user out, regardless of the lease time.

CHAPTER 28

Addresses

This chapter describes how to set up addresses and address groups for the ZyWALL. [See the Objects section](#) in the Configuration Overview chapter for related information on these screens.

28.1 Address Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

Address objects and address groups are used in dynamic routes, firewall rules, application patrol, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

28.2 Address Screens

The address screens are used to create, maintain, and remove addresses. There are the types of address objects.













- **HOST** - a host address is defined by an **IP Address**.
- **RANGE** - a range address is defined by a **Starting IP Address** and an **Ending IP Address**.
- **SUBNET** - a network address is defined by a **Network IP address** and **Netmask** subnet mask.

There are two different screens, the **Address** summary screen and the **Address Add/Edit** screen.

28.2.1 Address Summary

The **Address** screen provides a summary of all addresses in the ZyWALL. To access this screen, click **Object > Address > Address**.

Figure 284 Object > Address > Address

Address		Address Group		
Configuration				
#	Name	Type	Address	
1	LAN_SUBNET	SUBNET	192.168.10.0/24	  
2	REMOTE_SUBNET	SUBNET	192.168.1.0/24	  
3	VPN_LOCAL_SUBNET	SUBNET	192.168.10.0/24	  
4	VPN_REMOTE_SUBNET	SUBNET	192.168.1.0/24	  

The following table describes the labels in this screen. See [Section 28.2.2 on page 438](#) for more information as well.

Table 142 Object > Address > Address

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific address.
Name	This field displays the name of each address.
Type	This field displays the type of each address.
Address	This field displays the IP addresses represented by each address object.
Add icon	<p>This column provides icons to add, edit, and remove addresses.</p> <p>To add an address, click the Add icon at the top of the column. The Address Add/Edit screen appears.</p> <p>To edit an address, click the Edit icon next to the address. The Address Add/Edit screen appears.</p> <p>To delete an address, click on the Remove icon next to the address. The web configurator confirms that you want to delete the address before doing so.</p>

28.2.2 Address Add/Edit

The **Address Add/Edit** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see [Section 28.2.1 on page 437](#)), and click either the **Add** icon or an **Edit** icon.

Figure 285 Object > Address > Address > Edit

Name	LAN_SUBNET
Address Type	SUBNET
Network	192.168.10.0
Netmask	255.255.255.0
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

Table 143 Object > Address > Address > Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Address Type	Select the type of address you want to create. Choices are: HOST , RANGE , and SUBNET .
IP Address	This field is only available if the Address Type is HOST . This field cannot be blank. Enter the IP address that this address object represents.
Starting IP Address	This field is only available if the Address Type is RANGE . This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
Ending IP Address	This field is only available if the Address Type is RANGE . This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network	This field is only available if the Address Type is SUBNET , in which case this field cannot be blank. Enter the IP address of the network that this address object represents.
Netmask	This field is only available if the Address Type is SUBNET , in which case this field cannot be blank. Enter the subnet mask of the network that this address object represents. Use dotted decimal format.

28.3 Address Group Screens

Use the **Address Group** summary screen and the **Address Group Add/Edit** screen, to maintain address groups in the ZyWALL.

28.3.1 Address Group Summary

The **Address Group** screen provides a summary of all address groups. To access this screen, click **Object > Address > Address Group**.

Figure 286 Object > Address > Address Group

The following table describes the labels in this screen. See [Section 28.3.2 on page 440](#) for more information as well.

Table 144 Object > Address > Address Group

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.
Add icon	This column provides icons to add, edit, and remove address groups. To add an address group, click the Add icon at the top of the column. The Address Group Add/Edit screen appears. To edit an address group, click the Edit icon next to the address group. The Address Group Add/Edit screen appears. To delete an address group, click on the Remove icon next to the address group. The web configurator confirms that you want to delete the address group.

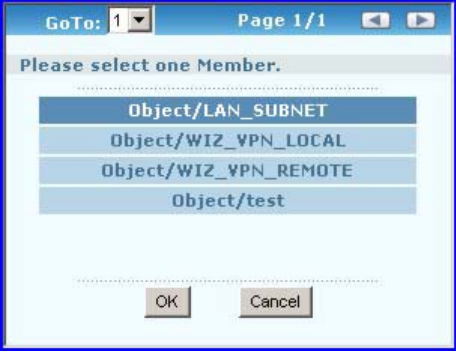
28.3.2 Address Group Add/Edit

The **Address Group Add/Edit** screen allows you to create a new address group or edit an existing one. To access this screen, go to the **Address Group** screen (see [Section 28.3.1 on page 439](#)), and click either the **Add** icon or an **Edit** icon.

Figure 287 Objects > Address > Address Group > Edit

The following table describes the labels in this screen.

Table 145 Object > Address > Address Group > Edit

LABEL	DESCRIPTION
Name	This field displays the name of each address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	This field displays the description of each address group, if any. You can use up to 60 characters, punctuation marks, and spaces.
#	This field is a sequential value, and it is not associated with a specific member in the address group.
Member List	<p>This field displays the name of each member in the address group. The word in front of the name indicates whether this member is an address object or address group.</p> <p>Object - this member is an address object.</p> <p>Group - this member is another address group object.</p> <p>Click the Popup icon to change this member in the group. The following screen appears.</p> <p>Figure 288 Object > Address > Address Group > Member</p> 
Add icon	<p>This column provides icons to add members to and remove members from the address group.</p> <p>To add a member to the address group, click the Add icon at the top of the column to add the new member at the beginning of the list, or click the Add icon next to an existing member to add the new member after the existing one. The web configurator chooses a new member alphabetically. You can use the Popup icon next to the new member to change this.</p> <p>To remove a member from the address group, click on the Remove icon next to the member. The web configurator confirms that you want to remove the member.</p>

CHAPTER 29

Services

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features. [See the Objects section](#) in the Configuration Overview chapter for related information on these screens.

29.1 Services Overview

See [Appendix B on page 547](#) for a list of commonly-used services.

29.1.1 IP Protocols

IP protocols are based on the eight-bit protocol field in the IP header. This field represents the next-level protocol that is sent in this packet. This section discusses three of the most common IP protocols.

Computers use Transmission Control Protocol (TCP, IP protocol 6) and User Datagram Protocol (UDP, IP protocol 17) to exchange data with each other. TCP guarantees reliable delivery but is slower and more complex. Some uses are FTP, HTTP, SMTP, and TELNET. UDP is simpler and faster but is less reliable. Some uses are DHCP, DNS, RIP, and SNMP.

TCP creates connections between computers to exchange data. Once the connection is established, the computers exchange data. If data arrives out of sequence or is missing, TCP puts it in sequence or waits for the data to be re-transmitted. Then, the connection is terminated.

In contrast, computers use UDP to send short messages to each other. There is no guarantee that the messages arrive in sequence or that the messages arrive at all.

Both TCP and UDP use ports to identify the source and destination. Each port is a 16-bit number. Some port numbers have been standardized and are used by low-level system processes; many others have no particular meaning.

Unlike TCP and UDP, Internet Control Message Protocol (ICMP, IP protocol 1) is mainly used to send error messages or to investigate problems. For example, ICMP is used to send the response if a computer cannot be reached. Another use is ping. ICMP does not guarantee delivery, but networks often treat ICMP messages differently, sometimes looking at the message itself to decide where to send it.

29.1.2 Service Objects and Service Groups

Use service objects to define IP protocols.

- TCP applications
- UDP applications
- ICMP messages
- user-defined services (for other types of IP protocols)

These objects are used in policy routes, firewall rules, and IDP profiles.

Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

29.2 Service Summary Screen

The **Service** summary screen provides a summary of all services and their definition. In addition, this screen allows you to add, edit, and remove services.

To access this screen, log in to the web configurator, and click **Object > Service > Service**.

Figure 289 Object > Service > Service

#	Name	Content	
61	SSH_UDP	UDP=22	
62	STRMWORKS	UDP=1558	
63	SYSLOG	UDP=514	
64	TACACS	UDP=49	
65	TELNET	TCP=23	
66	TFTP	UDP=69	
67	VDOLIVE	TCP=7000	
68	ICMP_Echo_Reply	ICMP/echo-reply	

The following table describes the labels in this screen.

Table 146 Object > Service > Service

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific service.
Name	This field displays the name of each service.

Table 146 Object > Service > Service (continued)

LABEL	DESCRIPTION
Content	This field displays a description of each service.
Add icon	This column provides icons to add, edit, and remove services. To add a service, click the Add icon at the top of the column. The Service Add/Edit screen appears. To edit a service, click the Edit icon next to the service. The Service Add/Edit screen appears. To delete a service, click the Remove icon next to the service. The web configurator confirms that you want to delete the service before doing so.

29.2.1 Service Add/Edit

The **Service Add/Edit** screen allows you to create a new service or edit an existing one. To access this screen, go to the **Service** screen (see [Section 29.2 on page 444](#)), and click either the **Add** icon or an **Edit** icon.

Figure 290 Object > Service > Service > Edit

The following table describes the labels in this screen.

Table 147 Object > Service > Service > Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IP Protocol	Select the protocol the service uses. Choices are: TCP , UDP , ICMP , and User Defined .
	These fields appear if the IP Protocol is TCP or UDP .
Starting Port Destination Port	Specify the port number(s) used by this service. If you fill in one of these fields, the service uses that port. If you fill in both fields, the service uses the range of ports.
	These fields appear if the IP Protocol is ICMP Type .
ICMP Type	Select the ICMP message used by this service. This field displays the message text, not the message number.
	These fields appear if the IP Protocol is User Defined .
IP Protocol Number	Enter the number of the next-level protocol (IP protocol). Allowed values are 1 - 255.

29.3 Service Group Summary Screen

The **Service Group** summary screen provides a summary of all service groups. In addition, this screen allows you to add, edit, and remove service groups.

To access this screen, log in to the web configurator, and click **Object > Service > Service Group**.

Figure 291 Object > Service > Service Group

#	Name	Description	Add icon
1	CU-SEEME		[Add] [Edit] [Delete]
2	DNS		[Add] [Edit] [Delete]
3	IRC		[Add] [Edit] [Delete]
4	NetBIOS		[Add] [Edit] [Delete]
5	ROADRUNNER		[Add] [Edit] [Delete]
6	RTSP		[Add] [Edit] [Delete]
7	SNMP		[Add] [Edit] [Delete]
8	SNMP-TRAPS		[Add] [Edit] [Delete]
9	SSH		[Add] [Edit] [Delete]

The following table describes the labels in this screen. See [Section 29.3.1 on page 446](#) for more information as well.

Table 148 Object > Service > Service Group

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific service group.
Name	This field displays the name of each service group.
Description	This field displays the description of each service group, if any.
Add icon	<p>This column provides icons to add, edit, and remove service groups.</p> <p>To add a service group, click the Add icon at the top of the column. The Service Group Add/Edit screen appears.</p> <p>To edit a service group, click the Edit icon next to the service group. The Service Group Add/Edit screen appears.</p> <p>To delete a service group, click on the Remove icon next to the service group. The web configurator confirms that you want to delete the service group.</p>

29.3.1 Service Group Add/Edit

The **Service Group Add/Edit** screen allows you to create a new service group or edit an existing one. To access this screen, go to the **Service Group** screen (see [Section 29.3 on page 446](#)), and click either the **Add** icon or an **Edit** icon.

Figure 292 Object > Service > Service Group > Edit

Configuration

Name:

Description:

#	Member List	
1	Object/NetBIOS_TCP1	
2	Object/NetBIOS_TCP2	
3	Object/NetBIOS_UDP1	
4	Object/NetBIOS_UDP2	


OK Cancel

The following table describes the labels in this screen.

Table 149 Object > Service > Service Group > Edit

LABEL	DESCRIPTION
Name	Enter the name of each service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter the description of each service group, if any. You can use up to 60 printable ASCII characters.
#	This field is a sequential value, and it is not associated with a specific member in the service group. The order of members is not important.

Table 149 Object > Service > Service Group > Edit (continued)

LABEL	DESCRIPTION
Member List	<p>This field displays the name of each member in the service group. The word in front of the name indicates whether this member is a service or service group.</p> <p>Object - this member is a service object.</p> <p>Group - this member is another service group object.</p> <p>Click the Popup icon to change this member in the group. The following screen appears.</p> <p>Figure 293 Object > Service > Service Group > Member</p> 
Add icon	<p>This column provides icons to add members to and remove members from the service group.</p> <p>To add a member to the service group, click the Add icon at the top of the column to add the new member at the beginning of the list, or click the Add icon next to an existing member to add the new member after the existing one. The web configurator chooses a new member automatically. You can use the Popup icon next to the new member to change this.</p> <p>To remove a member from the service group, click on the Remove icon next to the member. The web configurator confirms that you want to remove the member.</p>

CHAPTER 30

Schedules

Use schedules to set up one-time and recurring schedules for policy routes, firewall rules, application patrol, and content filtering. [See the Objects section](#) in the Configuration Overview chapter for related information on these screens.

30.1 Schedule Overview

The ZyWALL supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the ZyWALL. See [Section 34.3 on page 490](#) for information about the current date and time.

Note: Schedules are based on the current date and time in the ZyWALL.

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.









30.2 Schedule Screens

Use the **Schedule** summary screen and the **Schedule Add/Edit** screen to maintain schedules in the ZyWALL.

30.2.1 Schedule Summary

The **Schedule** summary screen provides a summary of all schedules in the ZyWALL. To access this screen, click **Object > Schedule**.

Figure 294 Configuration > Object > Schedule

One Time				
#	Name	Start Day/Time	Stop Day/Time	
Recurring				
#	Name	Start Time	Stop Time	
1	WORK_DAY	08:00	19:00	 
2	OFF_WORK1	00:00	07:59	 
3	OFF_WORK2	19:01	23:59	 

The following table describes the labels in this screen. See [Section 30.2.2 on page 451](#) and [Section 30.2.3 on page 452](#) for more information as well.

Table 150 Configuration > Object > Schedule

LABEL	DESCRIPTION
One Time	
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Day / Time	This field displays the date and time at which the schedule begins.
Stop Day / Time	This field displays the date and time at which the schedule ends.
Add icon	This column provides icons to add, edit, and remove schedules. To add a schedule, click the Add icon at the top of the column. The Schedule Add/Edit screen appears. To edit a schedule, click the Edit icon next to the schedule. The Schedule Add/Edit screen appears. To delete a schedule, click the Remove icon next to the schedule. The web configurator confirms that you want to delete the schedule before doing so.
Recurring	
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Time	This field displays the time at which the schedule begins.
Stop Time	This field displays the time at which the schedule ends.
Add icon	This column provides icons to add, edit, and remove schedules. To add a schedule, click the Add icon at the top of the column. The Schedule Add/Edit screen appears. To edit a schedule, click the Edit icon next to the schedule. The Schedule Add/Edit screen appears. To delete a schedule, click the Remove icon next to the schedule. The web configurator confirms that you want to delete the schedule before doing so.

30.2.2 One-Time Schedule Add/Edit

The **One-Time Schedule Add/Edit** screen allows you to define a one-time schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see [Section 30.2.1 on page 449](#)), and click either the **Add** icon or an **Edit** icon in the **One Time** section.

Figure 295 Configuration > Object > Schedule > One Time_1

Configuration					
Name	<input type="text"/>				
Day Time					
Item #	Day			Time	
	Year	Month	Day	Hour	minute
Start	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Stop	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

The following table describes the labels in this screen.

Table 151 Configuration > Object > Schedule > One Time_1

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the one-time schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Day Time	
Start	Type the year, month, day, hour, and minute when the schedule begins. year - 1900 - 2999 month - 1 - 12 day - 1 - 31 (it is not possible to specify illegal dates, such as February 31.) hour - 0 - 23 minute - 0 - 59 All of these fields are required.
Stop	Type the year, month, day, hour, and minute when the schedule ends. year - 1900 - 2999 month - 1 - 12 day - 1 - 31 (it is not possible to specify illegal dates, such as February 31.) hour - 0 - 23 minute - 0 - 59 All of these fields are required.

30.2.3 Recurring Schedule Add/Edit

The **Recurring Schedule Add/Edit** screen allows you to define a recurring schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see [Section 30.2.1 on page 449](#)), and click either the **Add** icon or an **Edit** icon in the **Recurring** section.

Figure 296 Configuration > Object > Schedule > Recurring_1

Configuration						
Name	WORK_DAY					
Day Time						
Item #	Day			Time		
	Year	Month	Day	Hour	minute	
Start				08	00	
Stop				19	00	
Weekly						
Week Days	<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday	<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input checked="" type="checkbox"/> Saturday
	<input checked="" type="checkbox"/> Sunday					
<input type="button" value="OK"/> <input type="button" value="Cancel"/>						

The **Year**, **Month**, and **Day** columns are not used in recurring schedules and are disabled in this screen. The following table describes the remaining labels in this screen.

Table 152 Configuration > Object > Schedule > Recurring_1

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Day Time	
Start	Type the hour and minute when the schedule begins each day. year - disabled month - disabled day - disabled hour - 0 - 23 minute - 0 - 59 Both fields are required.
Stop	Type the hour and minute when the schedule ends each day. year - disabled month - disabled day - disabled hour - 0 - 23 minute - 0 - 59 Both fields are required.

Table 152 Configuration > Object > Schedule > Recurring_1 (continued)

LABEL	DESCRIPTION
Weekly	
Weekdays	Select each day of the week the recurring schedule is effective.

CHAPTER 31

AAA Server

This chapter introduces and shows you how to configure the ZyWALL to use external authentication servers.

31.1 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network.

The following lists the types of authentication server the ZyWALL supports.

- Local user database

The ZyWALL uses the built-in local user database to authenticate administrative users logging into the ZyWALL's web configurator or network access users logging into the network through the ZyWALL. You can also use the local user database to authenticate VPN users.

- LDAP (Lightweight Directory Access Protocol)

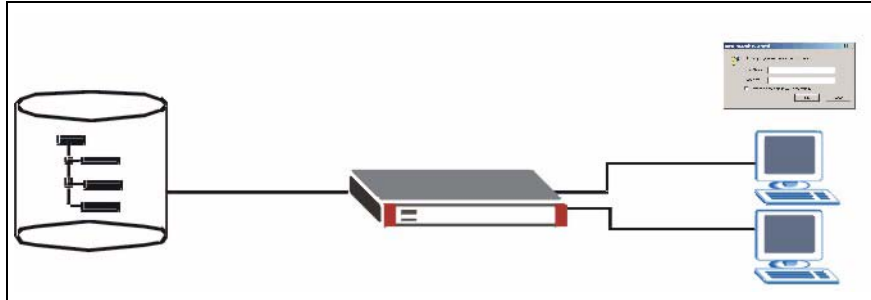
LDAP (Lightweight Directory Access Protocol) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities.

- RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

31.2 LDAP

LDAP allows a client (the ZyWALL) to connect to a server to retrieve information from a directory. A network example is shown next.

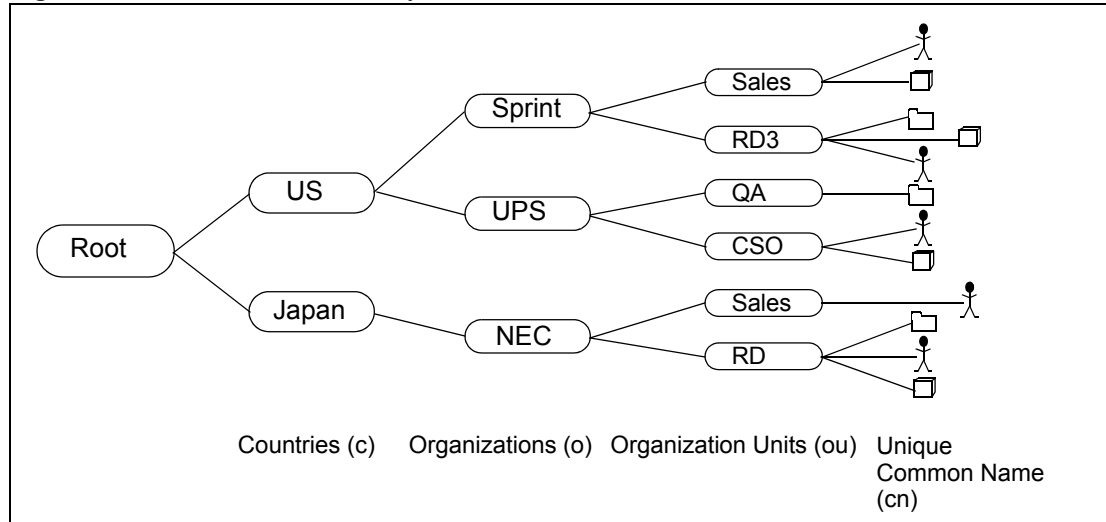
Figure 297 Example: LDAP Client and Server

The following describes the user authentication procedure via an LDAP server.

- 1** The ZyWALL is set to use LDAP authentication for user authentication.
- 2** A user logs in with a user name and password pair.
- 3** The ZyWALL tries to bind (or log in) to the LDAP server.
- 4** When the binding process is successful, the ZyWALL checks the user information in the LDAP directory against the user name and password pair.
- 5** If it matches, the user is allowed access. Otherwise, access is blocked.

