ZyWALL 10/10W/30W/50/100

Internet Security Gateway

User's Guide

Versions 3.52 and 3.61

June 2003

ZyXEL

Unleash Networking Power

Copyright

Copyright © 2003 by ZyXEL Communications Corporation.

Disclaimer

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

This publication is subject to change without notice.

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

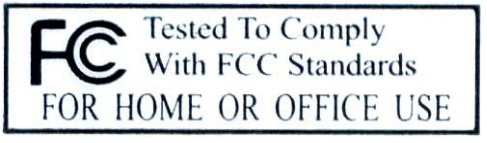
This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
This device may not cause harmful interference.
This device must accept any interference received, including interference that may cause undesired operations.
This equipment has been tested and found to comply with the limits for a CLASS B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.
If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
Reorient or relocate the receiving antenna.
Increase the separation between the equipment and the receiver.
Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

Certifications

Refer to the product page at www.zyxel.com.



Information for Canadian Users

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

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

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

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

Caution

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

Note

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

ZyXEL Limited Warranty

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

NOTE

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

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

Online Registration

Register online registration at www.zyxel.com for free future product updates and information.

Customer Support

When you contact your customer support representative please have the following information ready:
Please have the following information ready when you contact customer support.

- Product model and serial number.
- Information in **Menu 24.2.1 – System Information**.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu 300, Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen, Germany

Table of Contents

Copyright ii
Federal Communications Commission (FCC) Interference Statement iii
Information for Canadian Users iv
ZyXEL Limited Warranty v
Customer Support vi
List of Figures xviii
List of Tables xxv
Preface xxix
Getting Started I
Chapter 1 Getting to Know Your ZyWALL 1-1
1.1 ZyWALL Internet Security Gateway Overview 1-1
1.2 ZyWALL Features 1-2
1.3 Applications for the ZyWALL 1-8
Chapter 2 Introducing the Web Configurator 2-1
2.1 Web Configurator Overview 2-1
2.2 Accessing the ZyWALL Web Configurator 2-1
2.3 Resetting the ZyWALL 2-2
2.4 Navigating the ZyWALL Web Configurator 2-3
Chapter 3 Wizard Setup 3-1
3.1 Wizard Setup Overview 3-1
3.2 Wizard Setup: General Setup and System Name 3-1
3.3 Wizard Setup: Screen 2 3-2
3.4 Wizard Setup: Screen 3 3-8
3.5 Basic Setup Complete 3-12
System, LAN and Wireless LAN II

Chapter 4 System Screens....4-1
4.1 System Overview....4-1
4.2 Configuring General Setup....4-1
4.3 Dynamic DNS....4-2
4.4 Configuring Dynamic DNS....4-2
4.5 Configuring Password....4-4
4.6 Configuring Time Zone....4-5
Chapter 5 LAN Screens....5-1
5.1 LAN Overview....5-1
5.2 DHCP Setup....5-1
5.3 LAN TCP/IP....5-1
5.4 Configuring IP....5-3
5.5 Configuring Static DHCP....5-5
5.6 Configuring IP Alias....5-6
Chapter 6 Wireless LAN Screens....6-1
6.1 Wireless LAN Overview....6-1
6.2 Wireless LAN Basics....6-1
6.3 Wireless Security....6-3
6.4 Configuring Wireless LAN....6-4
6.5 Configuring MAC Filter....6-6
6.6 802.1x Overview....6-8
6.7 RADIUS....6-8
6.8 Local User Database....6-10
6.9 Configuring 802.1X....6-10
6.10 Configuring Local User Database....6-11
6.11 Configuring RADIUS....6-13
DMZ and WAN....III

Chapter 7 DMZ Screens **7-1**
7.1 DMZ Overview 7-1
7.2 Configuring DMZ 7-1
Chapter 8 WAN Screens **8-1**
8.1 WAN Overview 8-1
8.2 TCP/IP Priority (Metric) 8-1
8.3 Configuring Route 8-1
8.4 Configuring WAN ISP 8-2
8.5 Configuring WAN IP 8-10
8.6 Configuring WAN MAC 8-13
8.7 Traffic Redirect 8-14
8.8 Configuring Traffic Redirect 8-15
8.9 Configuring Dial Backup 8-16
8.10 Advanced Modem Setup 8-21
8.11 Configuring Advanced Modem Setup 8-21
NAT and Static Route ..... **IV**
Chapter 9 Network Address Translation (NAT) Screens **9-1**
9.1 NAT Overview 9-1
9.2 Using NAT 9-6
9.3 SUA Server 9-6
9.4 Configuring SUA Server 9-8
9.5 Configuring Address Mapping 9-10
9.6 Configuring Trigger Port 9-13
Chapter 10 Static Route Screens **10-1**
10.1 Static Route Overview 10-1
10.2 Configuring IP Static Route 10-1
Firewall and Content Filters ..... **V**

Chapter 11 Firewalls 11-1
11.1 Firewall Overview 11-1
11.2 Types of Firewalls 11-1
11.3 Introduction to ZyXEL's Firewall 11-2
11.4 Denial of Service 11-3
11.5 Stateful Inspection 11-7
11.6 Guidelines For Enhancing Security With Your Firewall 11-11
11.7 Packet Filtering Vs Firewall 11-12
Chapter 12 Firewall Screens 12-1
12.1 Access Methods 12-1
12.2 Firewall Policies Overview 12-1
12.3 Rule Logic Overview 12-2
12.4 Connection Direction Examples 12-4
12.5 Configuring Firewall 12-5
12.6 Example Firewall Rule 12-12
12.7 Predefined Services 12-17
12.8 Alerts 12-19
12.9 Configuring Attack Alert 12-20
Chapter 13 Content Filtering Screens 13-1
13.1 Content Filtering Overview 13-1
13.2 Configuring Categories 13-1
13.3 Configuring Free 13-5
13.4 Configuring iCard 13-7
13.5 Configuring List Update 13-8
13.6 Configuring Exempt Computers 13-9
13.7 Configuring Customize 13-11
13.8 Configuring Keyword Blocking 13-14

VPN/IPSec VI

Chapter 14 Introduction to IPSec 14-1

14.1 VPN Overview 14-1

14.2 IPSec Architecture 14-3

14.3 Encapsulation 14-5

14.4 IPSec and NAT 14-5

Chapter 15 VPN Screens 15-1

15.1 VPN/IPSec Overview 15-1

15.2 IPSec Algorithms 15-1

15.3 My IP Address 15-2

15.4 Secure Gateway Address 15-2

15.5 Summary Screen 15-3

15.6 Keep Alive 15-6

15.7 NAT Traversal 15-6

15.8 ID Type and Content 15-7

15.9 Pre-Shared Key 15-9

15.10 Editing VPN Policies 15-9

15.11 IKE Phases 15-15

15.12 Configuring Advanced IKE Settings 15-17

15.13 Manual Key Setup 15-21

15.14 Configuring Manual Key 15-21

15.15 Viewing SA Monitor 15-25

15.16 Configuring Global Setting 15-27

15.17 Telecommuter VPN/IPSec Examples 15-28

15.18 VPN and Remote Management 15-30

Remote Management and UPnP VII

Chapter 16 Remote Management Screens 16-1

16.1 Remote Management Overview 16-1
16.2 Telnet 16-2
16.3 Configuring TELNET 16-3
16.4 Configuring FTP 16-4
16.5 Configuring WWW 16-5
16.6 Configuring SNMP 16-7
16.7 Configuring DNS 16-11
16.8 Configuring Security 16-12
Chapter 17 UPnP 17-1
17.1 Universal Plug and Play Overview 17-1
17.2 UPnP and ZyXEL 17-2
17.3 Configuring UPnP 17-2
17.4 Installing UPnP in Windows Example 17-4
17.5 Using UPnP in Windows XP Example 17-6
Bandwidth Management VIII
Chapter 18 Bandwidth Management Screens 18-1
18.1 Bandwidth Management Overview 18-1
18.2 Bandwidth Classes and Filters 18-1
18.3 Proportional Bandwidth Allocation 18-2
18.4 Bandwidth Management Usage Examples 18-2
18.5 Scheduler 18-4
18.6 Maximize Bandwidth Usage 18-5
18.7 Bandwidth Borrowing 18-8
18.8 Configuring Summary 18-10
18.9 Configuring Class Setup 18-12
18.10 Configuring Monitor 18-18
Logs IX