31.2.1 LDAP Directory Structure

In LDAP, the directory entries are arranged in a hierarchical order much like a tree structure. Normally, the directory structure reflects the geographical or organizational boundaries. The following figure shows a basic directory structure branching from countries to organizations to organizational units to individuals.

Figure 298 Basic LDAP Directory Structure

31.2.2 Distinguished Name (DN)

A DN uniquely identifies an entry in a directory. A DN consists of attribute-value pairs separated by commas. The leftmost attribute is the Relative Distinguished Name (RDN). This provides a unique name for entries that have the same “parent DN” (“cn=domain1.com, o=MyCompany” in the following examples).

```
cn=domain1.com, o=MyCompany, c=US
cn=domain1.com, o=MyCompany, c=JP
```

31.2.2.1 Base DN

A base DN specifies a directory. A base DN usually contains information such as the name of an organization, a domain name and/or country. For example, o=MyCompany, c=UK where o means organization and c means country.

31.2.2.2 Bind DN

A bind DN is used to authenticate with an LDAP server. For example a bind DN of cn=zywallAdmin allows the ZyWALL to log into the LDAP server using the user name of zywallAdmin. The bind DN is used in conjunction with a bind password. When a bind DN is not specified, the ZyWALL will try to log in as an anonymous user. If the bind password is incorrect, the login will fail.

31.2.3 Configuring LDAP Default

To configure the default LDAP server settings, click **Objects > AAA Server** to display the screen as shown.

Figure 299 Objects: AAA Server: LDAP: Default

The screenshot shows the 'LDAP' configuration screen. At the top, there are tabs for 'LDAP' and 'RADIUS'. Below that, there are sub-tabs for 'Default' and 'Group'. The main area is titled 'Configuration' and contains the following fields:

- Host: [] (IP or FQDN)
- Port: 389 (1..65535)
- Bind DN: [] (Optional)
- Password: [] (Optional)
- Base DN: []
- CN Identifier: uid
- Search time limit: 60 (1~300)
- Use SSL

At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 153 Objects: AAA Server: LDAP: Default

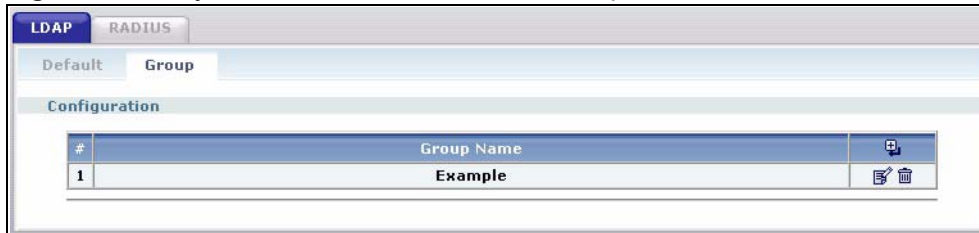
LABEL	DESCRIPTION
Host	Enter the IP address (in dotted decimal notation) or the fully-qualified domain name (up to 63 alphanumerical characters) of an LDAP server.
Port	Specify the port number on the LDAP server to which the ZyWALL sends authentication requests. Enter a number between 1 and 65535. The default is 389 .
Bind DN	Specify the bind DN for logging into the LDAP server. Enter up to 63 alphanumerical characters. For example, <code>cn=zywallAdmin</code> specifies <code>zywallAdmin</code> as the user name.
Password	If required, enter the password (up to 15 alphanumerical characters) for the ZyWALL to bind (or log in) to the LDAP server.
Base DN	Specify the directory (up to 63 alphanumerical characters). For example, <code>o=ZyXEL, c=US</code> .
CN Identifier	Specify the unique common name that uniquely identifies a record in the LDAP directory. Enter up to 63 alphanumerical characters.
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the LDAP server. In this case, user authentication fails. The search timeout occurs when either the user information is not in the LDAP server or the server is down.
Use SSL	Select Use SSL to establish a secure connection to the LDAP server.
Apply	Click Apply to save the changes.
Reset	Click Reset to start configuring this screen again.

31.3 LDAP Group Summary

You can configure a group of LDAP servers in the **LDAP > Group** screen. This is useful if you have more than one LDAP server for user authentication in a network. You can create up to 16 LDAP server groups with up to four members in each group on the ZyWALL.




1 Click **Objects > AAA Server > LDAP > Group** to display the screen.


Figure 300 Objects > AAA Server > LDAP > Group



The following table describes the labels in this screen.

Table 154 Objects > AAA Server > LDAP > Group

LABEL	DESCRIPTION
#	This field displays the index number.
Group Name	This field displays the descriptive name for identification purposes.
	Click  to add a new entry.
	Click  to edit the settings of an entry.
	Click  to delete an entry.

2 Click  to display the configuration fields.

31.3.1 Creating an LDAP Group



Figure 301 Objects > AAA Server > LDAP > Group > Add

The following table describes the labels in this screen.

Table 155 Objects > AAA Server > LDAP > Group > Add

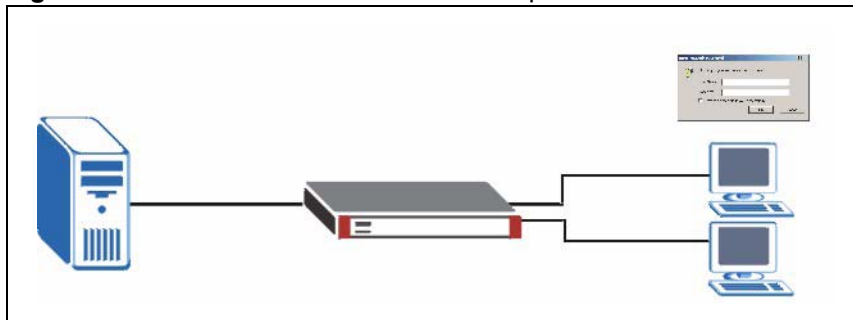
LABEL	DESCRIPTION
Configuration	All LDAP servers in a group share the same settings in the fields below.
Name	Enter a descriptive name (up to 63 alphanumeric characters). for identification purposes.
Port	Specify the port number on the LDAP server(s) to which the ZyWALL sends authentication requests. Enter a number between 1 and 65535. This port number should be the same on all LDAP server(s) in this group.
Password	If required, enter the password (up to 15 alphanumeric characters) the ZyWALL uses to log into the LDAP server(s).
Basedn	Specify the top level directory in the directory. For example, o=ZyXEL, c=US.
binddn	Specify the bind DN for logging into the LDAP server(s). For example, cn=zywallAdmin specifies zywallAdmin as the user name.
CN Identifier	Specify the unique common name that uniquely identifies a record in the LDAP directory. Enter up to 63 alphanumeric characters.
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the LDAP server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the LDAP server(s) or the LDAP server(s) is down.
Use SSL	Select Use SSL to establish a secure connection to the LDAP server(s).
Host Members	The ordering of the LDAP servers is important as the ZyWALL uses the LDAP servers for user authentication in the order they appear in this table.
#	This field displays the index number.

Table 155 Objects > AAA Server > LDAP > Group > Add (continued)

LABEL	DESCRIPTION
Members	Specify the URI (Uniform Resource Identifier) of an LDAP server. You can enter the IP address (in dotted decimal notation) or the fully qualified domain name (FQDN; up to 63 alphanumerical characters) of the LDAP server.
	Click  to add a new LDAP server. You can add up to four LDAP member servers. Click  to delete an LDAP server.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

31.4 RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate a large number of users from a central location.

Figure 302 RADIUS Server Network Example

31.5 Configuring a Default RADIUS Server

To configure the default external RADIUS server to use for user authentication, click **Objects > AAA Server > RADIUS** to display the screen as shown.

Figure 303 Objects > AAA Server > RADIUS > Default

The screenshot shows the configuration page for a RADIUS server. At the top, there are tabs for 'LDAP' and 'RADIUS', with 'RADIUS' selected. Below this, there are sub-tabs for 'Default' and 'Group', with 'Default' selected. The main area is titled 'Configuration' and contains four input fields: 'Host' with the value '192.168.1.200' and a note '(IP or FQDN)', 'Authentication Port' with the value '1812', 'Key' with a masked value '*****', and 'Timeout' with the value '5' and a note '(1~300)'. At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

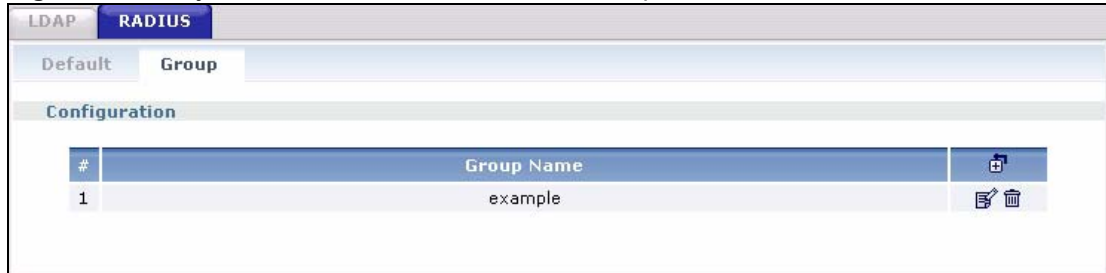
Table 156 Objects > AAA Server > RADIUS > Default

LABEL	DESCRIPTION
Host	Enter the IP address (in dotted decimal notation) or the domain name (up to 63 alphanumeric characters) of a RADIUS server.
Authentication Port	The default port of the RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 15 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 the ZyWALL.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
Apply	Click Apply to save the changes.
Reset	Click Reset to start configuring this screen again.

31.6 Configuring a Group of RADIUS Servers




You can configure a group of RADIUS servers in the **RADIUS > Group** screen. This is useful if you have more than one authentication server for user authentication in a network.


- 1 Click **Objects > AAA Server > RADIUS > Group** to display the screen.

Figure 304 Objects > AAA Server > RADIUS > Group

The following table describes the labels in this screen.

Table 157 Objects > AAA Server > RADIUS > Group

LABEL	DESCRIPTION
#	This field displays the index number.
Group Name	This field displays the descriptive name for identification purposes.
	Click  to add a new entry.
	Click  to edit the settings of an entry.
	Click  to delete an entry.



2 Click  to display the configuration fields.

31.6.1 Adding a RADIUS Server Member

Figure 305 Objects > AAA Server > RADIUS > Group > Add

The following table describes the labels in this screen.

Table 158 Objects > AAA Server > RADIUS > Group > Add

LABEL	DESCRIPTION
Configuration	All RADIUS servers in a group share the same settings in the fields below.
Name	Enter a descriptive name (up to 63 alphanumeric characters) for identification purposes.
Key	Enter a password (up to 15 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 the ZyWALL.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
Host Members	The ordering of the RADIUS servers is important as the ZyWALL uses the RADIUS servers for user authentication in the order they appear in this table.
#	This field displays the index number.
Members	Enter the IP address (in dotted decimal notation) or the domain name (up to 63 alphanumeric characters) of a RADIUS server.
Authentication Port	The default port of the RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.
	Click  to add a new RADIUS server. You can add up to four RADIUS member servers. Click  to delete a RADIUS server.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

CHAPTER 32

Authentication Objects

This chapter shows you how to select different authentication methods for user authentication using the AAA servers or the internal user database.

32.1 Authentication Objects Overview

After you have created the AAA server objects in the **AAA Server** screens, you can specify the authentication objects (containing the AAA server information) that the ZyWALL uses to authenticate users (using VPN or managing through HTTP/HTTPS).

Specify the authentication server(s) and/or server group(s) in the **Auth. Method** screen to create an authentication object.

32.2 Viewing Authentication Objects

Click **Objects > Auth. Method** to display the screen as shown.

Note: You can create up to 16 authentication objects.

Figure 306 Objects: Auth. Method




#	Method Name	Method List	
1	default	local	
2	Example	group ldap	

The following table describes the labels in this screen.

Table 159 Objects > Auth. Method



LABEL	DESCRIPTION
#	This field displays the index number.
Method Name	This field displays a descriptive name for identification purposes.

Table 159 Objects > Auth. Method (continued)

LABEL	DESCRIPTION
Method List	This field displays the authentication method(s) for this entry.
	<p>Click  to add a new entry.</p> <p>Click  to edit the settings of an entry.</p> <p>Click  to delete an entry.</p>

32.3 Creating an Authentication Object

Follow the steps below to create an authentication object.

- 1 Click **Objects > Auth. Method**.
- 2 Click .
- 3 Specify a descriptive name for identification purposes in the **Name** field. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".
- 4 Click  to insert an authentication method in the table.
- 5 Select a server object from the **Method List** drop-down list box.
- 6 You can add up to three server objects to the table. The ordering of the **Method List** column is important. The ZyWALL authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

If two accounts with the same username exist on two authentication servers you specify, the ZyWALL does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.




Note: You can NOT select two server objects of the same type.

- 7 Click **OK** to save the settings or click **Cancel** to discard all changes and return to the previous screen.

Figure 307 Objects > Auth. Method > Add

The following table describes the labels in this screen.

Table 160 Objects > Auth. Method > Add

LABEL	DESCRIPTION
Name	Specify a descriptive name for identification purposes. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".
Method List	Select a server object from the drop-down list box. You can create a server object in in the Auth. Method screen (see Chapter 31 on page 455 for more information). The ZyWALL authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen. If two accounts with the same username exist on two authentication servers you specify, the ZyWALL does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.
	Click  to add a new entry. Click  to edit the settings of an entry. Click  to delete an entry.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

32.3.1 Example: Selecting a VPN Authentication Method

After you set up an authentication method in the **Auth. Method** screens, you can use it in the **VPN Gateway** screen to authenticate VPN users for establishing a VPN connection. Refer to the chapter on VPN for more information.

Follow the steps below to specify the authentication method for a VPN connection.

- 1** Access the **VPN Gateway** screen.
- 2** Select **Enable Extended Authentication**.
- 3** Select **Server Mode** and select an authentication method object from the drop-down list box.

4 Click **OK** to save the settings.

Figure 308 Example: Using Authentication Method in VPN

The screenshot displays the configuration interface for a VPN Gateway. The interface is divided into several sections:

- VPN Gateway:** Contains a text input field for "VPN Gateway Name".
- IKE Phase 1:** Contains a "Negotiation Mode" dropdown menu set to "Main" and a "Proposal" dropdown menu. The "Proposal" menu is open, showing options for "Encryption" and "Authentication".
- Extended Authentication:** This section is highlighted with a red circle. It includes:
 - An unchecked checkbox for "Enable Extended Authentication".
 - A radio button selected for "Server Mode", with a "default" dropdown menu next to it.
 - An unchecked radio button for "Client Mode".
 - Text input fields for "User Name" and "Password".

At the bottom of the interface, there are "OK" and "Cancel" buttons.

CHAPTER 33

Certificates

This chapter gives background information about public-key certificates and explains how to use the **Certificates** screens. [See the Objects section](#) in the Configuration Overview chapter for related information on these screens.

33.1 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).

33.1.1 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.

33.2 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.

33.3 Factory Default Certificate

The ZyWALL generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

33.3.1 Certificate File Formats

Any 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. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. 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.

- **Binary PKCS#12:** This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it decrypt the contents when you import the file into the ZyWALL.

Note: Be careful to not convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

33.4 Certificate Configuration Screens Summary

This section summarizes how to manage certificates on the ZyWALL.

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 Certificates** screens to save CA certificates and trusted remote host certificates to the ZyWALL. The ZyWALL will trust any valid certificate that you have imported as a trusted certificate. It will also trust any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

33.5 Verifying a Certificate

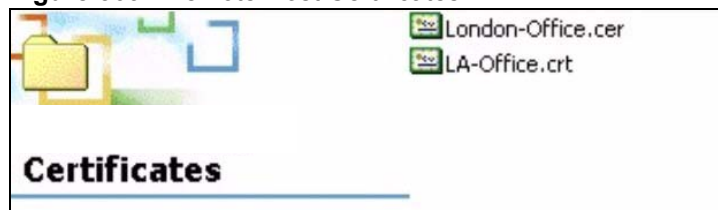
Before you import a certificate into the ZyWALL, you should verify that you have the actual certificate. This is especially true of trusted certificates since the ZyWALL also trusts any valid certificate signed by any of the imported trusted certificates.

33.5.1 Checking the Fingerprint of a Certificate on Your Computer

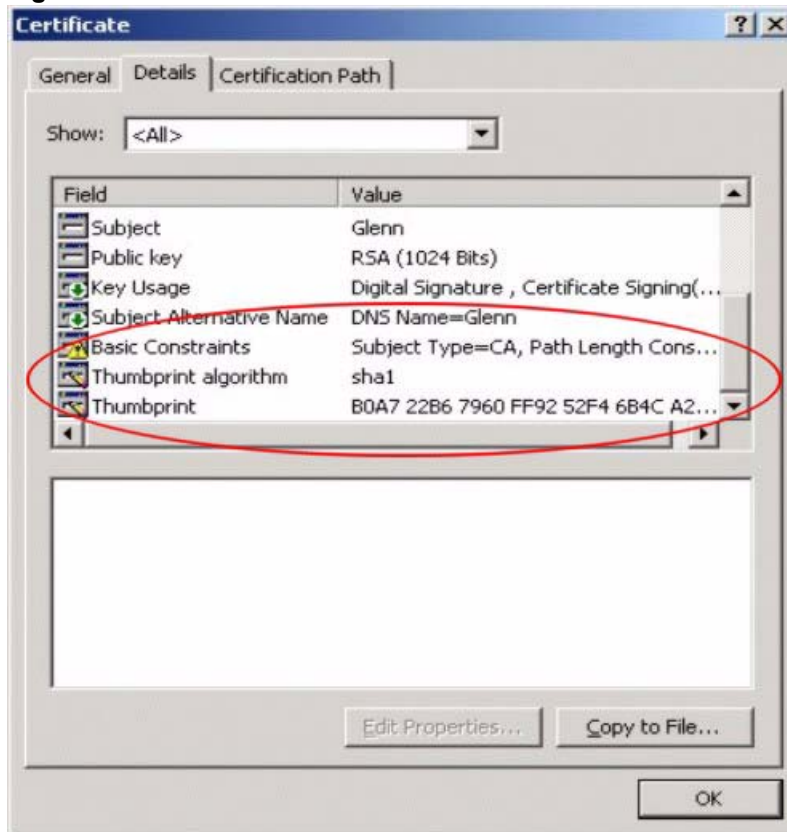
A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 309 Remote Host Certificates



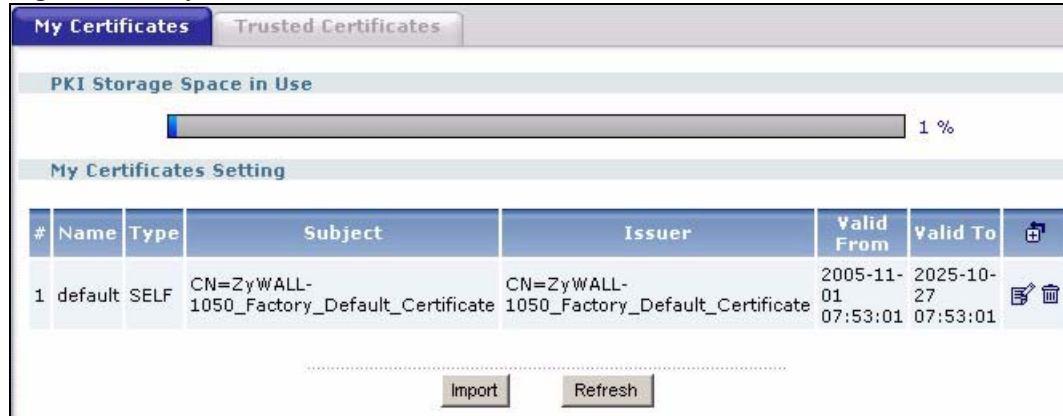
- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 310 Certificate Details

- 4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

33.6 My Certificates Screen

Click **Configuration > Object > Certificate > My Certificates** to open the **My Certificates** screen. This is the ZyWALL's summary list of certificates and certification requests.

Figure 311 My Certificates Screen

The following table describes the labels in this screen.

Table 161 My Certificates Screen

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, 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. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. REQ 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 My Certificate Import screen to import the certificate and replace the request. SELF represents a self-signed certificate. CERT represents a certificate issued by a certification authority.
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 Subject field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.

Table 161 My Certificates Screen (continued)

LABEL	DESCRIPTION
Modify	<p>Click the Add icon to go to the screen where you can have the ZyWALL generate a certificate or a certification request.</p> <p>Click the Edit icon to open a screen with an in-depth list of information about the certificate.</p> <p>The ZyWALL keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates.</p> <p>Click the Delete icon to remove a certificate. A window displays asking you to confirm that you want to delete the certificate. Subsequent certificates move up by one when you take this action.</p> <p>You cannot delete certificates that any of the ZyWALL's features are configured to use.</p>
Import	Click Import to open a screen where you can save a certificate to the ZyWALL.
Refresh	Click Refresh to display the current validity status of the certificates.

33.6.1 My Certificates Add Screen

Click **Configuration > Object > Certificate > My Certificates** and then the add icon to open the **My Certificates Add** 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 312 My Certificates Add Screen

The screenshot shows a web-based form for adding a certificate. It is divided into three main sections:

- Name:** A single text input field.
- Subject Information:** A section with a light blue header. It contains:
 - Common Name:** Three radio buttons: "Host IP Address" (selected), "Host Domain Name", and "E-Mail". Each has a corresponding text input field. The "Host IP Address" field contains "0.0.0.0".
 - Organizational Unit:** A text input field with "(Optional)" to its right.
 - Organization:** A text input field with "(Optional)" to its right.
 - Country:** A text input field with "(Optional)" to its right.
 - Key Type:** A dropdown menu currently set to "RSA".
 - Key Length:** A dropdown menu currently set to "512" followed by the text "bits".
- Enrollment Options:** A section with a light blue header. It contains:
 - Three radio buttons: "Create a self-signed certificate", "Create a certification request and save it locally for later manual enrollment", and "Create a certification request and enroll for a certificate immediately online" (selected).
 - Enrollment Protocol:** A dropdown menu set to "Certificate Management Protocol (CMP)".
 - CA Server Address:** A text input field.
 - CA Certificate:** A dropdown menu with "(See [Trusted CAs](#))" to its right.
 - Request Authentication:** A section with two text input fields: "Reference Number" and "Key".

At the bottom right, there are "OK" and "Cancel" buttons.

The following table describes the labels in this screen.

Table 162 My Certificates Add Screen

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;~!@#\$\$%^&()_+[]{}',.- characters.
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 Common Name 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.

Table 162 My Certificates Add Screen (continued)

LABEL	DESCRIPTION
Common Name	<p>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 is for identification purposes only and can be any string.</p> <p>A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.</p> <p>An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.</p>
Organizational Unit	<p>Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.</p>
Organization	<p>Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.</p>
Country	<p>Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.</p>
Key Type	<p>Select RSA to use the Rivest, Shamir and Adleman public-key algorithm.</p> <p>Select DSA to use the Digital Signature Algorithm public-key algorithm.</p>
Key Length	<p>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.</p>
Enrollment Options	<p>These radio buttons deal with how and when the certificate is to be generated.</p>
Create a self-signed certificate	<p>Select Create a self-signed certificate 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.</p>
Create a certification request and save it locally for later manual enrollment	<p>Select Create a certification request and save it locally for later manual enrollment to have the ZyWALL generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority.</p> <p>Copy the certification request from the My Certificate Details screen (see Section 33.6.2 on page 477) and then send it to the certification authority.</p>
Create a certification request and enroll for a certificate immediately online	<p>Select Create a certification request and enroll for a certificate immediately online to have the ZyWALL generate a request for a certificate and apply to a certification authority for a certificate.</p> <p>You must have the certification authority's certificate already imported in the Trusted Certificates screen.</p> <p>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 Reference Number and Key if the certification authority requires them.</p>
Enrollment Protocol	<p>This field applies when you select Create a certification request and enroll for a certificate immediately online. Select the certification authority's enrollment protocol from the drop-down list box.</p> <p>Simple Certificate Enrollment Protocol (SCEP) is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.</p> <p>Certificate Management Protocol (CMP) 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.</p>

Table 162 My Certificates Add Screen (continued)

LABEL	DESCRIPTION
CA Server Address	<p>This field applies when you select Create a certification request and enroll for a certificate immediately online. Enter the IP address (or URL) of the certification authority server.</p> <p>For a URL, you can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@\$_%&-</p>
CA Certificate	<p>This field applies when you select Create a certification request and enroll for a certificate immediately online. Select the certification authority's certificate from the CA Certificate drop-down list box.</p> <p>You must have the certification authority's certificate already imported in the Trusted Certificates screen. Click Trusted CAs to go to the Trusted Certificates screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities.</p>
Request Authentication	<p>When you select Create a certification request and enroll for a certificate immediately online, the certification authority may want you to include a reference number and key to identify you when you send a certification request.</p> <p>Fill in both the Reference Number and the Key fields if your certification authority uses CMP enrollment protocol. Just the Key field displays if your certification authority uses the SCEP enrollment protocol.</p> <p>For the reference number, use 0 to 99999999.</p> <p>For the key, use up to 31 of the following characters. a-zA-Z0-9; '~!@#%&*()_+{}';./<>=-</p>
OK	Click OK to begin certificate or certification request generation.
Cancel	Click Cancel to quit and return 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.

33.6.2 My Certificate Edit Screen

Click **Configuration > Object > Certificate > My Certificates** and then the edit icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 313 My Certificate Edit Screen

Name

Certification Path

Certificate Information

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	0
Subject	CN=ZyWALL-1050_Factory_Default_Certificate
Issuer	CN=ZyWALL-1050_Factory_Default_Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2005-11-01 07:53:01
Valid To	2025-10-27 07:53:01
Key Algorithm	rsaEncryption (1024 bits)
Subject Alternative Name	ZyWALL-1050_Factory_Default_Certificate
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	6c:df:bb:7b:68:b3:dd:07:e8:fd:f6:6a:27:b7:e1:91
SHA1 Fingerprint	46:dc:4e:2e:fd:7f:48:c8:77:1f:cd:ee:08:bc:49:1c:d4:7e:99:ab

Certificate in PEM (Base-64) Encoded Format

```

-----BEGIN X509 CERTIFICATE-----
MIICNDCCA22gAwIBAgIBADANBgkqhkiG9w0BAQUFADAYMTAwLgYDVQDDCdaeVdB
TEwtMTA1MF9GYWNOb3J5XORlZmF1bHRfQ2VydG1maWNhdGUwHhcNMDUxMTAxMDc1
MzAxWhcNMjUxMDUxMDc1MzAxWjAyMTAwLgYDVQDDCdaeVdBTEwtMTA1MF9GYWNO
b3J5XORlZmF1bHRfQ2VydG1maWNhdGUwZ8wDQYJKoZIhvcNAQEBBQADgYOA MIGJ
AoGBAMqIZzqV/JHn5vkkLv1WkbCE2sU8Sae6zLt9VsWtgFhYxhxEDi+8wSk35dM7
Loexra7z71ycObUcBpfo5DFp7hJFpjAIfMnIM6Xr5WbWtom25RiQFqKZBLjHB8tn
z1YH2cTm7BHOsXTicSKP+nQO7upELGR4GnBZZrMyuCC2VkJAgMBAAGjWjBYMA4G
A1UdDwEB/wQEAWICpDyBgNVHREEKzApgSdaeVdBTEwtMTA1MF9GYWNOb3J5XORl
ZmF1bHRfQ2VydG1maWNhdGUwEgYDVROTAQH/BAGwBgEB/wIBATANBgkqhkiG9w0B
    
```

Password:
 (Optional)

The following table describes the labels in this screen.

Table 163 My Certificate Edit Screen

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#\$\$%^&()_+[]{}',.-= characters.
Certification Path	This field displays for a certificate, not a certification request. Click the Refresh 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 Refresh 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 Subject Name field. "none" displays for a certification request.
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. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
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 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.

Table 163 My Certificate Edit Screen (continued)

LABEL	DESCRIPTION
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. This field does not display for a certification request.
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	This button displays for a certification request. Use this button to save a copy of the request without its private key. Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
OK	Click OK to save your changes back to the ZyWALL. You can only change the name.
Cancel	Click Cancel to quit and return to the My Certificates screen.

33.6.3 My Certificate Import Screen

Click **Configuration > Object > Certificate > 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 import a certificate that matches a corresponding certification request that was generated by the ZyWALL. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

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.

Figure 314 My Certificate Import Screen

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
- Binary PKCS#12

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: Password: (PKCS#12 only)

.....

The following table describes the labels in this screen.

Table 164 My Certificate Import Screen

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the ZyWALL.
Browse	Click Browse to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.

33.7 Trusted Certificates Screen

Click **Configuration > Object > Certificate > Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the ZyWALL to accept as trusted. The ZyWALL also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

33.7.1 OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the ZyWALL checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the ZyWALL only gets information on the certificates that it needs to verify, not a huge list. When the ZyWALL requests certificate status information, the OCSP server returns a “expired”, “current” or “unknown” response.

Figure 315 Trusted Certificates Screen



The following table describes the labels in this screen.

Table 165 Trusted Certificates Screen

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, 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 Subject field.
Valid From	This field displays the date that the certificate becomes applicable.

Table 165 Trusted Certificates Screen (continued)

LABEL	DESCRIPTION
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Modify	<p>Click the Edit icon to open a screen with an in-depth list of information about the certificate.</p> <p>The ZyWALL keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates.</p> <p>Click the Delete icon to remove a 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.</p>
Import	Click Import 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.

33.8 Trusted Certificates Edit Screen

Click **Configuration > Object > Certificate > Trusted Certificates** and then a certificate's edit icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the 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.

The following table describes the labels in this screen.

Table 166 Trusted Certificates Edit Screen

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;~!@#\$\$%^&()_+[]{}',.- characters.
Certification Path	Click the Refresh 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 certificate, 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 Refresh to display the certification path.
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this check box to have the ZyWALL check incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) or an OCSP server. You also need to configure the OCSP or LDAP server details.
OCSP Server	Select this check box if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and pathname of the OCSP server.
ID	The ZyWALL may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The ZyWALL may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
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.

Table 166 Trusted Certificates Edit Screen (continued)

LABEL	DESCRIPTION
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 Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
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 Certificate	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
OK	Click OK to save your changes back to the ZyWALL. You can only change the name.
Cancel	Click Cancel to quit and return to the Trusted Certificates screen.

33.9 Trusted Certificates Import Screen

Click **Configuration > Object > Certificate > Trusted Certificates > Import** to open the **Trusted Certificates Import** screen. Follow the instructions in this screen to save a trusted certificate to the ZyWALL.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 317 Trusted Certificates Import Screen

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

File Path:

The following table describes the labels in this screen.

Table 167 Trusted Certificates Import Screen

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the ZyWALL.
Browse	Click Browse to find the certificate file you want to upload.

CHAPTER 34

System

This chapter provides information on the system screens.

34.1 System Overview

The system screens can help you configure general ZyWALL information, the system time and the console port connection speed for a terminal emulation program. The screens also allow you to configure DNS settings and determine which services/protocols can access which ZyWALL zones (if any) from which computers.

34.2 Host Name

A host name is the unique name by which a device is known on a network. Click **Configuration > System > Host Name** to open the **Host Name** screen.

Figure 318 System > Host Name

The screenshot shows a web-based configuration interface for the ZyWALL Host Name. It features a header 'General settings' in a light blue bar. Below this, there are two text input fields. The first is labeled 'System Name' and contains the text 'zw1050'. The second is labeled 'Domain Name' and is currently empty. To the right of each input field is the text '(Optional)'. At the bottom of the form, there are two buttons: 'Apply' and 'Reset', separated by a dotted line.

The following table describes the labels in this screen.

Table 168 System > Host Name

LABEL	DESCRIPTION
General Settings	
System Name	Choose a descriptive name to identify your ZyWALL device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

34.3 Time and Date

This section shows you how:

- 1 To manually set the ZyWALL date and time.
- 2 To get the ZyWALL date and time from a time server.

For effective scheduling and logging, the ZyWALL system time must be accurate. The ZyWALL's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

To change your ZyWALL's time based on your local time zone and date, click **Configuration > System > Date/Time**. The screen displays as shown.

Figure 319 System > Date and Time

The following table describes the labels in this screen.

Table 169 System > Date and Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your ZyWALL.
Current Date	This field displays the present date of your ZyWALL.
Time and Date Setup	

Table 169 System > Date and Time (continued)

LABEL	DESCRIPTION
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 time zone and daylight saving will affect the new time and date you entered.
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 Time and Date Setup to Manual , enter the new time in this field and then click Apply .
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 Time and Date Setup to Manual , enter the new date in this field and then click Apply .
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 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 Time Server Address field). This also saves your changes (except the daylight saving settings).
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	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. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Enable Daylight Saving . The at field uses the 24 hour format. Here are a couple of examples: 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 First, Sunday, April and type 2 in the at field. 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 Last, Sunday, March . The time you type in the at 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).
End Date	Configure the day and time when Daylight Saving Time ends if you selected Enable Daylight Saving . The at field uses the 24 hour format. Here are a couple of examples: 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 Last, Sunday, October and type 2 in the at field. 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 Last, Sunday, October . The time you type in the at 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).

Table 169 System > Date and Time (continued)

LABEL	DESCRIPTION
Offset	Specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments). For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

34.3.1 Pre-defined NTP Time Servers List

When you turn on the ZyWALL for the first time, the date and time start at 2003-01-01 00:00:00. The ZyWALL then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (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.

Table 170 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

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.

34.3.2 Updating the Time

The ZyWALL gets the time and date from a time server in the following instances:

- When you click **Synchronize Now**.
- On saving your changes.
- 24-hour intervals after you click **Apply**.

34.3.3 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Please Wait...** screen appears, you may have to wait up to one minute.

Figure 320 Synchronization in Process

The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try reconfiguring the **Date/Time** screen.

To manually set the ZyWALL date and time

- 1 Click **Configuration > System > Date/Time**.
- 2 Select **Manual** under **Time and Date Setup**.
- 3 Enter the ZyWALL's time in the **New Time** field.
- 4 Enter the ZyWALL's date in the **New Date** field.
- 5 Under **Time Zone Setup**, select your **Time Zone** from the list.
- 6 As an option you can select the **Enable Daylight Saving** check box to adjust the ZyWALL clock for daylight savings.
- 7 Click **Apply**.

To get the ZyWALL date and time from a time server

- 1 Click **Configuration > System > Date/Time**.
- 2 Select **Get from Time Server** under **Time and Date Setup**.
- 3 Under **Time Zone Setup**, select your **Time Zone** from the list.
- 4 As an option you can select the **Enable Daylight Saving** check box to adjust the ZyWALL clock for daylight savings.
- 5 Under **Time and Date Setup**, enter a **Time Server Address** ([Table 170 on page 492](#)).
- 6 Click **Apply**.

34.4 Console Port Speed

This section shows you how to set the console port speed when you connect to the ZyWALL via the console port using a terminal emulation program. See [Table 2 on page 49](#) for default console port settings.

Click **Configuration > System > Console Speed** to open the **Console Speed** screen.

Figure 321 System > Console Port Speed

The following table describes the labels in this screen.

Table 171 System > Console Port Speed

LABEL	DESCRIPTION
Configuration	
Console Port Speed	Use the drop-down list box to change the speed of the console port. Your ZyWALL supports 9600, 19200, 38400, 57600, and 115200 bps (default) for the console port. The Console Port Speed applies to a console port connection using terminal emulation software and NOT the Console in the ZyWALL web configurator Status screen.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

34.5 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.

34.5.1 DNS Server Address Assignment

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

- 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.
- 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.

- You can manually enter the IP addresses of other DNS servers.

34.5.2 DNS Servers

Use the **DNS** 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. You can also configure the ZyWALL to accept or discard DNS queries. Use the **Network > Interface** screens to configure the DNS server information that the ZyWALL sends to the specified DHCP client devices.

34.5.3 Configuring DNS

Click **Configuration > System > DNS** to change your ZyWALL's DNS settings.

Figure 322 System > DNS

DNS Server				
Address/PTR Record				
#	FQDN	IP Address		
1	www.xyz.com	1.2.3.4	[Add] [Edit] [Delete]	
Domain Zone Forwarder				
#	Domain Zone	From	DNS Server	
1	abc.com.tw	User-Defined	10.1.2.3	[Add] [Edit] [Delete] [Refresh]
2	zyxel.com	ge2(N/A)	N/A	[Add] [Edit] [Delete] [Refresh]
-	*	Default	N/A	N/A
MX Record (for My FQDN)				
#	Domain Name	IP/FQDN		
1	zyxel.com.tw	zmail.zyxel.com.tw	[Add] [Edit] [Delete]	
Service Control				
#	Zone	Address	Action	
1	ALL	ALL	Accept	[Add] [Edit] [Delete] [Refresh]

The following table describes the labels in this screen.

Table 172 System > DNS

LABEL	DESCRIPTION
Address/PTR Record	This record specifies the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain.
#	This is the index number of the address/PTR record.
FQDN	This is a host's fully qualified domain name.
IP Address	This is the IP address of a host.

Table 172 System > DNS (continued)

















LABEL	DESCRIPTION
  	<p>Click the Add icon in the heading row to open a screen where you can add a new address/PTR record. Refer to Table 173 on page 498 for information on the fields.</p> <p>Click the Edit icon to go to the screen where you can edit the record.</p> <p>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.</p>
Domain Zone Forwarder	<p>This specifies a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server.</p> <p>When the ZyWALL needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.</p>
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence.
Domain Zone	<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.</p> <p>A "*" means all domain zones. The default record is not configurable. The ZyWALL uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.</p>
From	This displays whether the DNS server IP address is assigned by the ISP dynamically through a specified interface or configured manually.
DNS Server	This is the IP address of a DNS server. This field displays N/A if you have the ZyWALL get a DNS server IP address from the ISP dynamically but the specified interface is not active.
    	<p>Click the Add icon in the heading row to open a screen where you can add a new domain zone forwarder record. Refer to Table 174 on page 499 for information on the fields.</p> <p>Click the Edit icon to go to the screen where you can edit the record.</p> <p>Click the Add icon in an entry to add a record below the current entry.</p> <p>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.</p> <p>Click the Move to N icon to display a field to type a number for where you want to put that record and press [ENTER] to move the record to the number that you typed.</p>
MX Record (for My FQDN)	A MX (Mail eXchange) record identifies a mail server that handles the mail for a particular domain.
#	This is the index number of the MX record.
Domain Name	This is the domain name where the mail is destined for.
IP/FQDN	This is the IP address or fully qualified domain name of a mail server that handles the mail for the domain specified in the field above.

Table 172 System > DNS (continued)

LABEL	DESCRIPTION
  	<p>Click the Add icon in the heading row to open a screen where you can add a new MX record. Refer to Table 175 on page 500 for information on the fields.</p> <p>Click the Edit icon to go to the screen where you can edit the record.</p> <p>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.</p>
Service Control	This specifies from which computers and zones you can send DNS queries to the ZyWALL.
#	This the index number of the service control rule. The ordering of your rules is important as rules are applied in sequence.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to send DNS queries.
Action	This displays whether the ZyWALL accepts DNS queries from the computer with the IP address specified above through the specified zone (Accept) or discards them (Deny).
    	<p>Click the Add icon in the heading row to open a screen where you can add a new rule. Refer to Table 176 on page 501 for information on the fields.</p> <p>Click the Edit icon to go to the screen where you can edit the rule.</p> <p>Click the Add icon in an entry to add a rule below the current entry.</p> <p>Click the Delete icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.</p> <p>Click the Move to N icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.</p>
Apply	Click Apply to save your customized settings.
Reset	Click Reset to begin configuring this screen afresh.

34.5.4 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. For example, `www.zyxel.com` is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com” is the top level domain. `mail.myZyXEL.com.tw` is also a FQDN, where “mail” is the host, “myZyXEL” is the third-level domain, “com” is the second-level domain, and “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.

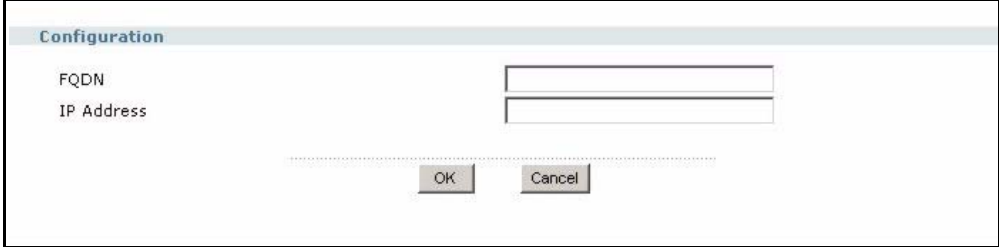
34.5.5 PTR Record

A PTR (pointer) record is also called a reverse record or a reverse lookup record. It is a mapping of an IP address to a domain name.

34.5.6 Adding an Address/PTR Record

Click the Add () icon in the **Address/PTR Record** table to add an address/PTR record.

Figure 323 System > DNS > Address/PTR Record Edit



The following table describes the labels in this screen.