Chapter 19 Logs Screens 19-1
19.1 Configuring View Log 19-1
19.2 Configuring Log Settings 19-3
19.3 Configuring Reports 19-6
Maintenance X
Chapter 20 Maintenance 20-1
20.1 Maintenance Overview 20-1
20.2 Status Screen 20-1
20.3 DHCP Table Screen 20-4
20.4 F/W Upload Screen 20-5
20.5 Configuration Screen 20-7
SMT General Configuration XI
Chapter 21 Introducing the SMT 21-1
21.1 Introduction to the SMT 21-1
21.2 Accessing the Console Port via the Console Port 21-1
21.3 Navigating the SMT Interface 21-2
21.4 Changing the System Password 21-7
21.5 Resetting the ZyWALL 21-8
Chapter 22 SMT Menu 1 - General Setup 22-1
22.1 Introduction to General Setup 22-1
22.2 Configuring General Setup 22-1
Chapter 23 WAN and Dial Backup Setup 23-1
23.1 Introduction to WAN and Dial Backup Setup 23-1
23.2 WAN Setup 23-1
23.3 Dial Backup 23-2
23.4 Configuring Dial Backup in Menu 2 23-2
23.5 Advanced WAN Setup 23-4

23.6 Remote Node Profile (Backup ISP) 23-6
23.7 Editing PPP Options 23-8
23.8 Editing TCP/IP Options 23-10
23.9 Editing Login Script 23-12
23.10 Remote Node Filter 23-14
Chapter 24 LAN Setup 24-1
24.1 Introduction to LAN Setup 24-1
24.2 Accessing the LAN Menus 24-1
24.3 LAN Port Filter Setup 24-1
24.4 TCP/IP and DHCP Ethernet Setup Menu 24-2
24.5 Wireless LAN Setup 24-6
Chapter 25 DMZ Setup 25-1
25.1 Configuring DMZ Setup 25-1
25.2 DMZ Port Filter Setup 25-1
25.3 TCP/IP Setup 25-2
Chapter 26 Internet Access 26-1
26.1 Introduction to Internet Access Setup 26-1
26.2 Ethernet Encapsulation 26-1
26.3 Configuring the PPTP Client 26-3
26.4 Configuring the PPPoE Client 26-4
26.5 Basic Setup Complete 26-5
SMT Advanced Applications XII
Chapter 27 Remote Node Setup 27-1
27.1 Introduction to Remote Node Setup 27-1
27.2 Remote Node Setup 27-1
27.3 Remote Node Profile Setup 27-2
27.4 Edit IP 27-8

27.5 Remote Node Filter 27-10
Chapter 28 IP Static Route Setup 28-1
28.1 IP Static Route Setup 28-1
Chapter 29 Network Address Translation (NAT) 29-1
29.1 Using NAT 29-1
29.2 NAT Setup 29-4
29.3 Configuring a Server behind NAT 29-9
29.4 General NAT Examples 29-11
29.5 Trigger Port Forwarding 29-18
Chapter 30 Introducing the ZyWALL Firewall 30-1
30.1 Using ZyWALL SMT Menus 30-1
Chapter 31 Filter Configuration 31-1
31.1 Introduction to Filters 31-1
31.2 Configuring a Filter Set 31-4
31.3 Example Filter 31-13
31.4 Filter Types and NAT 31-15
31.5 Firewall Versus Filters 31-16
31.6 Applying a Filter 31-16
Chapter 32 SNMP Configuration 32-1
32.1 SNMP Configuration 32-1
32.2 SNMP Traps 32-2
SMT System Maintenance XIII
Chapter 33 System Information & Diagnosis 33-1
33.1 Introduction to System Status 33-1
33.2 System Status 33-1
33.3 System Information and Console Port Speed 33-3
33.4 Log and Trace 33-6

33.5 Diagnostic 33-11
Chapter 34 Firmware and Configuration File Maintenance 34-1
34.1 Introduction 34-1
34.2 Filename Conventions 34-1
34.3 Backup Configuration 34-2
34.4 Restore Configuration 34-8
34.5 Uploading Firmware and Configuration Files 34-11
Chapter 35 System Maintenance Menus 8 to 10 35-1
35.1 Command Interpreter Mode 35-1
35.2 Call Control Support 35-3
35.3 Time and Date Setting 35-6
Chapter 36 Remote Management 36-1
36.1 Remote Management 36-1
SMT Advanced Management XIV
Chapter 37 IP Policy Routing 37-1
37.1 Introduction to IP Policy Routing 37-1
37.2 Benefits 37-1
37.3 Routing Policy 37-1
37.4 IP Routing Policy Setup 37-2
37.5 Applying an IP Policy 37-6
37.6 IP Policy Routing Example 37-7
Chapter 38 Call Scheduling 38-1
38.1 Introduction to Call Scheduling 38-1
Chapter 39 VPN/IPSec Setup 39-1
39.1 Introduction 39-1
39.2 IPSec Summary Screen 39-2
39.3 IPSec Setup 39-6

39.4 IKE Setup 39-11
39.5 Manual Setup 39-14
Chapter 40 SA Monitor 40-1
40.1 Introduction 40-1
40.2 Using SA Monitor 40-1
Appendices and Index XV
Appendix A Troubleshooting ..... A
Appendix B Hardware Specifications ..... E
Appendix C Safety Warnings and Instructions ..... J
Appendix D Removing and Installing a ZyWALL 100 Fuse ..... K
Index ..... M

List of Figures

Figure 1-1 Secure Internet Access via Cable, DSL or Wireless Modem....1-9
Figure 1-2 VPN Application....1-10
Figure 2-1 Change Password Screen....2-1
Figure 2-2 Example Xmodem Upload....2-3
Figure 2-3 The MAIN MENU Screen of the Web Configurator....2-4
Figure 3-1 Wizard 1....3-2
Figure 3-2 Wizard 2: Ethernet Encapsulation....3-3
Figure 3-3 Wizard 2: PPTP Encapsulation....3-5
Figure 3-4 Wizard2: PPPoE Encapsulation....3-7
Figure 3-5 Wizard 3....3-11
Figure 4-1 System General Setup....4-1
Figure 4-2 DDNS....4-3
Figure 4-3 Password....4-4
Figure 4-4 Time Zone....4-5
Figure 5-1 IP....5-3
Figure 5-2 Static DHCP....5-6
Figure 5-3 IP Alias....5-7
Figure 6-1 RTS Threshold....6-2
Figure 6-2 ZyWALL Wireless Security Levels....6-3
Figure 6-3 Wireless....6-4
Figure 6-4 MAC Address Filter....6-7
Figure 6-5 EAP Authentication....6-9
Figure 6-6 802.1X Authentication....6-10
Figure 6-7 Local User Database....6-12
Figure 6-8 RADIUS....6-13
Figure 7-1 DMZ....7-2
Figure 8-1 WAN Setup: Route....8-2
Figure 8-2 Ethernet Encapsulation....8-3
Figure 8-3 PPPoE Encapsulation....8-5
Figure 8-4 PPTP Encapsulation....8-7
Figure 8-5 RR Service Type....8-9
Figure 8-6 IP Setup....8-10
Figure 8-7 MAC Setup....8-13
Figure 8-8 Traffic Redirect WAN Setup....8-14
Figure 8-9 Traffic Redirect LAN Setup....8-14
Figure 8-10 Traffic Redirect....8-15
Figure 8-11 Dial Backup Setup....8-17
Figure 8-12 Advanced Setup....8-22