Table 173 System > DNS > Address/PTR Record Edit

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 third-level domain, “com” is the second-level domain, and “tw” is the top level domain.
IP Address	Enter the IP address of the host in dotted decimal notation.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

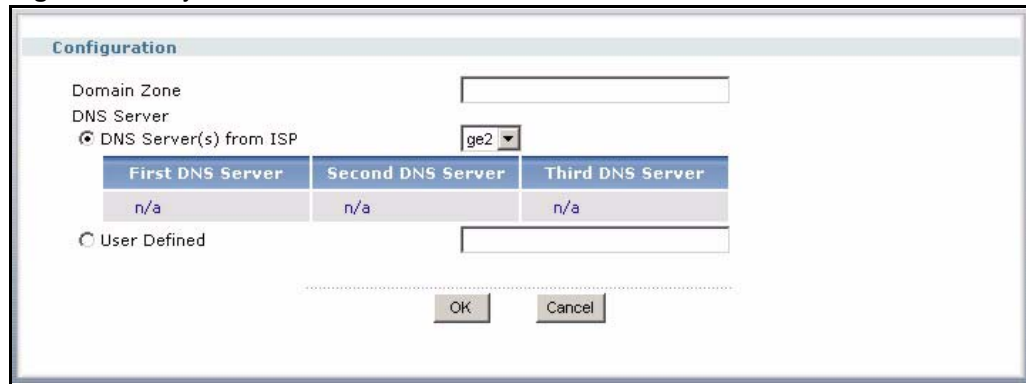
34.5.7 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. 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.

34.5.8 Adding a Domain Zone Forwarder

Click the Add ( or ) icon in the **Domain Zone Forwarder** table to add a **domain zone forwarder** record.

Figure 324 System > DNS > Domain Zone Forwarder Edit



The following table describes the labels in this screen.

Table 174 System > DNS > Domain Zone Forwarder Edit

LABEL	DESCRIPTION
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. 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. Enter * if all domain zones are served by the specified DNS server(s).
DNS Server	Select DNS Server(s) from ISP if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set to be a DHCP client. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. N/A displays for any DNS server IP address fields for which the ISP does not assign an IP address. Select User Defined 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. User Defined entries with the IP address set to 0.0.0.0 are not allowed.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

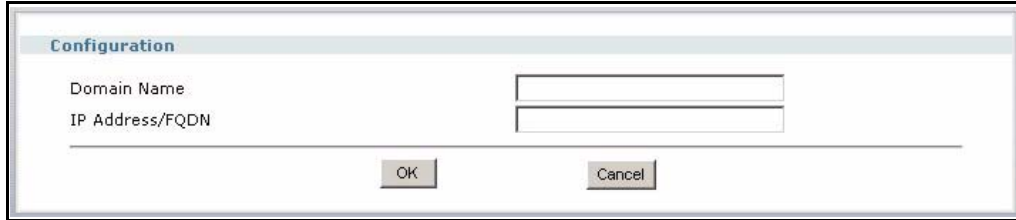
34.5.9 MX Record

A MX (Mail eXchange) record indicates which host is responsible for the mail for a particular domain, that is, controls where mail is sent for that domain. If you do not configure proper MX records for your domain or other domain, external e-mail from other mail servers will not be able to be delivered to your mail server and vice versa. Each host or domain can have only one MX record, that is, one domain is mapping to one host.

34.5.10 Adding a MX Record

Click the Add () icon in the **MX Record** table to add a MX record.

Figure 325 System > DNS > MX Record Edit



The following table describes the labels in this screen.

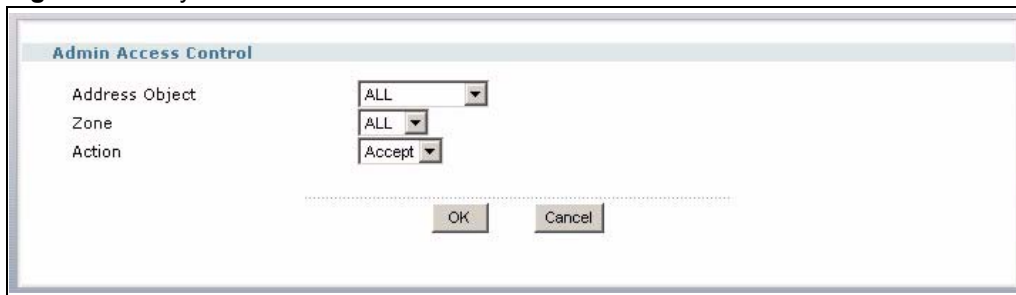
Table 175 System > DNS > MX Record Edit

LABEL	DESCRIPTION
Domain Name	Enter the domain name where the mail is destined for.
IP Address/FQDN	Enter the IP address or fully qualified domain name of a mail server that handles the mail for the domain specified in the field above.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

34.5.11 DNS Service Control

Click the Add ( or ) icon in the **Service Control** table to add a service control rule.

Figure 326 System > DNS > Service Control Rule Edit



The following table describes the labels in this screen.

Table 176 System > DNS > Service Control Rule Edit

LABEL	DESCRIPTION
Address Object	Select ALL to allow or deny any computer to send DNS queries to the ZyWALL. Select a predefined address object to just allow or deny the computer with the IP address that you specified to send DNS queries to the ZyWALL.
Zone	Select ALL to allow or prevent DNS queries through any zones. Select a predefined zone on which a DNS query to the ZyWALL is allowed or denied.
Action	Select Accept to have the ZyWALL allow the DNS queries from the specified computer. Select Deny to have the ZyWALL reject the DNS queries from the specified computer.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

CHAPTER 35

System Remote Management

This chapter shows you how to determine what services may access what zones on the ZyWALL.

35.1 Remote Management Overview

The **WWW**, **SSH**, **Telnet**, **FTP** and **SNMP** screens allow you to determine which services/protocols can access which ZyWALL zones (if any) from which computers.

See the [DNS, WWW, SSH, TELNET, FTP, SNMP](#) section for related information on these screens.

Note: To allow the ZyWALL to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-ZyWALL rule to block that traffic.

This section is related to the to-ZyWALL firewall rules, see [Section 19.2.2 on page 303](#) for more information.

You may manage your ZyWALL from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN&WAN&DMZ)
- DMZ only

To disable remote management of a service, deselect **Enable** in the corresponding service screen.

35.1.1 Remote Management Limitations

Remote management will not work when:

- 1 You have disabled that service in the corresponding screen.
- 2 The allowed IP address (address object) in the **Service Control** table does not match the client IP address (the ZyWALL disconnects the session immediately).
- 3 The IP address (address object) in the **Service Control** table is not in the allowed zone or the action is set to **Deny**.
- 4 There is a firewall rule that blocks it.

35.1.2 System Timeout

There is a lease timeout for administrators. 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.

Each user is also forced to log in the ZyWALL for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User/Group** screens.

35.2 Introduction to HTTPS

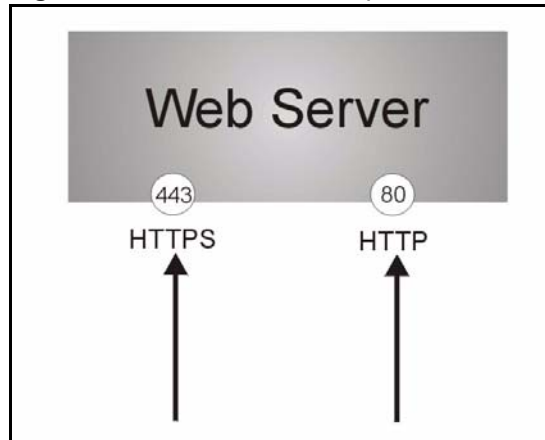
HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the 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 33 on page 469](#) for more information).

HTTPS on the ZyWALL is used so that you can securely access the ZyWALL using the web configurator. The SSL protocol specifies that the HTTPS server (the ZyWALL) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the ZyWALL), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS 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 web server.
- 2 HTTP connection requests from a web browser go to port 80 (by default) on the ZyWALL's web server.

Figure 327 HTTP/HTTPS Implementation

Note: If you disable **HTTP** in the **WWW** screen, then the ZyWALL blocks all HTTP connection attempts.

35.3 Configuring WWW

Click **Configuration > System > WWW** to open the **WWW** screen. Use this screen to change your ZyWALL's web settings.

Figure 328 System > WWW

HTTPS

Enable

Server Port

Authenticate Client Certificates (See [Trusted CAs](#))

Server Certificate (See [My Certificates](#))

Redirect HTTP to HTTPS

Admin Service Control

#	Zone	Address	Action	
1	ALL	ALL	Accept	

User Service Control

#	Zone	Address	Action	
#	Zone	Address	Action	

HTTP

Enable

Server Port

Admin Service Control

#	Zone	Address	Action	
1	ALL	ALL	Accept	

User Service Control

#	Zone	Address	Action	
#	Zone	Address	Action	

Authentication

Client Authentication Method

The following table describes the labels in this screen.

Table 177 System > WWW

LABEL	DESCRIPTION
HTTPS	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the ZyWALL web configurator using secure HTTPs connections.
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS 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.
Authenticate Client Certificates	Select Authenticate Client Certificates (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.
Server Certificate	Select a certificate the HTTPS server (the ZyWALL) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the My Certificates screen.
Redirect HTTP to HTTPS	To allow only secure web configurator access, select this to redirect all HTTP connection requests to the HTTPS server.

Table 177 System > WWW (continued)











LABEL	DESCRIPTION
Admin/User Service Control	This specifies from which computers an administrator or non-administrator can access the specified ZyWALL zones.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the Zone field (Accept) or not (Deny).
    	<p>Click the Add icon in the heading row to open a screen where you can add a new rule. Refer to Table 178 on page 509 for information on the fields.</p> <p>Click the Edit icon to go to the screen where you can edit the rule.</p> <p>Click the Add icon in an entry to add a rule below the current entry.</p> <p>Click the Delete icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.</p> <p>Click the Move to N icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.</p>
HTTP	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the ZyWALL web configurator using HTTP connections.
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.
Admin/User Service Control	This specifies from which computers an administrator or non-administrator can access the specified ZyWALL zones.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the Zone field (Accept) or not (Deny).

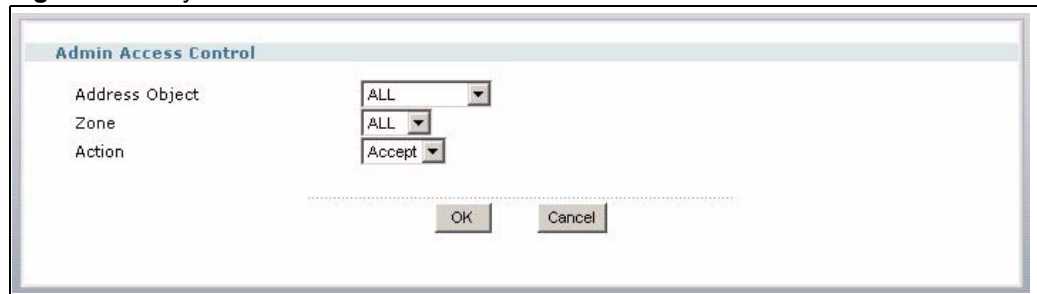
Table 177 System > WWW (continued)

LABEL	DESCRIPTION
	Click the Add icon in the heading row to open a screen where you can add a new rule. Refer to Table 178 on page 509 for information on the fields.
	Click the Edit icon to go to the screen where you can edit the rule.
	Click the Add icon in an entry to add a rule below the current entry.
	Click the Delete icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.
	Click the Move to N icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.
Authentication	
Client Authentication Method	Select a method the HTTPS or HTTP server uses to authenticate a client. You must have configured the authentication methods in the Auth. method screen.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

35.4 Service Control Rules

Click **Add** or **Edit** in the **Service Control** table in a **WWW, SSH, Telnet, FTP** or **SNMP** screen to add a service control rule.

Figure 329 System > Service Control Rule Edit



The following table describes the labels in this screen.

Table 178 Edit Service Control Rule

LABEL	DESCRIPTION
Address Object	Select ALL to allow or deny any computer to communicate with the ZyWALL using this service. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the ZyWALL using this service.
Zone	Select ALL to allow or prevent any ZyWALL zones from being accessed using this service. Select a predefined ZyWALL zone on which a incoming service is allowed or denied.
Action	Select Accept to allow the user to access the ZyWALL from the specified computers. Select Deny to block the user's access to the ZyWALL from the specified computers.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

35.5 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.

35.5.1 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 330 Security Alert Dialog Box (Internet Explorer)

35.5.2 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.

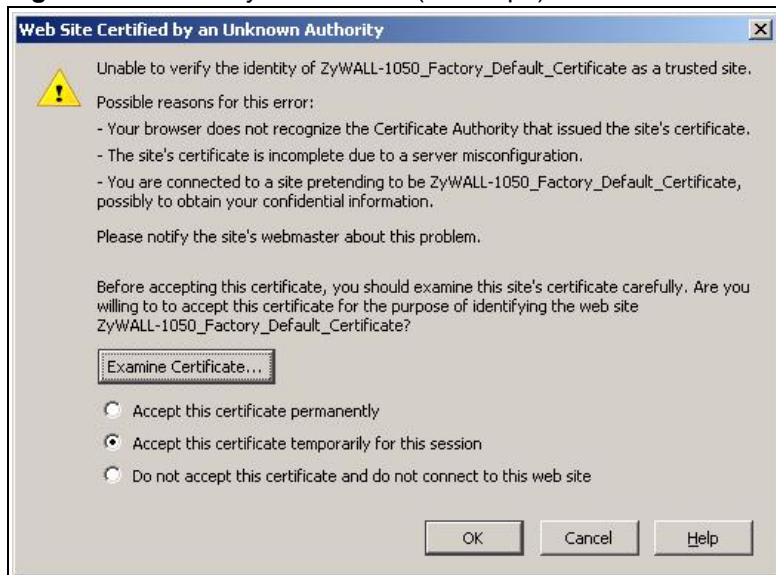
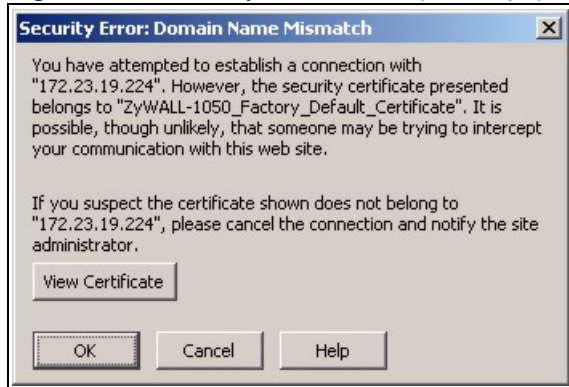
Figure 331 Security Certificate 1 (Netscape)

Figure 332 Security Certificate 2 (Netscape)

35.5.3 Avoiding 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.

35.5.4 Login Screen

After you accept the certificate, the ZyWALL login screen appears. The lock displayed in the bottom of the browser status bar denotes a secure connection.

Figure 333 Login Screen (Internet Explorer)

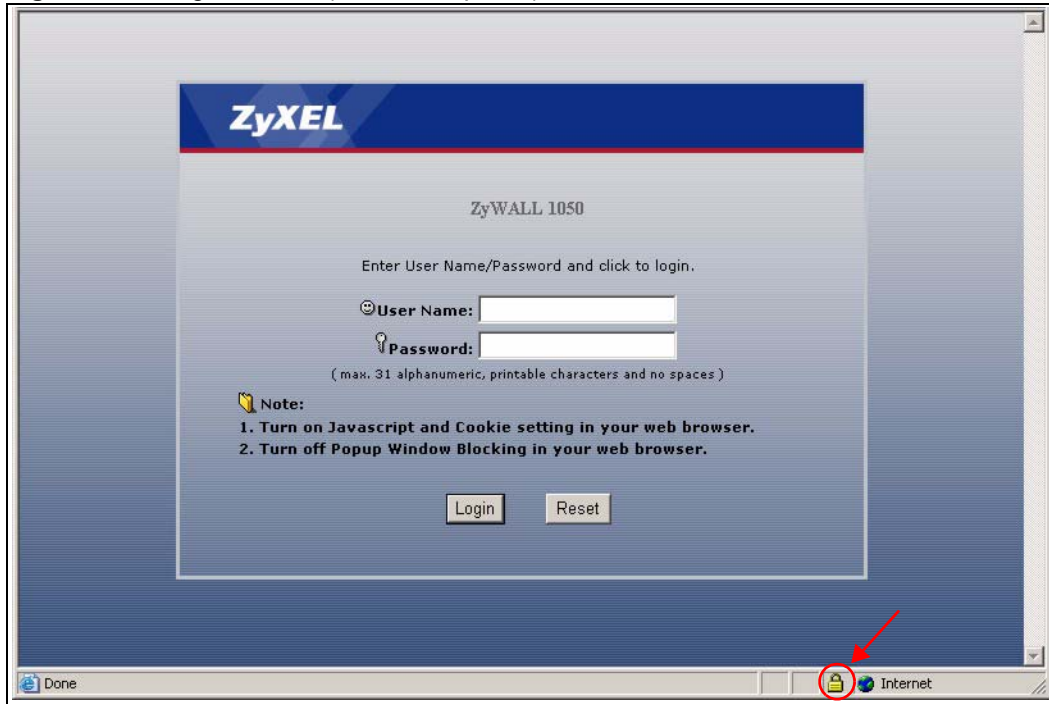
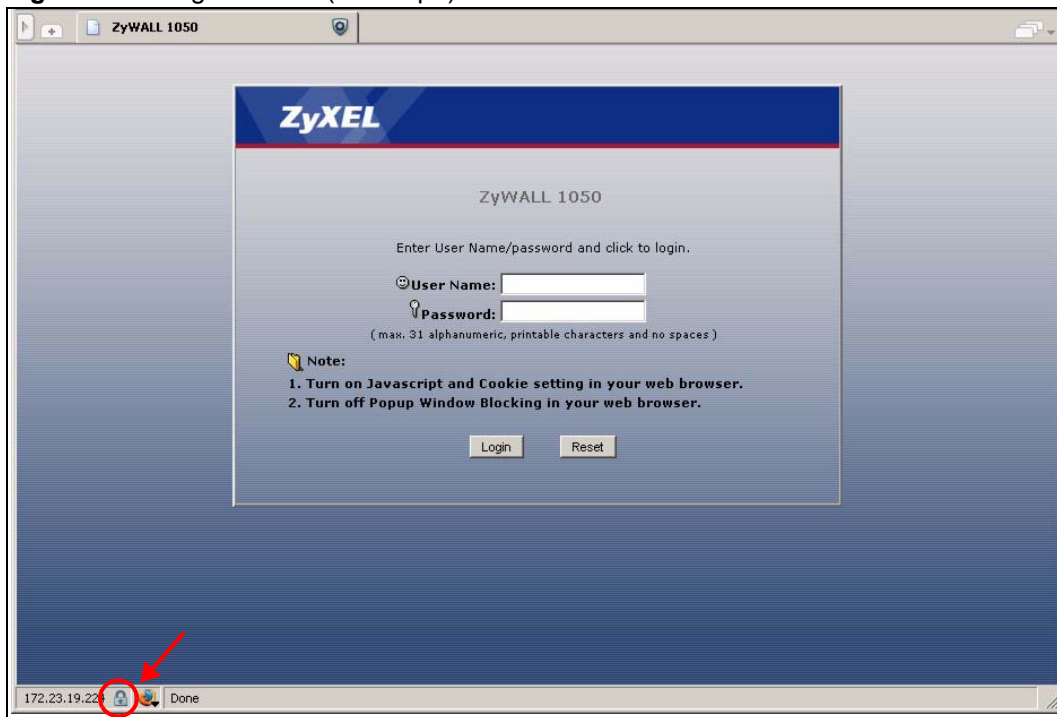


Figure 334 Login Screen (Netscape)



35.6 SSH

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

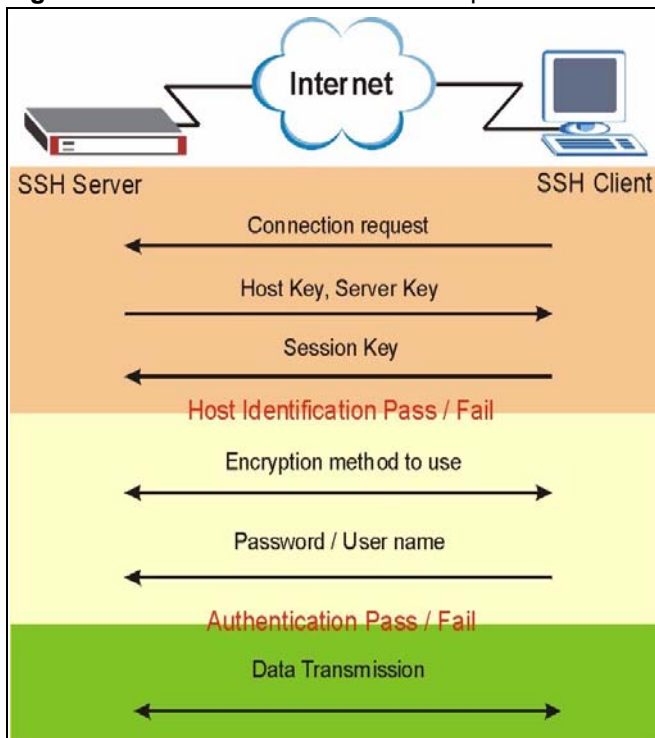
Figure 335 SSH Communication Example



35.6.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

Figure 336 How SSH v1 Works Example



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.

35.6.2 SSH Implementation on the ZyWALL

Your ZyWALL supports SSH versions 1 and 2 using RSA and DSA authentication and four encryption methods (AES, 3DES, Archfour and Blowfish). The SSH server is implemented on the ZyWALL for remote management on port 22 (by default).

35.6.3 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.

35.6.4 Configuring SSH

Click **Configuration > System > 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 337 System > SSH






The screenshot displays the SSH configuration page. At the top, there are checkboxes for 'Enable' (checked) and 'Version 1'. Below these are input fields for 'Server Port' (set to 22) and 'Server Certificate' (set to 'default'). A link '(See My Certificates)' is provided next to the certificate dropdown. The 'Service Control' section contains a table with the following data:

#	Zone	Address	Action	
1	ALL	ALL	Accept	[Edit] [Delete] [New]

At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 179 System > SSH

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the ZyWALL CLI using this service.
Version 1	Select the check box to have the ZyWALL use both SSH version 1 and version 2 protocols. If you clear the check box, the ZyWALL uses only SSH version 2 protocol.
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 Certificate	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 My Certificates screen (Click My Certificates and see Chapter 33 on page 469 for details).
Service Control	This specifies from which computers you can access which ZyWALL zones.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the Zone field (Accept) or not (Deny).
	Click the Add icon in the heading row to open a screen where you can add a new rule. Refer to Table 178 on page 509 for information on the fields.
	Click the Edit icon to go to the screen where you can edit the rule.
	Click the Add icon in an entry to add a rule below the current entry.
	Click the Delete icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.
	Click the Move to N icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

35.7 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.

35.7.1 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) 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 338 SSH Example 1: Store Host Key



Enter the password to log in to the ZyWALL. The CLI screen displays next.

35.7.2 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 339 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 340 SSH Example 2: Log in

```

$ ssh -l 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:

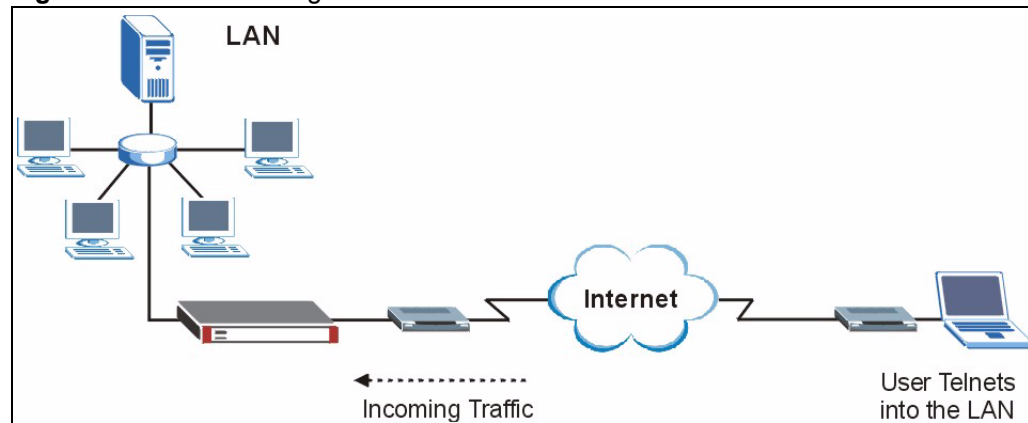
```

3 The CLI screen displays next.

35.8 Telnet

You can configure your ZyWALL for remote Telnet access as shown next.

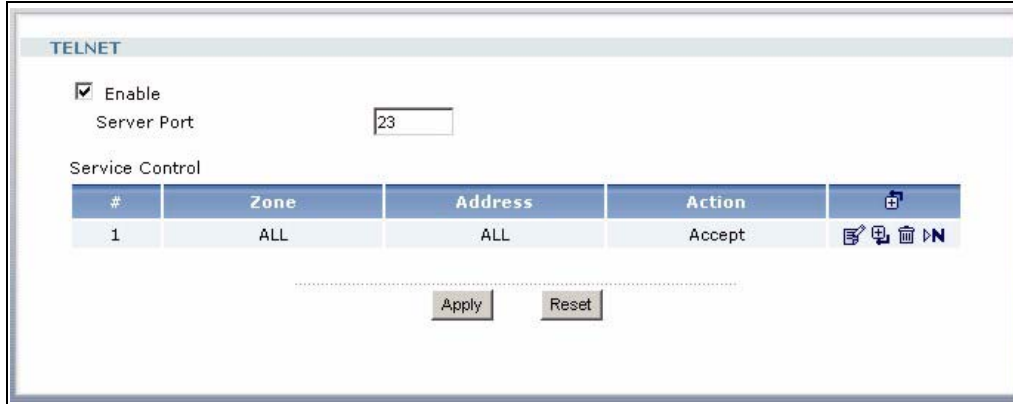
Figure 341 Telnet Configuration on a TCP/IP Network



35.8.1 Configuring Telnet






Click **Configuration > System > TELNET** to configure your ZyWALL for remote Telnet access.

Figure 342 System > Telnet



The following table describes the labels in this screen.

Table 180 System > Telnet

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the ZyWALL CLI using this service.
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.
Service Control	This specifies from which computers you can access which ZyWALL zones.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the Zone field (Accept) or not (Deny).
	Click the Add icon in the heading row to open a screen where you can add a new rule. Refer to Table 178 on page 509 for information on the fields.
	Click the Edit icon to go to the screen where you can edit the rule.
	Click the Add icon in an entry to add a rule below the current entry.
	Click the Delete icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.
	Click the Move to N icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.
Apply	Click Apply to ave your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

35.9 Configuring FTP

You can upload and download the ZyWALL's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. Please see [Chapter 9 on page 167](#) for more information about firmware and configuration files.

To change your ZyWALL's FTP settings, click **Configuration > System > FTP** tab. The screen appears as shown.

Figure 343 System > FTP

The screenshot shows the 'FTP' configuration page. It includes the following elements:






- Enable:** A checked checkbox.
- TLS required:** An unchecked checkbox.
- Server Port:** A text input field containing '21'.
- Server Certificate:** A dropdown menu set to 'default' with a link '(See My Certificates)'.
- Service Control:** A table with columns: #, Zone, Address, Action, and a plus icon.
- Buttons:** 'Apply' and 'Reset' buttons at the bottom.

The following table describes the labels in this screen.

Table 181 System > FTP

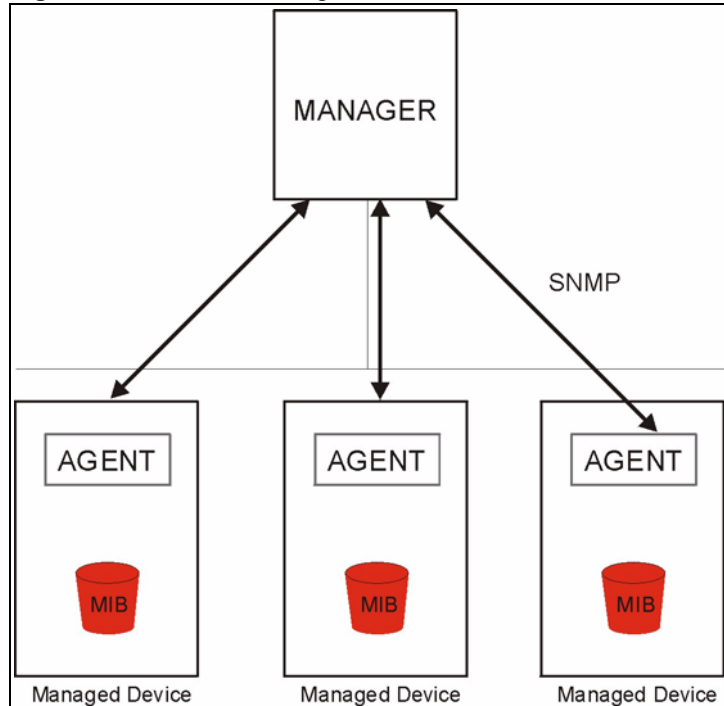
LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the ZyWALL using this service.
TLS required	Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
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 Certificate	Select the certificate whose corresponding private key is to be used to identify the ZyWALL for FTP connections. You must have certificates already configured in the My Certificates screen (Click My Certificates and see Chapter 33 on page 469 for details).
Service Control	This specifies from which computers you can access which ZyWALL zones.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the Zone field (Accept) or not (Deny).

Table 181 System > FTP (continued)

LABEL	DESCRIPTION
	Click the Add icon in the heading row to open a screen where you can add a new rule. Refer to Table 178 on page 509 for information on the fields.
	Click the Edit icon to go to the screen where you can edit the rule.
	Click the Add icon in an entry to add a rule below the current entry.
	Click the Delete icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.
	Click the Move to N icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.
Apply	Click Apply to save your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

35.10 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. 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) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 344 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.

35.10.1 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.

35.10.2 SNMP Traps

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

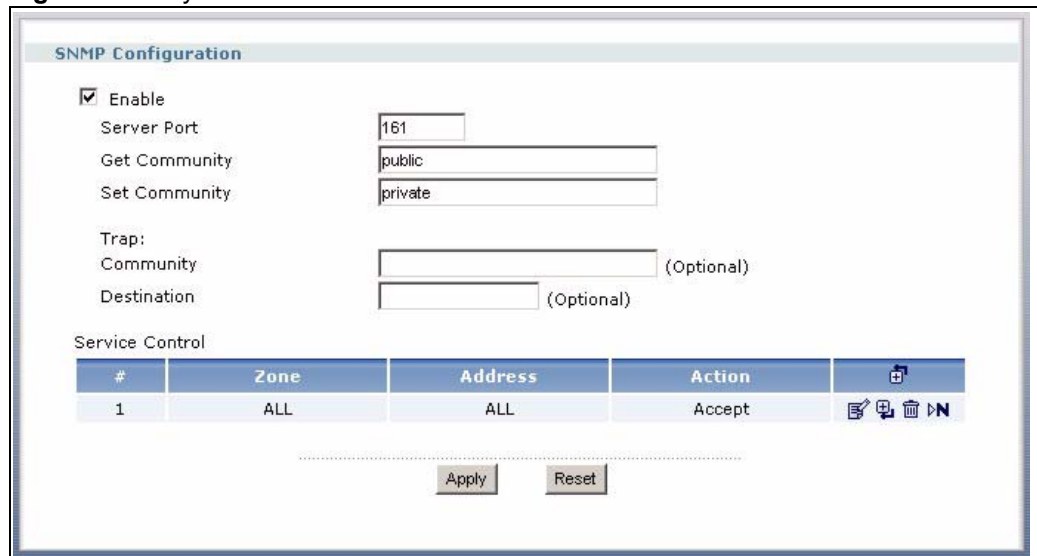
Table 182 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the ZyWALL is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

35.10.3 Configuring SNMP






To change your ZyWALL's SNMP settings, click **Configuration > System > SNMP** tab. The screen appears as shown.

Figure 345 System > SNMP



The following table describes the labels in this screen.

Table 183 System > SNMP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the ZyWALL using this service.
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.
Get Community	Enter the Get Community , 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 Set community , which is the password for incoming Set requests from the management station. The default is private 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.
Service Control	This specifies from which computers you can access which ZyWALL zones.
#	This the index number of the service control rule.
Zone	This is the zone on the ZyWALL the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the Zone field (Accept) or not (Deny).
	Click the Add icon in the heading row to open a screen where you can add a new rule. Refer to Table 178 on page 509 for information on the fields.
	Click the Edit icon to go to the screen where you can edit the rule.
	Click the Add icon in an entry to add a rule below the current entry.
	Click the Delete icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.
	Click the Move to N icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.
Apply	Click Apply to ave your changes back to the ZyWALL.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 36

Logs

This chapter provides information about the ZyWALL's logs.

The following table displays the maximum number of system log messages in the ZyWALL.

Table 184 Specifications: Logs

LABEL	DESCRIPTION
Maximum Number of Log Messages (System Log)	512
Maximum Number of Log Messages (Debug Log)	1024

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

36.1 View Log Screen

The **View Log** screen displays the current log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen.

Log messages are stored in two separate logs, one for regular log messages and one for debugging messages. In the regular log, you can look at all the log messages by selecting **All Logs**, or you can select a specific category of log messages (for example, firewall or user). You can also look at the debugging log by selecting **Debug Log**. All debugging messages have the same priority.

To access this screen, click **Maintenance > Log**. The log is displayed in the following screen.

Figure 346 Maintenance > Logs > View Log

#	Time	Priority	Category	Message	Source	Destination	Note
1	2006-01-26 19:13:39	info	IKE	IKE Packet Retransmit	172.23.19.244:500	5.5.5.5:500	IKE_LOG
2	2006-01-26 19:13:39	info	IKE	The cookie pair is : 0x5a31ab28aa0d235b / 0x0000000000000000	172.23.19.244:500	5.5.5.5:500	IKE_LOG
3	2006-01-26 19:13:24	info	IKE	IKE Packet Retransmit [count=4]	172.23.19.244:500	5.5.5.5:500	IKE_LOG
4	2006-01-26 19:13:24	info	IKE	Send:[SA][VID][VID] [VID][VID][VID][VID] [VID][VID][VID]	172.23.19.244:500	5.5.5.5:500	IKE_LOG
5	2006-01-26 19:13:24	info	IKE	Send Main Mode request to [5.5.5.5]	172.23.19.244:500	5.5.5.5:500	IKE_LOG
6	2006-01-26 19:13:24	info	IKE	Tunnel [WIZ_VPN] Sending IKE request	172.23.19.244:500	5.5.5.5:500	IKE_LOG

If an event generates log messages and alerts, it is displayed in red. Otherwise, it is displayed in black. The following table describes the labels in this screen.

Table 185 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the Display , Email Log Now , Refresh , and Clear Log fields are available. If the filter settings are shown, the Display , Priority , Source Address , Destination Address , Service , Keyword , and Search fields are available.
No Filter	These fields are displayed when you hide the filter.
Display	Select the log(s) you want to view. You can also view All Logs on one screen, or you can view the Debug Log . The screen is updated right after you change the selection.
Email Log Now	Click this button to send the selected log message(s) to the Active e-mail address(es) specified in the Send Log To field on the Log Settings page. (See Table 186 on page 529 or Table 187 on page 531 for more information about these fields.)
Refresh	Click this button to update the information on the log screen.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
Filter	These fields are displayed when you show the filter. When the filter is shown, the filter criteria are not applied until you click the Search button.
Display	Select the log message(s) you want to view. You can also view All Logs at one time, or you can view the Debug Log .

Table 185 Maintenance > Logs > View Log (continued)

LABEL	DESCRIPTION
Priority	This field is read-only if the Category is Debug Log . Select the lowest-priority log messages you would like to see. The log will display every log message with this priority or higher. Choices are: emerg , alert , crit , error , warn , notice , and info , from highest priority to lowest priority.
Source Address	Type the IP address of the source of the incoming packet when the log message was generated. Do not include the port in this filter.
Destination Address	Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Service	Select the service whose log messages you would like to see. The web configurator uses the protocol and destination port number(s) of the service to select which log messages you see.
Keyword	Type a keyword to look for in the Message , Source , Destination and Note fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks () ' ; : ! + - * / = # \$ % @ ; the period, double quotes, and brackets are not allowed.
Search	Click this button to update the log using the current filter settings.
entries per page	Select the number of log messages you would like to see on one screen. Choices are: 30 , 50 , and 80 .
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the Priority field above.
Category	This field displays the log that generated the log message. It is the same value used in the Display and (other) Category fields.
Message	This field displays the reason the log message was generated. The text "[count=x]", where x is a number, appears at the end of the Message field if log consolidation is turned on (see Log Consolidation in Table 187 on page 531) and multiple entries were aggregated to generate into this one.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Note	This field displays any additional information about the log message.

The Web configurator saves the filter settings if you leave the **View Log** screen and return to it later.

36.2 Log Settings Screens

The **Log Settings** screens control log messages and alerts. A log message stores the information for viewing (for example, in the **View Log** tab) or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The ZyWALL provides a system log and supports e-mail profiles and remote syslog servers. The system log is available on the **View Log** tab, the e-mail profiles are used to mail log messages to the specified destinations, and the other four logs are stored on specified syslog servers.

The **Log Settings** tab also controls what information is saved in each log. For the system log, you can also specify which log messages is e-mailed, where it is e-mailed, and how often it is e-mailed.











For alerts, the **Log Settings** tab controls which events generate alerts and where alerts are e-mailed.

The **Log Settings Summary** screen provides a summary of all the settings. You can use the **Log Settings Edit** screen to maintain the detailed settings (such as log categories, e-mail addresses, server names, etc.) for any log. Alternatively, if you want to edit what events is included in each log, you can also use the **Active Log Summary** screen to edit this information for all logs at the same time.

36.3 Log Settings Summary

To access this screen, click **Maintenance > Log > Log Settings**.

Figure 347 Maintenance > Logs > Log Setting

#	Name	Log Format	Summary	Modify
1	System Log	Internal	Mail Server : Mail Subject : Send From : Send Log to : Send Alert to : Schedule : Send log weekly on Sunday at 00 : 00	 
2	Remote Server 1	ZyXEL VRPT.	Server Address: Log Facility: Local 1	 
3	Remote Server 2	ZyXEL VRPT.	Server Address: Log Facility: Local 1	 
4	Remote Server 3	ZyXEL VRPT.	Server Address: Log Facility: Local 1	 
5	Remote Server 4	ZyXEL VRPT.	Server Address: Log Facility: Local 1	 

The following table describes the labels in this screen.

Table 186 Maintenance > Logs > Log Setting

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific log.
Name	This field displays the name of the log (system log or one of the remote servers).
Log Format	This field displays the format of the log. Formats are Internal and ZyXEL VRPT . Internal - system log; you can view the log on the View Log tab. ZyXEL VRPT - syslog-compatible format.
Summary	This field is a summary of the settings for each log. Please see Section 36.3.1 on page 529 for more information.
Modify	This column provides icons to activate or deactivate logs and to modify the settings. To activate or deactivate a log, click the Active icon. To edit the settings, click the Edit icon next to the associated log. The Log Settings Edit screen appears.
Active Log Summary	Click this button to open the Active Log Summary Edit screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

36.3.1 Log Settings Edit E-mail

The **Log Settings Edit** screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Go to the **Log Settings Summary** screen (see [Section 36.3 on page 528](#)), and click the appropriate **Edit** icon.

Figure 348 Maintenance > Logs > Log Setting > E-mail > Edit

E-mail Server 1

Active

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject:

Send From: (E-Mail Address)

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Sending Log: (Dropdown)

Day for Sending Log: (Dropdown)

Time for Sending Log: (Hour) (Minute)

SMTP Authentication

User Name:

Password:

E-mail Server 2

Active

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject:

Send From: (E-Mail Address)

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Sending Log: (Dropdown)

Day for Sending Log: (Dropdown)

Time for Sending Log: (Hour) (Minute)

SMTP Authentication

User Name:

Password:

Active Log and Alert

Log Category	System log	E-mail Server 1	E-mail Server 2
	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
All Logs	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Content Filter	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Content Filter Forward	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
User	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
MyZyXEL.com	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
ZySH	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
IDP	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Application Patrol	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
IKE	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
IPSec	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Firewall	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Sessions Limit	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Policy Route	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Built-in Service	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
System	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Connectivity Check	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Device HA	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Routing Protocol	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
NAT	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
PKI	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Interface	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Account	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Port Grouping	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Force Authentication	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
File Manager	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Default	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Log Consolidation

Active

Log Consolidation Interval (seconds): (10 - 600)

The following table describes the labels in this screen.

Table 187 Maintenance > Logs > Log Setting > E-mail > Edit

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the Active Log and Alert section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Type the subject line for the outgoing e-mail.
Send From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Send Log To	Type the e-mail address to which the outgoing e-mail is delivered.
Send Alerts To	Type the e-mail address to which alerts are delivered.
Sending Log	Select how often log information is e-mailed. Choices are: When Full , Hourly , Daily , and Weekly .
Day for Sending Log	This field is available if the log is e-mailed Weekly . Select the day of the week the log is e-mailed.
Time for Sending Log	This field is available if the log is e-mailed Weekly or Daily . Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the SMTP Authentication check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the SMTP Authentication check box. Type the password to provide to the SMTP server when the log is e-mailed.
Active Log and Alert	
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
System log	Select which events you want to log by Log Category (except All Logs ; see below). There are three choices: Disable All Logs (red X) - do not log any information from this category Enable Normal Logs (green checkmark) - create log messages and alerts from this category Enable All Logs (yellow checkmark) - create log messages, alerts, and debugging information from this category; the ZyWALL does not e-mail debugging information, however, even if this setting is selected. If you select one of the check boxes for All Logs , it affects the settings for every category.
E-mail Server 1	Select whether this category of events should be included in the log messages when it is e-mailed (green checkmark) and/or in alerts (yellow exclamation point) for the e-mail settings specified in E-Mail Server 1 . The ZyWALL does not e-mail debugging information, even if it is recorded in the System log .