Figure 9-1 How NAT Works 9-3
Figure 9-2 NAT Application With IP Alias 9-4
Figure 9-3 Multiple Servers Behind NAT Example 9-8
Figure 9-4 SUA/NAT Setup 9-9
Figure 9-5 Address Mapping 9-11
Figure 9-6Address Mapping Edit 9-12
Figure 9-7 Trigger Port 9-15
Figure 10-1 Example of Static Routing Topology 10-1
Figure 10-2 Edit IP Static Route 10-2
Figure 11-1 ZyWALL Firewall Application 11-3
Figure 11-2 Three-Way Handshake 11-5
Figure 11-3 SYN Flood 11-5
Figure 11-4 Smurf Attack 11-6
Figure 11-5 Stateful Inspection 11-8
Figure 12-1 LAN to WAN Traffic 12-4
Figure 12-2 WAN to LAN Traffic 12-5
Figure 12-3 Enabling the Firewall (ZyWALL 100) 12-6
Figure 12-4 Creating/Editing A Firewall Rule (ZyWALL100) 12-9
Figure 12-5 Adding/Editing Source and Destination Addresses 12-11
Figure 12-6 Creating/Editing A Custom Port 12-12
Figure 12-7 Firewall IP Config Screen 12-13
Figure 12-8 Firewall Rule Edit IP Example 12-14
Figure 12-9 Edit Custom Port Example 12-14
Figure 12-10 MyService Rule Configuration (ZyWALL100) 12-15
Figure 12-11 My Service Example Rule Summary (ZyWALL100) 12-16
Figure 12-12 Attack Alert 12-22
Figure 13-1Content Filter: Categories 13-2
Figure 13-2 Content Filter: Free 13-6
Figure 13-3 Content Filter: iCard 13-7
Figure 13-4 Content Filter: List Update 13-8
Figure 13-5 Content Filter: Exempt Zone 13-10
Figure 13-6 Content Filter: Customize 13-12
Figure 13-7 Content Filter: Keyword Blocking 13-14
Figure 14-1 Encryption and Decryption 14-2
Figure 14-2 VPN Application 14-3
Figure 14-3 IPSec Architecture 14-4
Figure 14-4 Transport and Tunnel Mode IPSec Encapsulation 14-5
Figure 15-1 IPSec Summary Fields 15-3
Figure 15-2 Summary 15-4
Figure 15-3 NAT Router Between IPSec Routers 15-6
Figure 15-4 VPN IKE 15-10

Figure 15-5 Two Phases to Set Up the IPSec SA....15-16
Figure 15-6 VPN IKE: Advanced....15-18
Figure 15-7 Manual Setup....15-22
Figure 15-8 SA Monitor....15-26
Figure 15-9 Global Setting....15-27
Figure 15-10 Telecommuters Sharing One VPN Rule Example....15-29
Figure 15-11 Telecommuters Using Unique VPN Rules Example....15-30
Figure 16-1 Telnet Configuration on a TCP/IP Network....16-3
Figure 16-2 Telnet....16-3
Figure 16-3 FTP....16-5
Figure 16-4 WWW....16-6
Figure 16-5 SNMP Management Model....16-7
Figure 16-6 SNMP....16-10
Figure 16-7 DNS....16-12
Figure 16-8 Security....16-13
Figure 17-1 Configuring UPnP....17-3
Figure 18-1 Application-based Bandwidth Management Example....18-3
Figure 18-2 Subnet-based Bandwidth Management Example....18-3
Figure 18-3 Application and Subnet-based Bandwidth Management Example....18-4
Figure 18-4 Bandwidth Allotment Example....18-6
Figure 18-5 Maximize Bandwidth Usage Example....18-7
Figure 18-6 Bandwidth Borrowing Example....18-9
Figure 18-7 Bandwidth Manager: Summary....18-11
Figure 18-8 Bandwidth Manager: Class Setup....18-13
Figure 18-9 Bandwidth Manager: Class Configuration....18-14
Figure 18-10 Bandwidth Management Statistics....18-17
Figure 18-11 Bandwidth Manager Monitor....18-18
Figure 19-1 View Log....19-2
Figure 19-2 Log Settings (ZyWALL 10W)....19-4
Figure 19-3 Reports....19-7
Figure 19-4 Web Site Hits Report Example....19-9
Figure 19-5 Protocol/Port Report Example....19-10
Figure 19-6 LAN IP Address Report Example....19-11
Figure 20-1 System Status....20-1
Figure 20-2 System Status: Show Statistics....20-3
Figure 20-3 DHCP Table....20-4
Figure 20-4 Firmware Upgrade....20-5
Figure 20-5 Firmware Upgrade....20-6
Figure 20-6 Firmware Upload In Process....20-6
Figure 20-7 Network Temporarily Disconnected....20-6
Figure 20-8 Firmware Upload Error....20-7

Figure 20-9 Configuration 20-8
Figure 20-10 Reset Warning Message..... 20-9
Figure 20-11 Configuration Upload Successful 20-10
Figure 20-12 Network Temporarily Disconnected..... 20-10
Figure 20-13 Configuration Upload Error 20-11
Figure 21-1 Initial Screen 21-1
Figure 21-2 Password Screen..... 21-2
Figure 21-3 Main Menu (ZyWALL 100) 21-3
Figure 21-4 Getting Started and Advanced Applications SMT Menus 21-5
Figure 21-5 Advanced Management SMT Menus 21-6
Figure 21-6 Schedule Setup and IPSec VPN Configuration SMT Menus 21-7
Figure 21-7 Menu 23: System Password..... 21-7
Figure 21-8 Example Xmodem Upload 21-8
Figure 22-1 Menu 1: General Setup..... 22-1
Figure 22-2 Configure Dynamic DNS 22-2
Figure 23-1 MAC Address Cloning in WAN Setup 23-1
Figure 23-2 Menu 2: Dial Backup Setup 23-3
Figure 23-3 Menu 2.1 Advanced WAN Setup..... 23-4
Figure 23-4 Menu 11.1 Remote Node Profile (Backup ISP)..... 23-6
Figure 23-5 Menu 11.2: Remote Node PPP Options..... 23-9
Figure 23-6 Remote Node PPP Options Menu Fields..... 23-9
Figure 23-7 Menu 11.3: Remote Node Network Layer Options 23-10
Figure 23-8 Menu 11.4 – Remote Node Setup Script 23-14
Figure 23-9 Menu 11.5: Dial Backup Remote Node Filter 23-15
Figure 24-1 Menu 3: LAN Setup 24-1
Figure 24-2 Menu 3.1: LAN Port Filter Setup 24-2
Figure 24-3 Menu 3: TCP/IP and DHCP Setup..... 24-2
Figure 24-4 Menu 3.2: TCP/IP and DHCP Ethernet Setup 24-3
Figure 24-5 Menu 3.2.1: IP Alias Setup..... 24-5
Figure 24-6 Menu 3.5 – Wireless LAN Setup..... 24-6
Figure 25-1 Menu 5: DMZ Setup..... 25-1
Figure 25-2 Menu 5.1: DMZ Port Filter Setup 25-1
Figure 25-3 Menu 5: TCP/IP Setup..... 25-2
Figure 25-4 Menu 5.2: TCP/IP Setup..... 25-3
Figure 25-5 Menu 5.2.1: IP Alias Setup..... 25-4
Figure 26-1 Menu 4: Internet Access Setup (Ethernet)..... 26-1
Figure 26-2 Internet Access Setup (PPTP)..... 26-4
Figure 26-3 Internet Access Setup (PPPoE)..... 26-5
Figure 27-1 Menu 11 Remote Node Setup..... 27-2
Figure 27-2 Menu 11.1: Remote Node Profile for Ethernet Encapsulation 27-3
Figure 27-3 Menu 11.1: Remote Node Profile for PPPoE Encapsulation..... 27-5

Figure 27-4 Menu 11.1: Remote Node Profile for PPTP Encapsulation....27-7
Figure 27-5 Menu 11.3: Remote Node Network Layer Options for Ethernet Encapsulation....27-8
Figure 27-6 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)....27-11
Figure 27-7 Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)....27-11
Figure 27-8 Menu 11.1: Remote Node Profile....27-12
Figure 27-9 Menu 11.6: Traffic Redirect Setup....27-13
Figure 28-1 Menu 12: IP Static Route Setup (ZyWALL 10W)....28-1
Figure 28-2 Menu 12. 1: Edit IP Static Route....28-2
Figure 29-1 Menu 4: Applying NAT for Internet Access....29-2
Figure 29-2 Menu 11.3: Applying NAT to the Remote Node....29-3
Figure 29-3 Menu 15: NAT Setup....29-4
Figure 29-4 Menu 15.1: Address Mapping Sets....29-5
Figure 29-5 Menu 15.1.255: SUA Address Mapping Rules....29-5
Figure 29-6 Menu 15.1.1: First Set....29-6
Figure 29-7 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set....29-8
Figure 29-8 Menu 15.2: NAT Server Setup (ZyWALL 10)....29-10
Figure 29-9 Multiple Servers Behind NAT Example....29-10
Figure 29-10 NAT Example 1....29-11
Figure 29-11 Menu 4: Internet Access & NAT Example....29-11
Figure 29-12 NAT Example 2....29-12
Figure 29-13 Menu 15.2: Specifying an Inside Server....29-13
Figure 29-14 NAT Example 3....29-14
Figure 29-15 Example 3: Menu 11.3....29-15
Figure 29-16 Example 3: Menu 15.1.1.1....29-15
Figure 29-17 Example 3: Final Menu 15.1.1....29-16
Figure 29-18 Example 3: Menu 15.2....29-16
Figure 29-19 NAT Example 4....29-17
Figure 29-20 Example 4: Menu 15.1.1.1: Address Mapping Rule....29-18
Figure 29-21 Example 4: Menu 15.1.1: Address Mapping Rules....29-18
Figure 29-22 Trigger Port Forwarding Process: Example....29-19
Figure 29-23 Menu 15.3—Trigger Port Setup....29-20
Figure 30-1 Menu 21: Filter and Firewall Setup....30-1
Figure 30-2 Menu 21.2: Firewall Setup....30-2
Figure 31-1 Outgoing Packet Filtering Process....31-2
Figure 31-2 Filter Rule Process....31-3
Figure 31-4 Menu 21: Filter and Firewall Setup....31-4
Figure 31-5 Menu 21.1: Filter Set Configuration....31-4
Figure 31-6 Menu 21.1.1.1: TCP/IP Filter Rule....31-7
Figure 31-7 Executing an IP Filter....31-10
Figure 31-8 Menu 21.1.4.1: Generic Filter Rule....31-11
Figure 31-9 Telnet Filter Example....31-13

Figure 31-10 Example Filter: Menu 21.1.3.1 31-14
Figure 31-11 Example Filter Rules Summary: Menu 21.1.3 31-15
Figure 31-12 Protocol and Device Filter Sets 31-16
Figure 31-13 Filtering LAN Traffic 31-17
Figure 31-14Filtering DMZ Traffic 31-18
Figure 31-15 Filtering Remote Node Traffic 31-18
Figure 32-1 Menu 22: SNMP Configuration 32-1
Figure 33-1 Menu 24: System Maintenance 33-1
Figure 33-2 Menu 24.1: System Maintenance: Status (ZyWALL 100) 33-2
Figure 33-3 Menu 24.2: System Information and Console Port Speed 33-4
Figure 33-4 Menu 24.2.1: System Maintenance: Information (ZyWALL 10W) 33-4
Figure 33-5 Menu 24.2.2: System Maintenance: Change Console Port Speed 33-5
Figure 33-6 Menu 24.3: System Maintenance: Log and Trace 33-6
Figure 33-7 Examples of Error and Information Messages 33-7
Figure 33-8 Menu 24.3.2: System Maintenance: UNIX Syslog (ZyWALL 100) 33-7
Figure 33-9 Call-Triggering Packet Example 33-11
Figure 33-10 Menu 24.4: System Maintenance: Diagnostic 33-12
Figure 33-11 WAN & LAN DHCP 33-13
Figure 34-1 Telnet into Menu 24.5 34-3
Figure 34-2 FTP Session Example 34-4
Figure 34-3 System Maintenance: Backup Configuration 34-7
Figure 34-4 System Maintenance: Starting Xmodem Download Screen 34-7
Figure 34-5 Backup Configuration Example 34-7
Figure 34-6 Successful Backup Confirmation Screen 34-8
Figure 34-7 Telnet into Menu 24.6 34-9
Figure 34-8 Restore Using FTP Session Example 34-10
Figure 34-9 System Maintenance: Restore Configuration 34-10
Figure 34-10 System Maintenance: Starting Xmodem Download Screen 34-10
Figure 34-11 Restore Configuration Example 34-11
Figure 34-12 Successful Restoration Confirmation Screen 34-11
Figure 34-13 Telnet Into Menu 24.7.1: Upload System Firmware 34-12
Figure 34-14 Telnet Into Menu 24.7.2: System Maintenance 34-13
Figure 34-15 FTP Session Example of Firmware File Upload 34-14
Figure 34-16 Menu 24.7.1 As Seen Using the Console Port 34-16
Figure 34-17 Example Xmodem Upload 34-17
Figure 34-18 Menu 24.7.2 As Seen Using the Console Port 34-18
Figure 34-19 Example Xmodem Upload 34-19
Figure 35-1 Command Mode in Menu 24 35-1
Figure 35-2 Valid Commands 35-2
Figure 35-3 Call Control 35-3
Figure 35-4 Budget Management 35-4

Figure 35-5 Call History 35-5
Figure 35-6 Menu 24: System Maintenance 35-6
Figure 35-7 Menu 24.10 System Maintenance: Time and Date Setting 35-7
Figure 36-1 Menu 24.11 – Remote Management Control 36-2
Figure 37-2 IP Routing Policy Setup 37-2
Figure 37-4 Menu 25.1: Sample IP Routing Policy Setup 37-3
Figure 37-5 IP Routing Policy 37-4
Figure 37-6 Menu 3.2: TCP/IP and DHCP Ethernet Setup 37-6
Figure 37-7 Example of IP Policy Routing 37-7
Figure 37-8 IP Routing Policy Example 37-8
Figure 37-9 IP Routing Policy 37-9
Figure 37-10 Applying IP Policies 37-10
Figure 38-1 Schedule Setup 38-1
Figure 38-2 Schedule Set Setup 38-2
Figure 38-3 Applying Schedule Set(s) to a Remote Node (PPPoE) 38-4
Figure 38-4 Applying Schedule Set(s) to a Remote Node (PPTP) 38-5
Figure 39-1 VPN SMT Menu Tree 39-1
Figure 39-2 Menu 27: VPN/IPSec Setup 39-2
Figure 39-3 Menu 27.1: IPSec Summary 39-2
Figure 39-4 Menu 27.1.1: IPSec Setup 39-6
Figure 39-5 Menu 27.1.1.1: IKE Setup 39-12
Figure 39-6 Menu 27.1.1.2: Manual Setup 39-15
Figure 40-1 Menu 27.2: SA Monitor 40-1

List of Tables

Table 1-1 Model Specific Features 1-6
Table 3-1 Ethernet Encapsulation 3-3
Table 3-2 PPTP Encapsulation 3-5
Table 3-3 PPPoE Encapsulation 3-7
Table 3-4 Private IP Address Ranges 3-8
Table 3-5 Example of Network Properties for LAN Servers with Fixed IP Addresses 3-10
Table 3-6 WAN Setup 3-11
Table 4-1 System General Setup 4-1
Table 4-2 DDNS 4-3
Table 4-3 Password 4-5
Table 4-4 Time Zone 4-6
Table 5-1 IP 5-4
Table 5-2 Static DHCP 5-6
Table 5-3 IP Alias 5-7
Table 6-1 Wireless 6-5
Table 6-2 MAC Address Filter 6-7
Table 6-3 802.1X Authentication 6-11
Table 6-4 Local User Database 6-13
Table 6-5 RADIUS 6-14
Table 7-1 DMZ 7-2
Table 8-1 WAN Setup: Route 8-2
Table 8-2 Ethernet Encapsulation 8-3
Table 8-3 PPPoE Encapsulation 8-5
Table 8-4 PPTP Encapsulation 8-7
Table 8-5 RR Service Type 8-9
Table 8-6 IP Setup 8-11
Table 8-7 Traffic Redirect 8-15
Table 8-8Dial Backup Setup 8-18
Table 8-9 Advanced Setup 8-22
Table 9-1 NAT Definitions 9-1
Table 9-2 NAT Mapping Types 9-5
Table 9-3 Services and Port Numbers 9-7
Table 9-4 SUA/NAT Setup 9-9
Table 9-5 Address Mapping 9-11
Table 9-6 Address Mapping Edit 9-13
Table 9-7 Trigger Port 9-15
Table 10-1 IP Static Route Summary 10-1
Table 10-2 Edit IP Static Route 10-3