Table 187 Maintenance > Logs > Log Setting > E-mail > Edit (continued)

LABEL	DESCRIPTION
E-mail Server 2	Select whether this category of events should be included in log messages when it is e-mailed (green checkmark) and/or in alerts (yellow exclamation point) for the e-mail settings specified in E-Mail Server 2 . The ZyWALL does not e-mail debugging information, even if it is recorded in the System log .
Log Consolidation	
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified Log Consolidation Interval . In the View Log tab, the text “[count=x]”, where x is the number of original log messages, is appended at the end of the Message field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text “[count=x]”, where x is the number of original log messages, appended at the end of the Message field.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

36.3.2 Log Settings Edit syslog

The **Log Settings Edit** screen controls the detailed settings for each log in the remote server (syslog). Go to the **Log Settings Summary** screen (see [Section 36.3 on page 528](#)), and click the appropriate **Edit** icon.

Figure 349 Maintenance > Logs > Log Setting > Remote Server > Edit

Log Settings for Remote Server 1

Active

Log Format: ZyXEL VRPT.

Server Address: (Server Name or IP Address)

Log Facility:

Active Log

Log Category	Selection		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Content Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Content Filter Forward	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
User	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
MyZyXEL.com	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ZySH	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IDP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Application Patrol	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IKE	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IPSec	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Firewall	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sessions Limit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Policy Route	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Built-in Service	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Connectivity Check	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Device HA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Routing Protocol	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
NAT	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PKI	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Interface	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port Grouping	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Force Authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Traffic Log	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
File Manager	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Default	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The following table describes the labels in this screen.

Table 188 Maintenance > Logs > Log Setting > Remote Server > Edit

LABEL	DESCRIPTION
Log Settings for Remote Server 1	
Active	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the Active Log section.

Table 188 Maintenance > Logs > Log Setting > Remote Server > Edit (continued)

LABEL	DESCRIPTION
Log Format	This field displays the format of the log information. It is read-only. Internal - system log; you can view the log on the View Log tab. ZyXEL VRPT - syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each Log Category (except All Logs ; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green checkmark) - log regular information and alerts from this category enable all logs (yellow checkmark) - log regular information, alerts, and debugging information from this category If you check one of the check boxes for All Logs , it affects the settings for every category.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

36.3.3 Active Log Summary

The **Active Log Summary** screen allows you to view and to edit what information is included in the system log, e-mail profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is e-mailed or remote server names). To access this screen, go to the **Log Settings Summary** screen (see [Section 36.3 on page 528](#)), and click the **Active Log Summary** button.

Figure 350 Active Log Summary

Active Log Summary								
Log Category	System log	E-mail Server 1	E-mail Server 2	Remote Server 1	Remote Server 2	Remote Server 3	Remote Server 4	
	-	E-mail	E-mail	ZyXEL VRPT.	ZyXEL VRPT.	ZyXEL VRPT.	ZyXEL VRPT.	
	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
All Logs	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Content Filter	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Content Filter Forward	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
User	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
MyZyXEL.com	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
ZySH	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
IDP	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Application Patrol	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
IKE	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
IPSec	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Firewall	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Sessions Limit	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Policy Route	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Built-in Service	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
System	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Connectivity Check	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Device HA	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Routing Protocol	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
NAT	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
PKI	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Interface	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Account	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Port Grouping	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Force Authentication	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Traffic Log	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
File Manager	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Default	<input type="radio"/> <input type="radio"/> <input checked="" type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>

This screen provides a different view and a different way of indicating which messages are included in each log and each alert. Please see [Section 36.3.1 on page 529](#), where this process is discussed. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 189 Maintenance > Logs > Log Setting > Active Log Summary

LABEL	DESCRIPTION
Active Log Summary	
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each Log Category (except All Logs ; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green checkmark) - log regular information and alerts from this category enable all logs (yellow checkmark) - log regular information, alerts, and debugging information from this category If you check one of the check boxes for All Logs , it affects the settings for every category.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

CHAPTER 37

Reports

This chapter provides information about the report screen, active session screen, and associated commands.

37.1 Report Screen

The **Report** screen provides basic information about the following metrics:

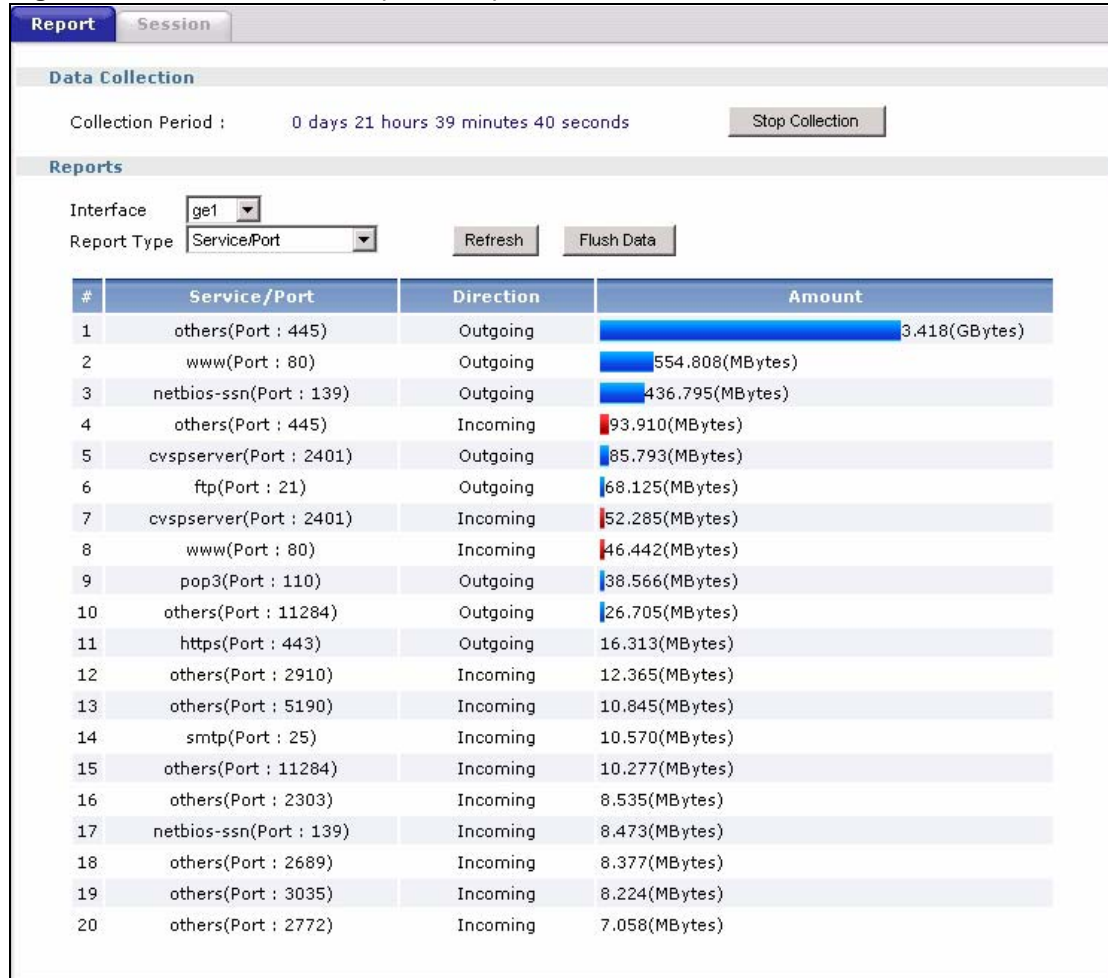
- Most-visited Web sites and the number of times each one was visited. This count may not be accurate in some cases because the ZyWALL counts HTTP GET packets. Please see [Table 190 on page 538](#) for more information.
- Most-used protocols or service ports and the amount of traffic on each one
- LAN IP with heaviest traffic and how much traffic has been sent to and from each one

Note: The reporting may decrease the overall throughput through the ZyWALL.

You use the **Report** screen to tell the ZyWALL when to start and when to stop collecting information for these reports. You cannot schedule data collection; you have to start and stop it manually in the **Report** screen.

To access the **Report** screen, login to the web configurator. When the main screen appears, click **Maintenance > Report**.

Figure 351 Maintenance > Report > Report



There is a limit on the number of records shown in the report. Please see [Table 191 on page 540](#) for more information. The following table describes the labels in this screen.

Table 190 Maintenance > Report > Report

LABEL	DESCRIPTION
Data Collection	
Collection Period	This field displays how long the ZyWALL collected information. If the ZyWALL is currently collecting information, the progress is not tracked here real-time, but you can click the Refresh button to update it.
Start / Stop Collection	Click this button to tell the ZyWALL to start or stop collecting data for the report.
Reports	
Interface	Select the interface from which to collect information. You can collect information from Ethernet, VLAN, bridge, PPPoE/PPTP, and auxiliary interfaces.

Table 190 Maintenance > Report > Report (continued)

LABEL	DESCRIPTION
Report Type	<p>Select the type of report to display. Choices are:</p> <p>IP Address/User - displays the IP addresses or users with the most traffic and how much traffic has been sent to and from each one.</p> <p>Service/Port - displays the most-used protocols or service ports and the amount of traffic for each one.</p> <p>Web Site - displays the most-visited Web sites and how many times each one has been visited.</p> <p>Each type of report has different information in the report (below).</p>
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard the report data for the selected interface and update the report display.
	These fields are available when the Report Type is IP Address/User .
#	This field is the rank of each record. The IP addresses and users are sorted by the amount of traffic.
IP Address/ User	This field displays the IP address or user in this record. The maximum number of IP addresses or users in this report is indicated in Table 191 on page 540 .
Direction	<p>This field indicates whether the IP address or user is sending or receiving traffic. Choices are Incoming and Outgoing.</p> <p>Incoming - traffic is coming from the IP address or user to the ZyWALL.</p> <p>Outgoing - traffic is going from the ZyWALL to the IP address or user.</p>
Amount	This field displays how much traffic was sent or received from the indicated IP address or user. If the Direction is Incoming , a red bar is displayed; if the Direction is Outgoing , a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes or Gbytes, depending on the amount of traffic for the particular IP address or user. The count starts over at zero if the number of bytes passes the byte count limit. See Table 191 on page 540 .
	These fields are available when the Report Type is Service/Port .
#	This field is the rank of each record. The protocols and service ports are sorted by the amount of traffic.
Service/Port	This field displays the protocol or service port in this record. The maximum number of protocols or service ports in this report is indicated in Table 191 on page 540 .
Direction	<p>This field indicates whether the indicated protocol or service port is sending or receiving traffic. Choices are Incoming and Outgoing.</p> <p>Incoming - traffic is coming into the router through the interface</p> <p>Outgoing - traffic is going out from the router through the interface</p>
Amount	This field displays how much traffic was sent or received from the indicated service / port. If the Direction is Incoming , a red bar is displayed; if the Direction is Outgoing , a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes, Gbytes, or Tbytes, depending on the amount of traffic for the particular protocol or service port. The count starts over at zero if the number of bytes passes the byte count limit. See Table 191 on page 540 .
	These fields are available when the Report Type is Web Site .
#	This field is the rank of each record. The domain names are sorted by the number of hits.

Table 190 Maintenance > Report > Report (continued)

LABEL	DESCRIPTION
Web Site	This field displays the domain names most often visited. The ZyWALL counts each page viewed on a Web site as another hit. The maximum number of domain names in this report is indicated in Table 191 on page 540 .
Hits	This field displays how many hits the Web site received. The ZyWALL counts hits by counting HTTP GET packets. Many Web sites have HTTP GET references to other Web sites, and the ZyWALL counts these as hits too. The count starts over at zero if the number of hits passes the hit count limit. See Table 191 on page 540 .

The following table displays the maximum number of records shown in the report, the byte count limit, and the hit count limit.

Table 191 Maximum Values for Reports

LABEL	DESCRIPTION
Maximum Number of Records	20
Byte Count Limit	2 ⁶⁴ bytes; this is just less than 17 million terabytes.
Hit Count Limit	2 ⁶⁴ hits; this is over 1.8 x 10 ¹⁹ hits.

37.2 Session Screen

The **Session** screen displays information about active sessions for debugging or statistical analysis. It is not possible to manage sessions in this screen. The following information is displayed.

- User who started the session
- Protocol or service port used
- Source address
- Destination address
- Number of bytes received (so far)
- Number of bytes transmitted (so far)
- Duration (so far)

You can look at all the active sessions by user or by service, or you can filter the information by user, protocol / service or service group, source address, and/or destination address and view it by user.

To access this screen, login to the web configurator. When the main screen appears, click **Maintenance > Report > Session**. The following screen appears.

Figure 352 Maintenance > Report > Session

Service	User	Source	Destination	Rx	Tx	Duration
Any_UDP	-	192.168.105.27:21613	172.17.2.5:161	218(Bytes)	662(Bytes)	
	-	172.21.119.1:137	172.23.5.1:53	109(Bytes)	106(Bytes)	11
	-	192.168.105.27:21613	172.17.2.1:161	0(Bytes)	225(Bytes)	11
	-	172.21.119.1:137	172.23.5.2:53	109(Bytes)	106(Bytes)	11
	-			0(Bytes)	225(Bytes)	7
Any_TCP						
DNS_UDP						
HTTP						
HTTPS						
MSN						
NetBIOS_TCP1						
POP3						
ROADRUNNER_TCP						
SNMP_UDP						
MS_RPC						

The following table describes the labels in this screen.

Table 192 Maintenance > Report > Session

LABEL	DESCRIPTION
View	Select how you want the information to be displayed. Choices are: sessions by users - display all active sessions by user sessions by services - display all active sessions by service or protocol all sessions - filter the active sessions by the User , Service , Source Address , and Destination Address , and display them by user The User , Service , Source Address , and Destination Address fields are only available when all sessions is selected.
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open and close the screen.
	The User , Service , Source Address , and Destination Address fields have no effect until you click the Search button, even if you click the Refresh button.
User	This field is only available when all sessions is selected. Type the user whose sessions you want to view. It is not possible to type part of the user name or use wildcards in this field; you must enter the whole user name.
Service	This field is only available when all sessions is selected. Select the service or service group whose sessions you want to view. The ZyWALL identifies the service by comparing the protocol and destination port of each packet to the protocol and port of each services that is defined. (See Chapter 29 on page 443 for more information about services.)
Source Address	This field is only available when all sessions is selected. Type the source IP address whose sessions you want to view. You cannot include the source port.
Destination Address	This field is only available when all sessions is selected. Type the destination IP address whose sessions you want to view. You cannot include the destination port.

Table 192 Maintenance > Report > Session (continued)

LABEL	DESCRIPTION
Search	Click this button to update the information on the screen using the filter criteria in the User , Service , Source Address , and Destination Address fields.
sessions per page	Select the number of active sessions displayed on each page. You can use the arrow keys on the right to change pages.
User	This field displays the user in each active session. If you are looking at the sessions by users or all sessions report, click the blue plus sign (+) next to each user to look at detailed session information by protocol.
Protocol Service	This field displays the protocol used in each active session. If you are looking at the sessions by services report, click the blue plus sign (+) next to each protocol to look at detailed session information by user.
Source	This field displays the source IP address and port in each active session.
Destination	This field displays the destination IP address and port in each active session.
Rx	This field displays the amount of information received by the source in the active session.
Tx	This field displays the amount of information transmitted by the source in the active session.
Duration	This field displays the length of the active session in seconds.

CHAPTER 38

Reboot

Use this to restart the device (for example, if the device begins behaving erratically). See also [Section 1.4 on page 50](#) for information on different ways to start and stop the ZyWALL.

If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Reboot is different to reset; (see [Section 1.5 on page 50](#)) reset returns the device to its default configuration.

The **Reboot** screen is part of the Web configurator so that remote users can restart the device. To access this screen, click **Maintenance > Reboot**.

Figure 353 Maintenance > Reboot



Click the **Reboot** button to restart the device. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

You can also use the CLI command `reboot` to restart the device.

Appendix A

Product Specifications

The following specifications are subject to change without notice. See the **Introduction** chapter for a general overview of key features.

This table provides basic device specifications.

Table 193 Device Specifications

ATTRIBUTE	SPECIFICATION
Default IP Address (ge1)	192.168.1.1
Default Subnet Mask (ge1)	255.255.255.0 (24 bits)
Default Password	1234

This table provides hardware specifications.

Table 194 Hardware Specifications

FEATURE	SPECIFICATION
Memory Size	512MB system memory, 256MB Flash
Number of MAC addresses	5
Ethernet Interfaces	Five Gigabit Ethernet, full duplex RJ-45 connectors Auto-crossover, auto-MDI/MDIX
Management interface	RS-232, DB9F connector
DIAL BACKUP port	RS-232, DB9M connector
USB	2, 2.0 plug and play
Power Requirements	100-240 V AC, 50/60 Hz, 1 A Max
Operating Requirements	Temperature: 0 C to 40 C Humidity: 5% to 90% (non-condensing)
Storage Requirements	Temperature: 0 C to 40 C Humidity: 5% to 90% (non-condensing)
Dimensions	430.7(W) x 292.0(D) x 43.5(H) mm
Weight	4.7 kg
Rack-mounting	Rack-mountable (rack-mount kit included)

Appendix B

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 195 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. www.zyxel.com) 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 195 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 195 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 C

Open Software Announcements

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

Note: This Product includes ppp-2.4.2 software under the PPP License.

PPP License

Copyright (c) 1993 The Australian National University.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the Australian National University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (c) 1989 Carnegie Mellon University.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Note: This Product includes Netkit Telnet -0.17 software under the Netkit Telnet License

Netkit Telnet License

Copyright (c) 1989 Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1.Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3.Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note: This Product includes openssh-3.0.2p1 software under the OpenSSH License

OpenSSH License

Copyright by Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1.Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The name of the above contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Note: This Product includes ntp-4.1.2 software under the NTP License

NTP License

Copyright (c) David L. Mills 1992-2004

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

Note: This Product includes expat-1.95.6 software under the Expat License

Expat License

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including

without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Note: This Product includes libtecla-1.6.1 software under the an X11-style License

X11-style license

This is a Free Software License

- This license is compatible with The GNU General Public License, Version 1
- This license is compatible with The GNU General Public License, Version 2

This is just like a Simple Permissive license, but it requires that a copyright notice be maintained.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

Note: This Product includes openssl-0.9.7d software under the OpenSSL License

OpenSSL

TN3270 Plus and SDI FTP SSL utilize the “OpenSSL toolkit” functionality provided by “The Open SSL Project” at <http://www.openssl.org>. SDI Limited acknowledges all patent rights therein.”

The OpenSSL toolkit is licensed under a dual-license (the OpenSSL license and the original SSLeay license). See the license text below.

OPENSSL licence

Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1.Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3.All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org>)
- 4.The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org
- 5.Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
- 6.Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN

CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric

Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

SSLey licence

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.

Note: This Product includes libevent-1.1a and xinetd-2.3.14 software under the a 3-clause BSD License

A 3-Clause BSD-style license

This is a Free Software License

- This license is compatible with The GNU General Public License, Version 1
- This license is compatible with The GNU General Public License, Version 2

This is the BSD license without the obnoxious advertising clause. It's also known as the "modified BSD license." Note that the University of California now prefers this license to the BSD license with advertising clause, and now allows BSD itself to be used under the three-clause license.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of [original copyright holder] nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT

LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note: This Product includes bind-9.2.3 and dhcp-3.0.3 software under the ISC License

The ISC license for bind is:

Copyright (c) 1993-1999 by Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Internet Software Consortium

950 Charter Street

Redwood City, CA 94063

Tel: 1-888-868-1001

Fax: 1-650-779-7055

E-mail: licensing@isc.org

Note: This Product includes Dhcp -3.0.3 software under the DHCP License

The DHCP license Terms

Copyright (c) 1996-1999 Internet Software Consortium.

Use is subject to license terms which appear in the file named ISC-LICENSE that should have accompanied this file when you received it. If a file named ISC-LICENSE did not accompany this file, or you are not sure the one you have is correct, you may obtain an applicable copy of the license at:

<http://www.isc.org/isc-license-1.0.html>

This file is part of the ISC DHCP distribution. The documentation associated with this file is listed in the file DOCUMENTATION, included in the top-level directory of this release.

Support and other services are available for ISC products - see <http://www.isc.org> for more information.

Note: This Product includes httpd-2.0.55 software developed by the Apache Software Foundation under Apache License.

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

“License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

“Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

“Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

“You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License.

“Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

“Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

“Work” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

“Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

“Contribution” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.”

“Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works hereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Version 1.1

Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <<http://www.apache.org/>>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

Note: This Product includes libosip2 and libgcgi-0.9.5 software under LGPL license.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the “Lesser” General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a “work based on the library” and a “work that uses the library”. The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License”).

Each licensee is addressed as “you”.

A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The “Library”, below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification”.)

“Source code” for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this

License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”. The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a “work that uses the Library” with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the “work that uses the Library” must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed

through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS.