Table 11-1 Common IP Ports 11-4
Table 11-2 ICMP Commands That Trigger Alerts 11-6
Table 11-3 Legal NetBIOS Commands 11-7
Table 11-4 Legal SMTP Commands 11-7
Table 12-1 Firewall Rules Summary: First Screen 12-6
Table 12-2 Creating/Editing A Firewall Rule 12-9
Table 12-3 Adding/Editing Source and Destination Addresses 12-11
Table 12-4 Creating/Editing A Custom Port 12-12
Table 12-5 Predefined Services 12-17
Table 12-6 Attack Alert 12-22
Table 13-1 Content Filter: Categories 13-2
Table 13-2 Content Filter: Free 13-6
Table 13-3 Content Filter: iCard 13-7
Table 13-4 Content Filter: List Update 13-9
Table 13-5 Content Filter: Exempt Zone 13-10
Table 13-6 Content Filter: Customize 13-12
Table 13-7 Content Filter: Keyword Blocking 13-14
Table 14-1 VPN and NAT 14-6
Table 15-1 AH and ESP 15-2
Table 15-2 Summary 15-4
Table 15-3 Local ID Type and Content Fields 15-7
Table 15-4 Peer ID Type and Content Fields 15-7
Table 15-5 Matching ID Type and Content Configuration Example 15-8
Table 15-6 Mismatching ID Type and Content Configuration Example 15-8
Table 15-7 VPN IKE 15-11
Table 15-8 VPN IKE: Advanced 15-18
Table 15-9 VPN Manual Setup 15-22
Table 15-10 SA Monitor 15-26
Table 15-11 SA Monitor 15-27
Table 15-12 Telecommuter and Headquarters Configuration Example 15-28
Table 16-1 Telnet 16-4
Table 16-2 FTP 16-5
Table 16-3 WWW 16-6
Table 16-4 SNMP Traps 16-8
Table 16-5 SNMP 16-10
Table 16-6 DNS 16-12
Table 16-7 Security 16-13
Table 17-1 Configuring UPnP 17-3
Table 18-1 Application and Subnet-based Bandwidth Management Example 18-4
Table 18-2 Bandwidth Manager: Summary 18-12
Table 18-3 Bandwidth Manager: Class Setup 18-13

Table 18-4 Bandwidth Manager: Class Configuration 18-15
Table 18-5Services and Port Numbers 18-16
Table 18-6 Bandwidth Management Statistics 18-17
Table 18-7 Bandwidth Manager Monitor 18-18
Table 19-1 View Log 19-3
Table 19-2 Log Settings Screen (ZyWALL 10W) 19-5
Table 19-3 Reports 19-7
Table 19-4 Web Site Hits Report 19-9
Table 19-5 Protocol/ Port Report 19-10
Table 19-6 LAN IP Address Report 19-11
Table 19-7 Report Specifications 19-12
Table 20-1 System Status 20-2
Table 20-2 System Status: Show Statistics 20-3
Table 20-3 DHCP Table 20-4
Table 20-4 Restore Configuration 20-9
Table 21-1 Main Menu Commands 21-2
Table 21-2 Main Menu Summary 21-3
Table 22-1 General Setup Menu Field 22-1
Table 22-2 Configure Dynamic DNS Menu Fields 22-3
Table 23-1 MAC Address Cloning in WAN Setup 23-2
Table 23-2 Menu 2: Dial Backup Setup 23-3
Table 23-3 Advanced WAN Port Setup: AT Commands Fields 23-4
Table 23-4 Advanced WAN Port Setup: Call Control Parameters 23-5
Table 23-5 Fields in Menu 11.1 Remote Node Profile (Backup ISP) 23-6
Table 23-6 Remote Node Network Layer Options Menu Fields 23-10
Table 23-7 Remote Node Script Menu Fields 23-14
Table 24-1 DHCP Ethernet Setup Menu Fields 24-3
Table 24-2 LAN TCP/IP Setup Menu Fields 24-4
Table 24-3 IP Alias Setup Menu Fields 24-5
Table 24-4 Wireless LAN Setup Menu Fields 24-7
Table 26-1 Menu 4: Internet Access Setup Menu Fields 26-1
Table 26-2 New Fields in Menu 4 (PPTP) Screen 26-4
Table 26-3 New Fields in Menu 4 (PPPoE) screen 26-5
Table 27-1 Fields in Menu 11.1 27-3
Table 27-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific) 27-6
Table 27-3 Fields in Menu 11.1 (PPTP Encapsulation) 27-7
Table 27-4 Remote Node Network Layer Options Menu Fields 27-8
Table 27-5 Menu 11.1: Remote Node Profile (Traffic Redirect Field) 27-12
Table 27-6 Traffic Redirect Setup 27-13
Table 28-1 IP Static Route Menu Fields 28-2
Table 29-1 Applying NAT in Menus 4 & 11.3 29-3

Table 29-2 SUA Address Mapping Rules 29-5
Table 29-3 Fields in Menu 15.1.1 29-7
Table 29-4 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set 29-8
Table 29-5 Menu 15.3—Trigger Port Setup Description 29-21
Table 31-1 Abbreviations Used in the Filter Rules Summary Menu 31-5
Table 31-2 Rule Abbreviations Used 31-6
Table 31-3 TCP/IP Filter Rule Menu Fields 31-7
Table 31-4 Generic Filter Rule Menu Fields 31-11
Table 32-1 SNMP Configuration Menu Fields 32-1
Table 32-2 SNMP Traps 32-2
Table 33-1 System Maintenance: Status Menu Fields 33-2
Table 33-2 Fields in System Maintenance: Information 33-5
Table 33-3 System Maintenance Menu Syslog Parameters 33-8
Table 33-4 System Maintenance Menu Diagnostic 33-13
Table 34-1 Filename Conventions 34-2
Table 34-2 General Commands for GUI-based FTP Clients 34-4
Table 34-3 General Commands for GUI-based TFTP Clients 34-6
Table 35-1 Valid Commands 35-2
Table 35-2 Budget Management 35-4
Table 35-3 Call History Fields 35-5
Table 35-4 Time and Date Setting Fields 35-7
Table 36-1 Menu 24.11 – Remote Management Control 36-2
Table 37-1 IP Routing Policy Setup 37-3
Table 37-2 IP Routing Policy 37-4
Table 38-1Schedule Set Setup Fields 38-2
Table 39-1 Menu 27.1: IPSec Summary 39-3
Table 39-2 Menu 27.1.1: IPSec Setup 39-6
Table 39-3 Menu 27.1.1.1: IKE Setup 39-12
Table 39-4 Active Protocol: Encapsulation and Security Protocol 39-14
Table 39-5 Menu 27.1.1.2: Manual Setup 39-15
Table 40-1 Menu 27.2: SA Monitor 40-2

Preface

About Your ZyWALL

Congratulations on your purchase of the ZyWALL Internet Security Gateway.

About This User's Manual

This manual is designed to guide you through the configuration of your ZyWALL for its various applications. The web configurator parts of this guide contain background information on features configurable by web configurator and SMT. The SMT parts of this guide contain background information on features not configurable by web configurator.
This manual may refer to the ZyWALL Internet Security Gateway as the ZyWALL.
This manual covers the ZyWALL 10 to100 models. Supported features and the details of the features, vary from model to model. Not every feature applies to every model; refer to the *Model Comparison Chart* in chapter 1 of this user's guide to see what features are specific to your ZyWALL model.

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

Related Documentation

- Support Disk
  Refer to the included CD for support documents.
- Read Me First or Quick Start Guide
  The Read Me First or Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
  Embedded web help for descriptions of individual screens and supplementary information.
- Packing List Card
  The Packing List Card lists all items that should have come in the package.
- Reference Guide
  The Reference Guide provides background information on some of the ZyWALL's features and also includes commands for use with the command interpreter.
- Certifications
  Refer to the product page at www.zyxel.com for information on product certifications.
- ZyXEL Glossary and Web Site
  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User's Guide Feedback

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

Syntax Conventions

- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one of the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- The choices of a menu item are in **Bold Arial** font.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g." as a shorthand for "for instance" and "i.e." for "that is" or "in other words" throughout this manual.

Part I:

Getting Started

This part helps you get to know your ZyWALL, introduces the web configurator and covers how to configure the Wizard Setup screens.

Chapter 1
Getting to Know Your ZyWALL

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

1.1 ZyWALL Internet Security Gateway Overview

The ZyWALL is the ideal secure gateways for all data passing between the Internet and the LAN.
By integrating NAT, firewall and VPN capability, ZyXEL's ZyWALL is a complete security solution that protects your Intranet and efficiently manages data traffic on your network.
The embedded web configurator is easy to operate and totally independent of your computer's operating system.

1.1.1 ZyWALL 10 Internet Security Gateway for Small/Home Offices

The ZyWALL 10 offers all necessary basic firewall functionality for small office or home use. It supports VPN connections, real time attack alert and log systems, and content filtering while providing a user-friendly interface for installation and configuration.

1.1.2 ZyWALL 10W Wireless Ready Internet Security Gateway

The ZyWALL 10W is wireless ready; thus giving you the option of adding a wireless LAN to your home or small business network.

1.1.3 ZyWALL 30W Internet Security Gateway with Wireless Ready for SOHO

The ZyWALL 30W adds more firewall protection and gives you the option of adding a wireless LAN to your small office or home office (SOHO).

1.1.4 ZyWALL 50 Internet Security Gateway for Small/Home Office and Small Businesses

The ZyWALL 50 adds more processing power to provide the robust firewall protection necessary for small to medium businesses to handle e-business.

1.1.5 ZyWALL 100 Internet Security Gateway for Small to Medium Businesses

The ZyWALL 100 offers the highest degree of functionality and security for business applications. It supports up to 100 IPSec VPN connections and increases network security by adding a De-Militarized Zone (DMZ) port for use with publicly accessible servers.

1.2 ZyWALL Features

The following sections describe ZyWALL features. Features vary by ZyWALL model.

1.2.1 Physical Features

Auto-negotiating 10/100 Mbps Ethernet LAN

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

Auto-crossover 10/100 Mbps Ethernet LAN

The LAN interface automatically adjusts to either a crossover or straight-through Ethernet cable. This feature is not available on all models.

Auto-negotiating 10/100 Mbps Ethernet DMZ

Public servers (Web, FTP, etc.) attached to the DeMilitarized Zone (DMZ) port are visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death) and can also be accessed from the secure LAN. This feature is not available on all models.

10/100 Mbps Ethernet WAN

The 10/100 Mbps Ethernet WAN port attaches to the Internet via broadband modem or router. This feature is not available on all models.

Backup WAN or Auxiliary

The Dial Backup or Auxiliary port can be used in reserve as a traditional dial-up connection when/if ever the broadband connection to the WAN port fails. This feature is not available on all models.

Time and Date

The ZyWALL allows you to get the current time and date from an external server when you turn on your ZyWALL. You can also set the time manually. The Real Time Chip (RTC) keeps track of the time and date (not available in all models).

Reset Button

The ZyWALL reset button is built into the rear panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33. This feature is not available on all models.

PCMCIA Port

The PCMCIA port provides the option of a wireless LAN. This feature is not available on all models.

IEEE 802.11b 11 Mbps Wireless LAN

The optional 11 Mbps wireless LAN card provides mobility and a fast network environment for small and home offices. Users can connect to the local area network without any wiring efforts and enjoy reliable high-speed connectivity. This feature is not available on all models.

1.2.2 Non-Physical Features

Bandwidth Management

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

IPSec VPN Capability

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

Firewall

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

RADIUS (RFC2138, 2139)

RADIUS (Remote Authentication Dial In User Service) server enables authentication, authorization and accounting for your wireless network. This feature is not available on all models.

IEEE 802.1x for Network Security

The ZyWALL supports the IEEE 802.1x standard that works with the IEEE 802.11 to enhance user authentication. With the local user profile, the ZyWALL allows you to configure up 32 user profiles without a network authentication server. In addition, centralized user and accounting management is possible on an optional network authentication server. This feature is not available on all models.

Content Filtering

The ZyWALL can block web features such as ActiveX controls, Java applets and cookies, as well as disable web proxies. The ZyWALL can block specific URLs by using the keyword feature. It also allows the

administrator to define time periods and days during which content filtering is enabled and to include or exclude a range of users on the LAN from content filtering.

Wireless LAN MAC Address Filtering

MAC Address Filtering together with ESSID (Extended Service Set IDentifier) and WEP (Wired Equivalent Privacy) ensure the most secure wireless solution. This feature is not available on all models.

Brute-Force Password Guessing Protection

The ZyWALL has a special protection mechanism to discourage brute-force password guessing attacks on the ZyWALL's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendices for details about this feature.[1]

Packet Filtering

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

Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the ZyWALL and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network. This feature is not available on all models.

Call Scheduling

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

PPPoE

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

PPTP Encapsulation

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

Dynamic DNS Support

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

[1] Brute Force Password Protection was not available on every model at the time of writing.

IP Multicast

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

IP Alias

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

IP Policy Routing

IP Policy Routing provides a mechanism to override the default routing behavior and alter packet forwarding based on the policies defined by the network administrator. This feature is not available on all models.

Central Network Management

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

SNMP

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

Network Address Translation (NAT)

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

Traffic Redirect

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

Port Forwarding

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

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyWALL has built-in DHCP server

capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client. The ZyWALL can also act as a surrogate DHCP server (**DHCP Relay**) where it relays IP address assignment from the actual real DHCP server to the clients.

Full Network Management

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

RoadRunner Support

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

Logging and Tracing

- Built-in message logging and packet tracing.
- Unix syslog facility support.
- Firewall logs.
- Content filtering logs.

Upgrade ZyWALL Firmware via LAN

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

Embedded FTP and TFTP Servers

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

1.2.3 Model Specific Features

This table lists the differences between models; it does not include features that are common to all of the ZyWALL 10 to 100 models.

Table 1-1 Model Specific Features

ZYWALL MODEL / FEATURES	100	50	10W	30W	10
Firmware Version Number	3.52	3.52	3.61	3.61	3.52
Dial Backup (or Auxiliary)	O		*	*	
PCMCIA Slot	O		O	O	
PCMCIA Card Release Button			O	O	

Table 1-1 Model Specific Features

ZYWALL MODEL / FEATURES	100	50	10W	30W	10
802.11b Wireless LAN Support	O		O	O	
802.1x Wireless LAN Support	O		O	O	
Real Time Chip	O	O	O	O	
Auto-crossover 10/100 Mbps Ethernet LAN			O	O	
Auto-negotiating 10/100 Mbps Ethernet DMZ	O				
Auto-negotiating 10/100 Mbps Ethernet WAN	O	O	O	O	
Reset Button	O	O	O	O	
Uplink Button	O	O	O	O	
Power Switch	O				
Traffic Redirect	O	O	O	O	
Bandwidth Management	O				
IP Policy Routing	O				
Number of Static Routes	50	30	12	30	12
Number of Firewall Rules	400	100	50	100	30
Number of Custom Ports for Firewall Rules	50	30	30	30	10
Number of IPSec VPN Security Associations	100	50	10	30	10
UPnP			O	O	

* The ZyWALL 10W and 30W use the same port for console management and for an auxiliary (backup) WAN connection.

Table Key: An “O” in a model’s column shows that the model has the specified feature.

1.2.4 ZyWALL 100 Note

The ZyWALL 100 is designed to act as a secure gateway for all data passing between the Internet and the LAN or the DMZ. It has three Ethernet ports, one RS-232 auxiliary port and one PCMCIA port (for optional wireless applications), which are used to physically separate the network into three areas.

I. LAN Network (a trusted network)

- LAN port: The auto-negotiating 10/100 Mbps Ethernet LAN interface automatically detects if it's on a 10 or a 100 Mbps Ethernet. Attach computers that are to be secured from the outside world to this port. These computers will have access to e-mail, FTP and the World Wide Web but incoming connections (from the Internet) are only allowed if the connection is originally initiated from the LAN computer or a firewall rule has been specifically configured to allow access.

II. DMZ Network

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

III. WAN Network

- WAN port: The 10/100 Mbps Ethernet WAN port attaches to the Internet via broadband modem or router.
- Dial Backup port: This auxiliary port can be used as a backup line when/if the broadband connection to the WAN port fails.