Note: This Product includes bridge-utils, dhcpcd-1.3.22-pl4, rp-pppoe-3.5, vlan-1.8, keepalived-1.1.11-p1, L7 Filter, snort, dietlibc, quagga-0.99.2, ez-ipupdate-3.0.11b7, proftpd-1.2.10, pam-0.76, tzcode2006c, iproute2, iptables-1.2.11/netfilter(kernel), dhcp-helper, busybox, Linux kernel, and pptp-linux-1.4.0 software under GPL license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Note: This Product include pcre, libpcap, libnet, libnet-1.1.2.1, net-snmp-5.1.1, libpcap-0.9.4, and openssl-3.0.2p1 software under BSD license

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note: This Product includes libxml2-2.6.8 software under the MIT License

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Note: This Product include openldap-2.1.10 software under the OpenLDAP License

The Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation (“Software”), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Note: Some components of the ZYWALL 1050 incorporate source code covered under the Apache License, GPL License, LGPL License, BSD License, Open SSL License, OpenLDAP License, X11-style License, A 3 clause BSD License, NTP License, Expat License, PPP License, Netkit-telnet License and MIT License. To obtain the source code covered under those Licenses, please contact ZyXEL Communications Corporation at: ZyXEL Technical Support.

End-User License Agreement for “ZYWALL 1050”

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1. Grant of License for Personal Use

ZyXEL Communications Corp. (“ZyXEL”) grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the “Software”), including any documentation files accompanying the Software (“Documentation”), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2. Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3. Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4. Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. You may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing.

5. Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6. No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7. Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL'S

AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED \$1,000. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

12.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in Taiwan (ROC). This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall

only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Index

Numerics

3DES [240](#)

A

AAA servers [455](#)

and authentication methods [465](#)

and users [424](#)

LDAP Default [457](#)

LDAP Group [458](#)

LDAP Group members [461](#)

LDAP. See also LDAP.

RADIUS Default [461](#)

RADIUS Group [462](#)

RADIUS Group members [464](#)

RADIUS. See also RADIUS.

where used [117](#)

access control [340](#)

access users [423](#), [425](#)

forcing login [425](#)

forcing login. See also force user authentication policies.

idle timeout [432](#)

in user-aware policies [425](#)

logging in [425](#)

multiple logins [432](#)

see also users [423](#)

web configurator [434](#)

action (IDP) [344](#)

active protocol [224](#)

AH [224](#)

and encapsulation [225](#)

ESP [224](#)

active sessions. See sessions.

ActiveX [390](#)

address groups [437](#)

and content filtering [375](#), [376](#), [380](#)

and firewall [316](#)

and force user authentication policies [434](#)

and FTP [519](#)

and SNMP [523](#)

and SSH [515](#)

and Telnet [518](#)

and WWW [509](#)

where used [116](#)

address objects [437](#)

and content filtering [375](#), [376](#), [380](#)

and firewall [316](#)

and force user authentication policies [434](#)

and FTP [519](#)

and NAT [296](#)

and policy routes [295](#), [296](#)

and SNMP [523](#)

and SSH [515](#)

and Telnet [518](#)

and virtual servers [406](#)

and VPN connections [228](#)

and WWW [509](#)

HOST [437](#)

RANGE [437](#)

SUBNET [437](#)

types of [437](#)

where used [116](#)

admin users [423](#)

multiple logins [432](#)

see also users [423](#)

Advanced Encryption Standard. See AES.

AES [240](#)

AH [224](#)

and transport mode [225](#)

alerts [527](#), [528](#), [531](#), [534](#), [535](#), [536](#)

IDP [343](#)

ALG

and NAT [413](#)

H.323 [413](#), [414](#)

see also VoIP pass through.

SIP [413](#), [415](#)

SIP timeout [416](#)

anomaly sensitivity [353](#)

Apache server [354](#), [355](#)

Application Layer Gateway. See ALG.

application patrol [321](#)

actions [321](#)

and firewall [321](#)

and HTTP redirect [409](#)

bandwidth management [322](#)

classification [321](#)

configuration overview [113](#)

exceptions [322](#)

port-base [321](#)

port-less [321](#)

prerequisites [113](#)

unidentified applications [322](#)

vs firewall [302](#)

applications [55](#)

ASCII-encoding [354](#)

asymmetrical routes [307](#)
vs virtual interfaces [307](#)

asymmetrical routes (firewall) [308](#), [311](#), [313](#)

authentication algorithms [239](#), [240](#), [256](#)
and active protocol [239](#)
and routing protocols [256](#)
MD5 [240](#), [256](#)
SHA1 [240](#)
text [256](#)

Authentication Header. See AH.

authentication methods [465](#), [466](#)
and AAA servers [465](#)
and IKE SA [465](#)
and users [424](#)
and WWW [465](#), [508](#)
where used [117](#)

authentication objects
create [466](#)
example [467](#)

Authentication, Authorization, Accounting servers. See AAA servers.

auxiliary interface [178](#), [211](#)
when used [211](#)

B

backdoor [340](#)

backup
configuration files [170](#)

bad-length-options [355](#)

bandwidth management
and policy routes [297](#)
in application patrol [322](#)
interface, outbound. See interfaces.
OSI level-7. See application patrol.

bandwidth management. See also policy routes.

Bare byte encoding [354](#)

base profiles [336](#), [337](#)

base36-encoding [354](#)

bindings [335](#)

Blaster [333](#)

boot module [173](#)

bridge interfaces [177](#), [201](#)
and virtual interfaces of members [201](#)
basic characteristics [178](#)
effect on routing table [201](#)
member interfaces [201](#)
virtual [213](#)

bridges [200](#)

BSMI [4](#)

buffer overflow [340](#)

C

CA [469](#)
and certificates [470](#)

CE Mark [4](#)

Certificate Management Protocol (CMP) [476](#)

Certificate Revocation List (CRL) [470](#)
vs OCSP [482](#)

certificates [469](#)
advantages [470](#)
and CA [470](#)
and FTP [519](#)
and HTTPS [504](#)
and IKE SA [244](#)
and SSH [515](#)
and synchronization (device HA) [281](#)
and VPN gateways [229](#)
and WWW [506](#)
certification path [470](#), [479](#), [485](#)
expired [470](#)
factory-default [470](#)
file formats [470](#)
fingerprints [480](#), [486](#)
importing [474](#)
in the VPN wizard [96](#)
not used for encryption [469](#)
revoked [470](#)
self-signed [470](#), [476](#)
serial number [479](#), [485](#)
storage space [473](#), [482](#)
thumbprint algorithms [471](#)
thumbprints [471](#)
used for authentication [469](#)
verifying fingerprints [471](#)
where used [117](#)

Certification Authority. See CA.

certification requests [469](#), [476](#)

certifications [4](#)

CLI [49](#)

cold start [50](#)

configuration
benefits of granularity [105](#)
granularity [105](#)

configuration files [167](#), [169](#)
at restart [169](#)
backup [170](#)
downloading [171](#)
downloading with FTP [519](#)
editing [169](#)
lastgood.conf [169](#)
managing [170](#)
not stopping or starting the ZyWALL [50](#)
startup-config.conf [169](#)
startup-config-bad.conf [169](#)
syntax [167](#)
system-default.conf [169](#)

- uploading [172](#)
- uploading with FTP [519](#)
- use without restart [169](#)
- way the ZyWALL runs [168](#)
- console port [49](#)
 - speed [494](#)
- contact information [8](#)
- content (pattern) [366](#)
- content filtering [375, 376](#)
 - and address groups [375, 376, 380](#)
 - and address objects [375, 376, 380](#)
 - and registration [378, 382](#)
 - and schedules [375, 376, 380](#)
 - and user groups [375, 380](#)
 - and users [375, 380](#)
 - by category [375, 381, 384](#)
 - by keyword (in URL) [376, 391](#)
 - by URL [376, 390](#)
 - by web feature [375, 390](#)
- cache [382, 391](#)
- categories [384](#)
- configuration overview [114](#)
- default policy [376, 377](#)
- external web filtering service [382, 384](#)
- filter list [376](#)
- license status [158](#)
- message for blocked access [378](#)
- policies [375, 376](#)
- prerequisites [114](#)
- registration status [166, 378, 379, 383](#)
- reports. See content filtering reports.
- submitting web sites [400](#)
- testing [388](#)
- trial service activation [165](#)
- uncategorized pages [384](#)
- upgrading license [166](#)
- URL for blocked access [378](#)
- content filtering reports [395](#)
 - and registration [395](#)
 - during trial service [395](#)
 - how to look at [382, 395](#)
- content filtering reports. See also content filtering.
- cookies [390](#)
- copyright [3](#)
- current date/time [157, 490](#)
 - and schedules [449](#)
 - daylight savings [491](#)
 - setting manually [493](#)
 - time server [493](#)
 - when updated [492](#)
- custom signatures [358, 366](#)
 - applying [370](#)
 - verifying [370](#)
- custom.rules [362](#)
- customer support [8](#)

D

- Data Encryption Standard. See DES.
- daylight savings [491](#)
- DDNS [285](#)
 - backup [286](#)
 - configuration overview [111](#)
 - high availability (HA) [285](#)
 - IP address update policies [286](#)
 - mail exchanger [286](#)
 - prerequisites [111](#)
 - service providers [285](#)
 - type of service [286](#)
 - wildcard [285](#)
- DES [240](#)
- device HA
 - configuration overview [111](#)
 - prerequisites [111](#)
- DHCP [180, 489](#)
 - and DNS servers [181](#)
 - and domain name [489](#)
 - and interfaces [180](#)
 - client list [161](#)
 - pool [181](#)
 - static DHCP [181](#)
- DIAL BACKUP port [178](#)
- DIAL BACKUP port. See also auxiliary interface.
- Differentiated Services Code Point (DSCP) [359](#)
- Diffie-Hellman key group [240](#)
 - Perfect Forward Secrecy (PFS) [225](#)
- directory traversals [354](#)
- disclaimer [3](#)
- distributed port scans [348](#)
- DNS [494, 495](#)
 - address records [497](#)
 - domain name forwarders [498](#)
 - domain name to IP address [497](#)
 - IP address to domain name [498](#)
 - Mail eXchange (MX) records [499](#)
 - pointer (PTR) records [498](#)
- DNS servers [494, 498](#)
 - and interfaces [181](#)
- Domain Name System. See DNS.
- double-encoding [354](#)
- Dynamic Domain Name System. See DDNS.
- Dynamic Host Configuration Protocol. See DHCP.
- DynDNS [285](#)
 - see also DDNS.

E

- e-Donkey [339](#)
- EGP (Exterior Gateway Protocol) [348](#)
- e-Mule [339](#)
- Encapsulating Security Payload. See ESP.
- encapsulation
 - and active protocol [225](#)
 - transport mode [225](#)
 - tunnel mode [225](#)
 - VPN [225](#)
- encryption algorithms [239](#), [240](#)
 - 3DES [240](#)
 - AES [240](#)
 - and active protocol [239](#)
 - DES [240](#)
- End of IP List [360](#)
- ESP [224](#)
 - and transport mode [225](#)
- Ethereal [367](#)
- Ethernet interfaces [177](#), [183](#)
 - and OSPF [183](#)
 - and RIP [183](#)
 - and routing protocols [183](#)
 - basic characteristics [178](#)
 - virtual [213](#)
 - with no physical ports [191](#)
- experimental-options [355](#)
- extended authentication
 - and VPN gateways [229](#)
 - IKE SA [243](#)
- external modems [211](#)

F

- false negatives [338](#)
- false positives [338](#), [353](#)
- FCC statement [4](#)
- file extensions
 - configuration files [167](#)
 - shell scripts [167](#)
- file manager
 - configuration overview [117](#)
- filtered port scan [349](#)
- firewall [53](#), [301](#)
 - actions [316](#)
 - and address groups [316](#)
 - and address objects [316](#)
 - and alerts [306](#)
 - and application patrol [321](#)
 - and H.323 (VoIP pass through) [414](#)
 - and HTTP redirect [409](#)

- and IPSec SA [304](#)
- and logs [316](#)
- and port triggering [292](#)
- and schedules [316](#)
- and service groups [316](#)
- and services [316](#), [444](#)
- and SIP [418](#)
- and SIP (VoIP pass through) [415](#)
- and user groups [316](#)
- and users [316](#)
- and virtual servers [303](#)
- and VoIP pass through [413](#), [416](#), [417](#)
- and VPN [229](#)
- and zones [301](#), [309](#)
- asymmetrical routes [308](#), [311](#), [313](#)
- configuration overview [112](#)
- criteria [302](#)
- global rules [303](#)
- prerequisites [112](#)
- priority [309](#), [311](#), [314](#)
- sessions, number of [309](#), [311](#), [314](#)
- to-ZyWALL. See also to-ZyWALL firewall.
- triangle routes [308](#), [311](#), [313](#)
- vs application patrol [302](#)

- firmware
 - and restart [172](#)
 - boot module. See boot module.
 - current version [157](#), [173](#)
 - getting updated [172](#)
 - uploading [172](#), [173](#)
 - uploading with FTP [519](#)
- flags [359](#)
- flood detection [349](#)
- force user authentication policies [433](#)
 - and address groups [434](#)
 - and address objects [434](#)
 - and schedules [434](#)
 - prerequisites [116](#)
- fragmentation flag [364](#)
- fragmentation offset [364](#)
- FTP [519](#)
 - and address groups [519](#)
 - and address objects [519](#)
 - and certificates [519](#)
 - and zones [519](#)
 - with Transport Layer Security (TLS) [519](#)
- Fully-Qualified Domain Name (FQDN) [497](#)

G

- gateway policy. See VPN gateways.
- Generic Routing Encapsulation. See GRE.
- GRE [207](#)

H

H.323 [414](#)
 and firewall [414](#)
 and RTP [414](#)

H.323. See also ALG.

header checksum [359](#)

host-based intrusions [333](#)

HTTP
 redirect to HTTPS [506](#)
 vs HTTPS [504](#)

HTTP Inspection [353](#)

HTTP over SSL. See HTTPS.

HTTP redirect [409](#)
 and application patrol [409](#)
 and firewall [409](#)
 and interfaces [412](#)
 and policy routes [409](#)
 configuration overview [115](#)
 packet flow [409](#)
 prerequisites [115](#)

HTTPS [504](#)
 and certificates [504](#)
 authenticating clients [504](#)
 avoiding warning messages [511](#)
 vs HTTP [504](#)
 with Internet Explorer [509](#)
 with Netscape Navigator [510](#)

HTTPS Example [509](#)

hub-and-spoke VPN. See VPN concentrator.

HyperText Transfer Protocol over Secure Socket Layer.
 See HTTPS.

I

ICMP [443](#)

ICMP code [365](#)

ICMP Decoder [353](#)

ICMP echo [350](#)

ICMP flood [349](#)

ICMP PortswEEP [349](#)

ICMP sequence number [366](#)

ICMP type [365](#)

ICMP unreachable [349](#)

identification (IP) [364](#)

IDP
 alerts [343](#)
 and services [444](#)
 and zones [335](#)
 configuration overview [113](#)
 license status [158](#)
 prerequisites [113](#)
 registration status [166](#)
 trial service activation [165](#)
 upgrading license [166](#)

IDP (Intrusion, Detection and Prevention) [333](#)

IDP policy types [339](#)

IDP profiles [335](#)

IDP registration status [335](#)

IDP service group [340](#)

IDP signatures
 and synchronization (device HA) [281](#)

IEEE 802.1q. See VLAN.

IGP (Interior Gateway Protocol) [348](#)

IHL (IP Header Length) [359](#)

IIS server [354](#)

IIS unicode [354](#)

IKE SA
 aggressive mode [239](#), [242](#), [243](#)
 and authentication methods [465](#)
 and certificates [244](#)
 and RADIUS [244](#)
 and to-ZyWALL firewall [229](#)
 authentication algorithms [239](#), [240](#)
 configuration overview [110](#)
 content [241](#)
 dead peer detection (DPD) [247](#)
 Diffie-Hellman key group [240](#)
 encryption algorithms [239](#), [240](#)
 extended authentication [243](#)
 ID type [241](#)
 IP address, remote IPsec router [239](#)
 IP address, ZyXEL device [239](#)
 local identity [241](#)
 main mode [239](#), [242](#)
 NAT traversal [243](#)
 negotiation mode [239](#)
 password [244](#)
 peer identity [241](#)
 prerequisites [110](#)
 pre-shared key [241](#)
 proposal [239](#)
 user name [244](#)

IKE SA. See also VPN.

inline profile [338](#)

instant messenger (IM)
 managing [321](#)

interface
 status [158](#)

interfaces
 and DNS servers [181](#)
 and HTTP redirect [412](#)
 and layer-3 virtualization [177](#)
 and physical ports [107](#), [177](#)
 and policy routes [295](#), [296](#)
 and static routes [300](#)
 and virtual servers [406](#)

- and VPN gateways [229](#)
 - and VRRP groups [277](#)
 - and zones [107](#), [177](#)
 - as DHCP relays [181](#)
 - as DHCP servers [181](#), [489](#)
 - auxiliary. See also auxiliary interface.
 - backup. See trunks.
 - bandwidth management [180](#), [220](#)
 - bridge. See also bridge interfaces.
 - configuration overview [109](#)
 - DHCP clients [179](#)
 - Ethernet. See also Ethernet interfaces.
 - gateway [180](#)
 - general characteristics [177](#)
 - IP address [178](#)
 - metric [180](#)
 - MTU [180](#)
 - overlapping IP address and subnet mask [179](#)
 - ping check [182](#)
 - port groups. See also port groups.
 - PPPoE/PPTP. See also PPPoE/PPTP interfaces.
 - prerequisites [109](#), [182](#)
 - relationships between [182](#)
 - static DHCP [181](#)
 - subnet mask [178](#)
 - trunks. See also trunks.
 - types [177](#)
 - virtual. See also virtual interfaces.
 - VLAN. See also VLAN interfaces.
 - where used [109](#)
- Internet Control Message Protocol. See ICMP.
- Internet Protocol Security. See IPSec.
- Internet Protocol. See IP.
- intrusions
- host [333](#)
 - network [333](#)
- IP [358](#)
- IP alias. See virtual interfaces.
- IP Decoy Portscan [348](#)
- IP Distributed Portscan [348](#)
- IP options [360](#), [365](#)
- IP policy routing. See policy routes.
- IP Portscan [348](#)
- IP Portsweep [349](#)
- IP protocols [443](#)
- ICMP. See ICMP.
 - TCP. See TCP.
 - UDP. See UDP.
- IP Security Option [360](#)
- IP static routes. See static routes.
- IP Stream Identifier [360](#)
- IP v4 packet headers [359](#)
- IPSec [223](#)
- IPSec SA
- active protocol [224](#)
 - and firewall [229](#), [304](#)
 - and to-ZyWALL firewall [229](#)
 - authentication algorithms [239](#), [240](#)
 - authentication key (manual keys) [226](#)
 - configuration overview [110](#)
 - destination NAT for inbound traffic [228](#)
 - encapsulation [225](#)
 - encryption algorithms [239](#), [240](#)
 - encryption key (manual keys) [226](#)
 - local policy [224](#)
 - manual keys [226](#)
 - NAT for inbound traffic [226](#)
 - NAT for outbound traffic [226](#)
 - overlapping policies [237](#)
 - Perfect Forward Secrecy (PFS) [225](#)
 - policy enforcement [233](#)
 - prerequisites [110](#)
 - proposal [225](#)
 - remote policy [224](#)
 - Security Parameter Index (SPI) (manual keys) [226](#)
 - source NAT for inbound traffic [228](#)
 - source NAT for outbound traffic [227](#)
 - status [254](#)
 - transport mode [225](#)
 - tunnel mode [225](#)
 - when IKE SA is disconnected [224](#)
 - where used [110](#)
- IPSec SA. See also VPN.
- IPSec. See also VPN.
- ISP accounts [271](#)
- and PPPoE/PPTP interfaces [207](#), [271](#)
 - authentication type [273](#)
 - encryption method [273](#)
 - stac compression [273](#)

J

Java [390](#)

L

LAND attack [351](#)

lastgood.conf [169](#)

LDAP [455](#)

- and users [424](#)
- base DN [457](#)
- bind DN [457](#)
- CN identifier [458](#)
- directory structure [456](#)
- Distinguished Name (DN) [457](#)
- in user authentication [456](#)
- Relative Distinguished Name (RDN) [457](#)

user attributes [424](#)
 least load first (for load balancing) [216](#)
 License Active [378](#), [383](#)
 License Inactive [378](#), [383](#)
 Lightweight Directory Access Protocol. See LDAP.
 load balancing [215](#)
 algorithms [216](#), [220](#)
 least load first [216](#)
 session-oriented [216](#)
 spillover [218](#)
 weighted round robin [217](#)
 load balancing. See also trunks.
 local user database [455](#)
 log messages [527](#)
 categories [531](#), [534](#), [535](#), [536](#)
 debugging [525](#)
 regular [525](#)
 types of [525](#)
 log options (IDP) [343](#)
 logs
 and firewall [316](#)
 configuration overview [118](#)
 e-mail profiles [528](#)
 e-mailing log messages [526](#), [531](#)
 formats [529](#)
 log consolidation [532](#)
 specifications [525](#)
 syslog servers [528](#)
 system [528](#)
 types of [528](#)
 Loose Source Routing [360](#)