1.3 Applications for the ZyWALL

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

1.3.1 Secure Broadband Internet Access via Cable or DSL Modem

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

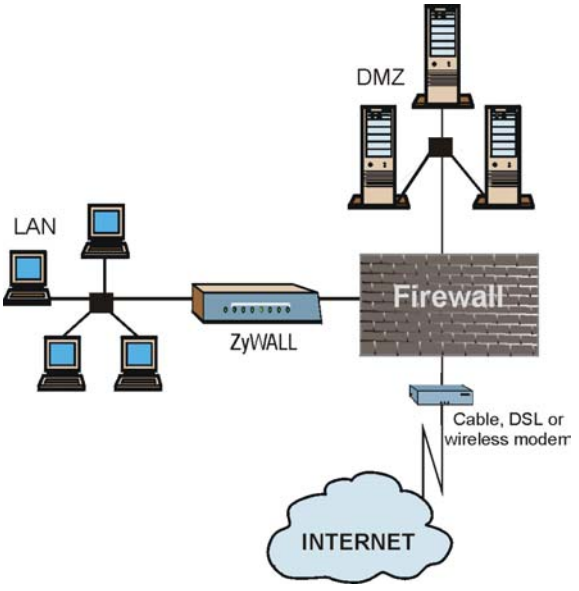


Figure 1-1 Secure Internet Access via Cable, DSL or Wireless Modem

1.3.2 VPN Application

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

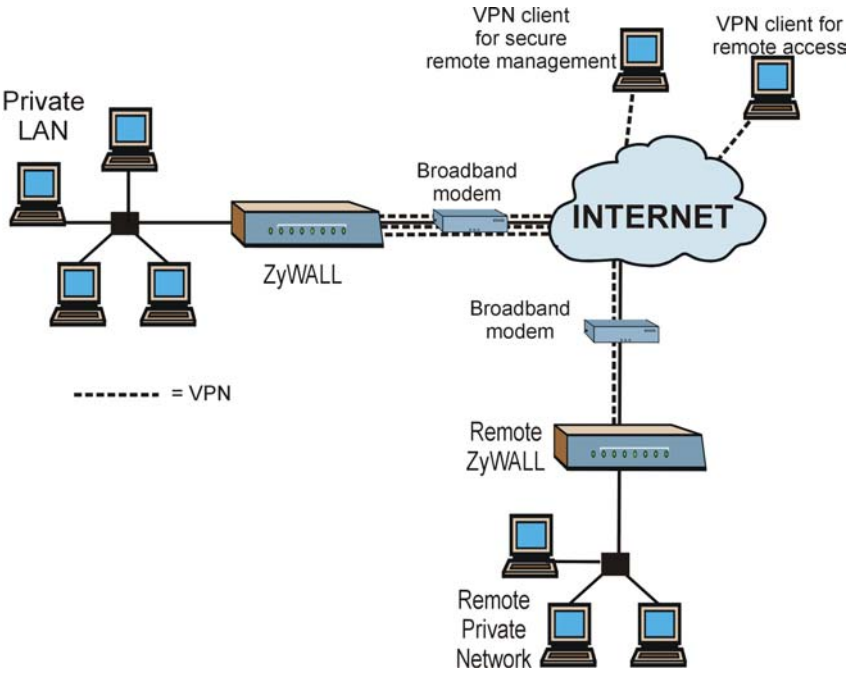


Figure 1-2 VPN Application

Chapter 2
Introducing the Web Configurator

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

2.1 Web Configurator Overview

The embedded web configurator allows you to manage the ZyWALL from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels. The screens you see in the web configurator may vary somewhat from the ones shown in this document due to differences between individual ZyWALL models or firmware versions.

2.2 Accessing the ZyWALL Web Configurator

Step 1. Make sure your ZyWALL hardware is properly connected and prepare your computer/computer network to connect to the ZyWALL (refer to the *Quick Start Guide*).

Step 2. Launch your web browser.

Step 3. Type "192.168.1.1" as the URL.

Step 4. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

Step 5. You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

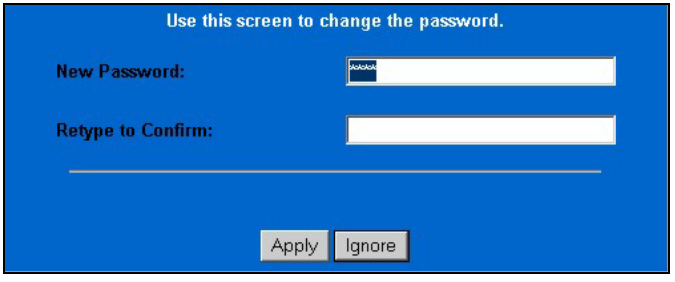


Figure 2-1 Change Password Screen

Step 6. You should now see the **MAIN MENU** screen (see *Figure 2-3*).

The ZyWALL automatically times out after five minutes of inactivity. Simply log back into the ZyWALL if this happens to you.

2.3 Resetting the ZyWALL

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

2.3.1 Procedure To Use The Reset Button

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

Step 1. Press the **RESET** button for ten seconds, and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the ZyWALL restarts. Otherwise, go to step 2.

Step 2. Turn the ZyWALL off.

Step 3. While pressing the **RESET** button, turn the ZyWALL on.

Step 4. Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 10 or 15 seconds. This indicates that the defaults have been restored and the ZyWALL is now restarting.

Step 5. Release the **RESET** button and wait for the ZyWALL to finish restarting.

2.3.2 Uploading a Configuration File Via Console Port

Step 6. Download the default configuration file from the ZyXEL FTP site, unzip it and save it in a folder.

Step 7. Turn off the ZyWALL, begin a terminal emulation software session and turn on the ZyWALL again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.

Step 8. Enter "y" at the prompt below to go into debug mode.

Step 9. Enter "atlc" after "Enter Debug Mode" message.

Step 10. Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.

Step 11. Click **Transfer**, then **Send File** to display the following screen.

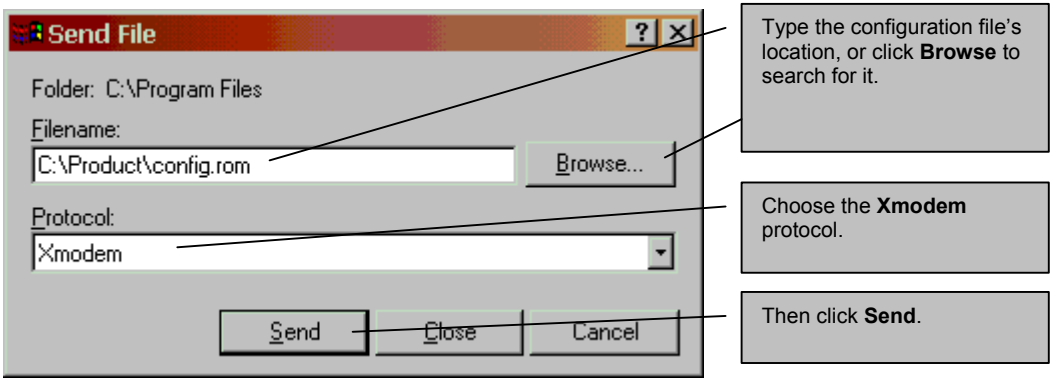


Figure 2-2 Example Xmodem Upload

Step 12. After successful firmware upload, enter "atgo" to restart the router.

2.4 Navigating the ZyWALL Web Configurator

The following summarizes how to navigate the web configurator from the **MAIN MENU** screen.

Follow the instructions you see in the MAIN MENU screen or click the HELP icon (located in the top right corner of most screens) to view online help.

The HELP icon does not appear in the MAIN MENU screen.