M

MAC addresses
 and VLAN [193](#)
 ZyWALL [157](#)
 Management Information Base (MIB) [521](#), [522](#)
 MD5 [240](#)
 Message Digest 5. See MD5.
 metrics. See reports.
 model name [157](#)
 monitor profile [338](#)
 MS-05-39 [367](#)
 multiple slash encoding [354](#)
 My Certificates. See also certificates. [472](#)
 MyDoom [333](#)
 myZyXEL.com [163](#), [372](#)
 accounts, creating [163](#)
 and IDP [335](#)

N

NAT [292](#), [404](#)
 address mapping. See policy routes.
 ALG. See ALG.
 and address objects [296](#)
 and ALG [413](#)
 and policy routes [291](#), [296](#)
 and VPN [243](#)
 and VPN. See also VPN.
 port forwarding. See virtual servers.
 port translation. See virtual servers.
 port triggering. See also policy routes.
 port triggering. See also port triggering.
 trigger port. See also policy routes.
 NAT traversal [243](#)
 NetMeeting. See H.323.
 Network Address Translation. See NAT.
 network policy. See VPN connections.
 Network Time Protocol (NTP) [492](#)
 network-based intrusions [333](#)
 Nimda [333](#)
 Nmap [348](#)
 No IP Options [360](#)
 non-RFC characters [354](#)
 non-rfc-http-delimiter [354](#)
 Notice 1 [4](#)

O

objects [116](#)
 obsolete-options [355](#)
 offset (patterns) [366](#)
 Online Certificate Status Protocol (OCSP) [482](#)
 vs CRL [482](#)
 Open Shortest Path First. See OSPF.
 original setting (IDP) [343](#)
 OSI (Open System Interconnection) [336](#)
 OSPF [258](#)
 and Ethernet interfaces [183](#)
 and RIP [260](#)
 and static routes [260](#)
 and to-ZyWALL firewall [258](#)
 area 0 [259](#)
 areas. See OSPF areas.
 authentication method [183](#)
 autonomous system (AS) [258](#)
 backbone [259](#)
 Configuration steps [261](#)
 direction [183](#)
 link cost [183](#)

- priority [183](#)
 - redistribute [260](#)
 - redistribute type (cost) [262](#)
 - routers. See OSPF routers.
 - virtual links [260](#)
 - vs RIP [255](#)
 - OSPF areas [258](#)
 - and Ethernet interfaces [183](#)
 - backbone [258](#)
 - Not So Stubby Area (NSSA) [258](#)
 - stub areas [258](#)
 - types of [258](#)
 - OSPF routers [259](#)
 - area border (ABR) [259](#)
 - autonomous system boundary (ASBR) [260](#)
 - backbone (BR) [260](#)
 - backup designated (BDR) [260](#)
 - designated (DR) [260](#)
 - internal (IR) [259](#)
 - link state advertisements
 - priority [260](#)
 - types of [259](#)
 - oversize-chunk-encoding [355](#)
 - oversize-offset [355](#)
 - oversize-request-uri-directory [355](#)
- ## P
- packet inspection signatures [336](#)
 - packet statistics [161](#)
 - padding [360](#)
 - payload option [366](#)
 - payload size [366](#)
 - peer-to-peer (P2P)
 - managing [321](#)
 - Perfect Forward Secrecy (PFS)
 - Diffie-Hellman key group [225](#)
 - physical port
 - packet statistics [161](#)
 - physical ports [107](#)
 - and interfaces [107](#)
 - ping check. See interfaces.
 - Point-to-Point Protocol over Ethernet. See PPPoE.
 - Point-to-Point Tunneling Protocol. See PPTP
 - policy routes [291](#)
 - actions [291](#)
 - and address objects [295, 296](#)
 - and HTTP redirect [409](#)
 - and interfaces [295, 296](#)
 - and NAT [291](#)
 - and schedules [296](#)
 - and service groups [296](#)
 - and services [296, 444](#)
 - and trunks [215, 296](#)
 - and user groups [295](#)
 - and users [295](#)
 - and VoIP pass through [413, 416, 417](#)
 - and VPN connections [229, 295, 296](#)
 - bandwidth management [297](#)
 - benefits [291](#)
 - configuration overview [111](#)
 - criteria [291](#)
 - prerequisites [111](#)
 - port forwarding. See virtual servers.
 - port groups [177, 190, 191](#)
 - and Ethernet interfaces [190](#)
 - and physical ports [190](#)
 - representative interfaces [191](#)
 - port sweep [349](#)
 - port translation. See virtual servers.
 - port triggering [292](#)
 - and firewall [292](#)
 - and policy routes [296](#)
 - and service groups [296](#)
 - and services [296](#)
 - power off [50](#)
 - power on [50](#)
 - PPPoE [207](#)
 - and RADIUS [207](#)
 - TCP port 1723 [207](#)
 - PPPoE/PPTP interfaces [177, 207](#)
 - and ISP accounts [207, 271](#)
 - basic characteristics [178](#)
 - gateway [208](#)
 - subnet mask [179, 208](#)
 - PPTP [207](#)
 - and GRE [207](#)
 - as VPN [207](#)
 - protocol anomaly [336, 354](#)
 - protocol anomaly detection [353](#)
 - proxy servers [409](#)
 - web. See web proxy servers.
 - Public-Key Infrastructure (PKI) [470](#)
 - public-private key pairs [469](#)
- ## Q
- query view (IDP) [343, 344](#)
 - Quick Start Guide [59](#)
- ## R
- RADIUS [455, 461](#)

- advantages [461](#)
 - and IKE SA [244](#)
 - and PPPoE [207](#)
 - and users [424](#)
 - user attributes [425](#)
 - Real-time Transport Protocol. See RTP.
 - reboot [50](#), [543](#)
 - vs reset [50](#), [543](#)
 - Record Route [360](#)
 - registration
 - and content filtering [378](#), [382](#)
 - configuration overview [118](#)
 - prerequisites [118](#)
 - subscription services. See subscription services.
 - reject-both (IDP) [344](#)
 - reject-receiver (IDP) [344](#)
 - reject-sender (IDP) [344](#)
 - Related Documentation [43](#)
 - Remote Authentication Dial-In User Service. See RADIUS.
 - remote management [503](#)
 - and to-ZyWALL firewall [503](#)
 - and users [504](#)
 - configuration overview [117](#)
 - FTP. See FTP.
 - limitations [503](#)
 - prerequisites [117](#)
 - SSH. See SSH.
 - Telnet. See Telnet.
 - timeouts [504](#)
 - to-ZyWALL firewall [303](#)
 - WWW. See WWW.
 - reports
 - collecting data [537](#)
 - configuration overview [118](#)
 - specifications [540](#)
 - types of [537](#)
 - reset [50](#)
 - vs reboot [50](#), [543](#)
 - RESET button [50](#)
 - RFC 1058. See RIP.
 - RFC 1389. See RIP.
 - RFC 1587. See OSPF areas.
 - RFC 1631. See NAT.
 - RFC 1889. See RTP.
 - RFC 2131. See DHCP.
 - RFC 2132. See DHCP.
 - RFC 2328. See OSPF.
 - RFC 2338. See VRRP.
 - RFC 2402. See AH.
 - RFC 2406. See ESP.
 - RFC 2510. See Certificate Management Protocol.
 - RFC 2516. See PPPoE.
 - RFC 2637. See PPTP.
 - RFC 2890. See GRE.
 - RFC 3261. See SIP.
 - RIP [255](#)
 - and Ethernet interfaces [183](#)
 - and OSPF [256](#)
 - and static routes [256](#)
 - and to-ZyWALL firewall [256](#)
 - authentication [255](#)
 - direction [183](#)
 - redistribute [256](#)
 - RIP-2 broadcasting methods [183](#)
 - versions [183](#)
 - vs OSPF [255](#)
 - round robin (for load balancing) [217](#)
 - Routing Information Protocol. See RIP
 - routing protocols [255](#)
 - and authentication algorithms [256](#)
 - and Ethernet interfaces [183](#)
 - RTP [414](#)
- ## S
- safety warnings [6](#)
 - same IP [365](#)
 - schedules [449](#)
 - and content filtering [375](#), [376](#), [380](#)
 - and current date/time [449](#)
 - and firewall [316](#)
 - and force user authentication policies [434](#)
 - and policy routes [296](#)
 - one-time [449](#)
 - recurring [449](#)
 - types of [449](#)
 - where used [117](#)
 - Secure Hash Algorithm. See SHA1.
 - Secure Shell. See SSH.
 - Secure Socket Layer. See SSL.
 - security associations. See VPN.
 - self-referential directories [355](#)
 - sensitivity level [353](#)
 - serial number [157](#)
 - service groups [444](#)
 - and firewall [316](#)
 - and policy routes [296](#)
 - and port triggering [296](#)
 - where used [116](#)
 - services [444](#)
 - and firewall [316](#), [444](#)
 - and IDP [444](#)
 - and policy routes [296](#), [444](#)
 - and port triggering [296](#)
 - where used [116](#)

- Session Initiation Protocol. See SIP.
- sessions [540](#)
- severity (IDP) [337](#), [343](#)
- SHA1 [240](#)
- shell scripts [167](#)
 - and users [425](#)
 - downloading [175](#)
 - editing [174](#)
 - managing [174](#)
 - not stopping or starting the ZyWALL [50](#)
 - syntax [167](#)
 - uploading [176](#)
 - way the ZyWALL runs [168](#)
- shutdown [50](#)
- Signature Categories
 - Access Control [340](#)
 - Buffer Overflow [340](#)
 - DoS/DDoS [339](#)
 - IM [339](#)
 - P2P [339](#)
 - Scan [339](#)
 - Spam [339](#)
 - Virus/Worm [340](#)
 - Web Attack [340](#)
- signature ID [343](#), [361](#), [364](#)
- Simple Certificate Enrollment Protocol (SCEP) [476](#)
- Simple Network Management Protocol. See SNMP.
- Simple Traversal of UDP through NAT. See STUN.
- SIP [415](#)
 - and firewall [415](#), [418](#)
 - and RTP [414](#)
 - media inactivity timeout [418](#)
 - signaling inactivity timeout [418](#)
- smurf attack [350](#)
- SNAT [292](#)
- SNMP [520](#), [521](#)
 - agents [521](#)
 - and address groups [523](#)
 - and address objects [523](#)
 - and zones [523](#)
 - Get [521](#)
 - GetNext [521](#)
 - Manager [521](#)
 - managers [521](#)
 - MIB [521](#), [522](#)
 - network components [521](#)
 - Set [521](#)
 - Trap [521](#)
 - traps [522](#)
 - versions [520](#)
- Snort equivalent terms [371](#)
- Snort rule header [371](#)
- Snort rule options [371](#)
- Snort signatures [371](#)
- Source Network Address Translation. See SNAT.
- spillover (for load balancing) [218](#)
- SQL slammer [333](#)
- SSH [513](#)
 - and address groups [515](#)
 - and address objects [515](#)
 - and certificates [515](#)
 - and zones [515](#)
 - client requirements [514](#)
 - encryption methods [514](#)
 - for secure Telnet [515](#)
 - how connection is established [513](#)
 - versions [514](#)
 - with Linux [516](#)
 - with Microsoft Windows [516](#)
- SSL [504](#)
- stac compression [273](#)
- starting the ZyWALL [50](#)
- startup-config.conf [169](#)
 - and synchronization (device HA) [281](#)
 - if errors [170](#)
 - missing at restart [169](#)
 - present at restart [170](#)
- startup-config-bad.conf [169](#)
- static routes [298](#)
 - and interfaces [300](#)
 - and OSPF [260](#)
 - and RIP [256](#)
 - configuration overview [112](#)
 - metric [300](#)
 - prerequisites [112](#)
- stopping the ZyWALL [50](#)
- streaming protocols
 - managing [321](#)
- Strict Source Routing [360](#)
- STUN
 - and VoIP pass through [413](#)
- subscription services [163](#)
 - and synchronization (device HA) [282](#)
 - content filtering [163](#)
 - content filtering. See also content filtering.
 - IDP [163](#)
 - IDP. See also IDP.
 - new IDP signatures [163](#)
 - status [166](#)
 - trial service activation [165](#)
 - upgrading [166](#)
- Supporting Disk [44](#)
- SYN Flood [351](#)
- synchronization [281](#)
 - and subscription services [282](#)
 - information synchronized [281](#)
 - password [283](#)
 - port number [283](#)
 - restrictions [282](#)
- Syntax Conventions [44](#)

syslog servers. See logs.
 system log. See logs.
 system name [156](#)
 system reports. See reports.
 system uptime [157](#)
 system-default.conf [169](#)

T

T/TCP [355](#)
 TCP [443](#)
 ACK (acknowledgment) [350](#)
 ACK number [365](#)
 connections [443](#)
 port numbers [443](#)
 SYN (synchronize) [350](#)
 window size [365](#)
 TCP Decoder [353](#)
 TCP Decoy Portscan [348](#)
 TCP Distributed Portscan [348](#)
 TCP flag bits [365](#)
 TCP Portscan [348](#)
 TCP Portsweep [349](#)
 TCP RST [349](#)
 TCP SYN flood [350](#)
 TCPdump [367](#)
 Telnet [517](#)
 and address groups [518](#)
 and address objects [518](#)
 and zones [518](#)
 with SSH [515](#)
 terminology differences
 bandwidth management [106](#)
 NAT [106](#)
 with other products [106](#)
 with ZyNOS [106](#)
 three-way handshake [350](#)
 through-ZyWALL firewall. See firewall.
 time servers (default) [492](#)
 time to live [359](#)
 Timestamp [360](#)
 to-ZyWALL firewall [303](#)
 and NAT traversal (VPN) [229](#)
 and OSPF [258](#)
 and remote management [303](#), [503](#)
 and RIP [256](#)
 and virtual servers [403](#)
 and VPN [229](#)
 and VRRP [276](#)
 and VRRP groups [277](#)
 global rules [303](#)

to-ZyWALL firewall. See also firewall.
 trademarks [3](#)
 traffic anomaly [336](#), [348](#)
 Transmission Control Protocol. See TCP.
 Transport Layer Security (TLS) [519](#)
 trial subscription services [165](#)
 triangle routes [307](#)
 vs virtual interfaces [307](#)
 triangle routes (firewall) [308](#), [311](#), [313](#)
 Triple Data Encryption Standard. See 3DES.
 truncated-address-header [356](#)
 truncated-header [356](#)
 truncated-options [355](#)
 truncated-timestamp-header [356](#)
 trunks [178](#), [215](#)
 and policy routes [215](#), [296](#)
 and VoIP pass through [413](#)
 configuration overview [110](#)
 member interface mode [220](#)
 member interfaces [220](#)
 prerequisites [110](#)
 where used [110](#)
 trunks. See also load balancing.
 Trusted Certificates. See also certificates. [481](#)

U

u encoding [355](#)
 UDP [443](#)
 messages [443](#)
 port numbers [443](#)
 UDP Decoder [353](#)
 UDP Decoy Portscan [348](#)
 UDP Distributed Portscan [348](#)
 UDP flood attack [351](#)
 UDP Portscan [348](#)
 UDP Portsweep [349](#)
 undersize-len [355](#)
 undersize-offset [355](#)
 updating IDP signatures [372](#)
 URI (Uniform Resource Identifier) [366](#)
 usage
 CPU [157](#)
 memory [157](#)
 onboard flash [157](#)
 sessions [157](#)
 user authentication [423](#), [455](#)
 external [423](#)
 local user database [455](#)
 User Datagram Protocol. See UDP.

- user groups [425](#)
 - and content filtering [375, 380](#)
 - and firewall [316](#)
 - and policy routes [295](#)
 - configuration overview [116](#)
- user names
 - rules [428](#)
- user sessions. See sessions.
- users [423](#)
 - access. See also access users.
 - Admin (type) [423](#)
 - admin. See also admin users.
 - and AAA servers [424](#)
 - and authentication methods [424](#)
 - and content filtering [375, 380](#)
 - and firewall [316](#)
 - and LDAP [424](#)
 - and policy routes [295](#)
 - and RADIUS [424](#)
 - and remote management [504](#)
 - and shell scripts [425](#)
 - attributes for Ext-User [424](#)
 - attributes for LDAP [424](#)
 - attributes for RADIUS [425](#)
 - attributes in AAA servers [424](#)
 - configuration overview [116](#)
 - currently logged in [157](#)
 - default lease time [432](#)
 - default reauthentication time [432](#)
 - default type for Ext-User [424](#)
 - Ext-User (type) [423](#)
 - groups. See user groups.
 - Guest (type) [423](#)
 - lease time [427](#)
 - Limited-Admin (type) [423](#)
 - lockout [432](#)
 - prerequisites (for force user authentication policies) [116](#)
 - reauthentication time [427](#)
 - types of [423](#)
 - User (type) [423](#)
 - user names [428](#)
- UTF-8 decode [355](#)

V

- virtual interfaces [177, 213](#)
 - basic characteristics [178](#)
 - not DHCP clients [179](#)
 - types of [213](#)
 - vs asymmetrical routes [307](#)
 - vs triangle routes [307](#)
- Virtual Local Area Network. See VLAN.
- Virtual Private Network. See VPN.

- Virtual Router Redundancy Protocol. See VRRP.
- virtual servers [403](#)
 - and address objects (HOST) [406](#)
 - and firewall [303](#)
 - and interfaces [406](#)
 - and to-ZyWALL firewall [403](#)
 - and VoIP pass through [416, 417](#)
 - configuration overview [114](#)
 - criteria [403](#)
 - limitations [292](#)
 - prerequisites [114](#)
 - where to forward [403](#)
- virus [340](#)
- VLAN [193](#)
 - advantages [194](#)
 - and MAC addresses [193](#)
 - ID [193](#)
- VLAN interfaces [177, 194](#)
 - and Ethernet interfaces [194](#)
 - basic characteristics [178](#)
 - virtual [213](#)
- VoIP pass through [413](#)
 - and firewall [413, 416, 417](#)
 - and policy routes [413, 416, 417](#)
 - and trunks [413](#)
 - and virtual servers [416, 417](#)
 - configuration overview [115](#)
 - peer-to-peer calls [416](#)
- VoIP pass through. See also ALG.
- VPN [223](#)
 - active protocol [224](#)
 - and NAT [243](#)
 - basic troubleshooting [229](#)
 - established in two phases [223](#)
 - hub-and-spoke. See VPN concentrator.
 - IKE SA. See IKE SA.
 - IPSec [223](#)
 - IPSec SA. See IPSec SA.
 - local network [223](#)
 - proposal [239](#)
 - remote IPSec router [223](#)
 - remote network [223](#)
 - security associations (SA) [223](#)
- VPN concentrator [250](#)
 - advantages [251](#)
 - and IPSec SA policy enforcement [253](#)
 - disadvantages [251](#)
- VPN connections
 - and address objects [228](#)
 - and policy routes [229, 295, 296](#)
- VPN gateways
 - and certificates [229](#)
 - and extended authentication [229](#)
 - and interfaces [229](#)
 - and to-ZyWALL firewall [229](#)
- VPN. See also IKE SA, IPSec SA.

VRRP 275

- advertisement interval [275](#)
- and to-ZyWALL firewall [276](#)
- backup router [275](#)
- management IP [275](#)
- master router [275](#)
- preempt [276](#)
- router priority [276](#)
- virtual router ID (VR ID) [275](#)

VRRP groups 277

- advertisement interval [277](#)
- and interfaces [277](#)
- and to-ZyWALL firewall [277](#)
- authentication [277](#)
- HA status [279](#)
- role (desired) [280](#)
- status [278](#)

VRRP groups. See also VRRP.

vs RIP [258](#)

W

warm start [50](#)

warranty [7](#)

Web attack [340](#)

Web Configurator [59](#)

web configurator [49, 59](#)

- access users [434](#)
- admin users [59](#)

web features

- ActiveX [390](#)
- cookies [390](#)
- Java [390](#)
- web proxy servers [390](#)

web proxy servers [390, 409](#)

- see also HTTP redirect.

webroot-directory-traversal [355](#)

weighted round robin (for load balancing) [217](#)

Wizard Setup [67](#)

worm [340](#)

WWW [505](#)

- and address groups [509](#)
- and address objects [509](#)
- and authentication methods [465, 508](#)
- and certificates [506](#)
- and zones [509](#)

WWW. See also HTTP, HTTPS. [505](#)

Z

zones [108, 267](#)

- and firewall [301, 309](#)
- and FTP [519](#)
- and IDP [335](#)
- and interfaces [107, 267](#)
- and SNMP [523](#)
- and SSH [515](#)
- and Telnet [518](#)
- and VPN [267](#)
- and WWW [509](#)
- block intra-zone traffic [269, 303](#)
- configuration overview [110](#)
- extra-zone traffic [268](#)
- inter-zone traffic [268](#)
- intra-zone traffic [268](#)
- prerequisites [110](#)
- types of traffic with [267](#)
- where used [110](#)

ZyWALL

configuration. See configuration.

domain name [489](#)

system name [489](#)

terminology differences. See terminology differences.