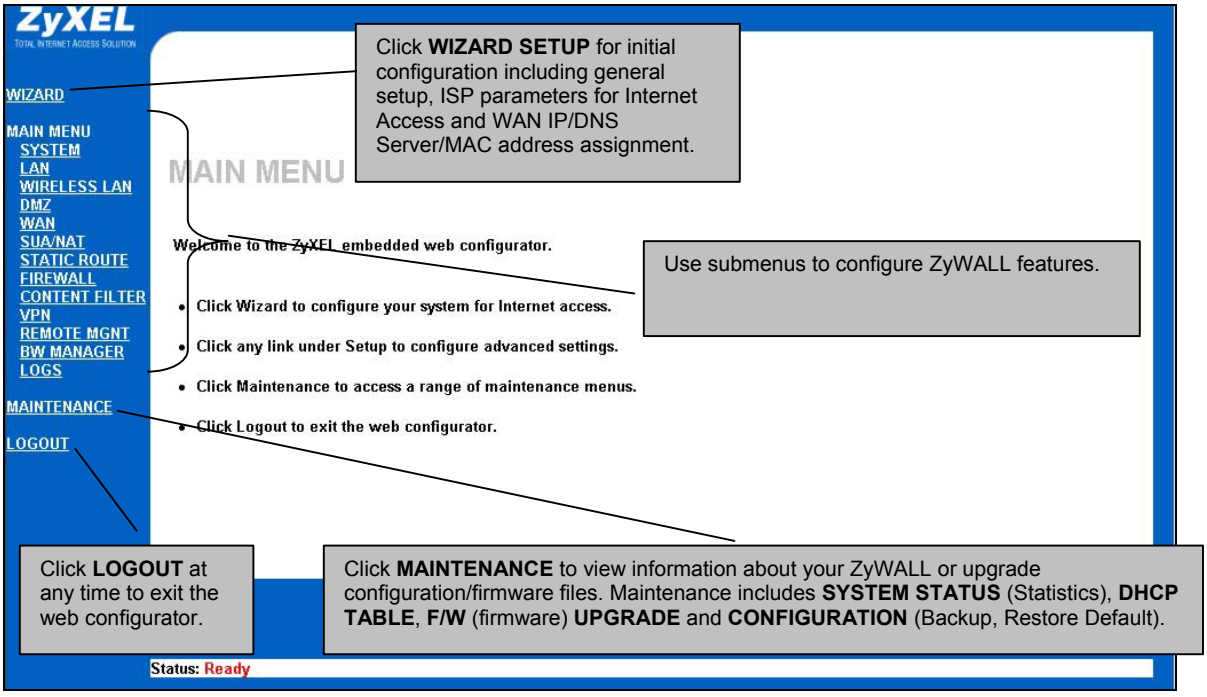


Figure 2-3 The MAIN MENU Screen of the Web Configurator

Chapter 3
Wizard Setup

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

3.1 Wizard Setup Overview

The web configurator's setup wizard helps you configure your device to access the Internet. The second screen has three variations depending on what encapsulation type you use. Refer to your ISP checklist in the *Quick Start Guide* to know what to enter in each field. Leave a field blank if you don't have that information.

3.2 Wizard Setup: General Setup and System Name

General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

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

3.2.1 Domain Name

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

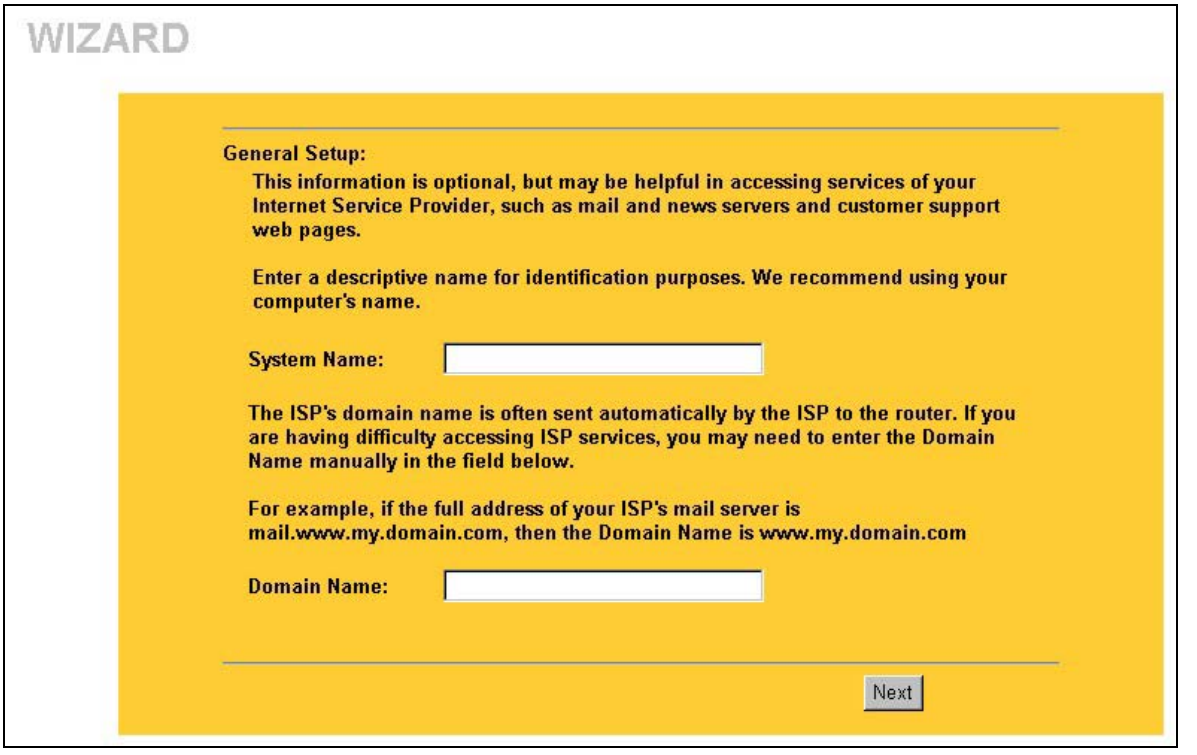


Figure 3-1 Wizard 1

3.3 Wizard Setup: Screen 2

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

3.3.1 Ethernet

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

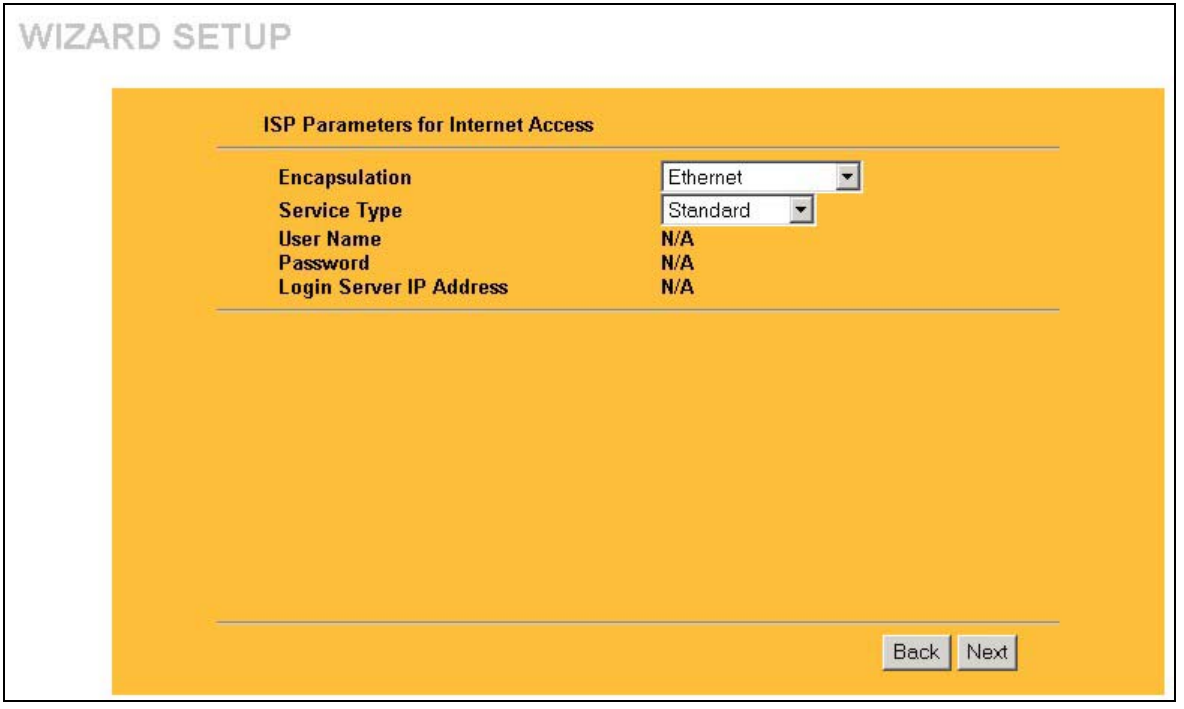


Figure 3-2 Wizard 2: Ethernet Encapsulation

The following table describes the fields in this screen.

Table 3-1 Ethernet Encapsulation

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

Table 3-1 Ethernet Encapsulation

LABEL	DESCRIPTION
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example “login1.telia.com”.
Relogin Period (min) (Telia Login only)	The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyWALL to wait between logins.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

3.3.2 PPTP Encapsulation

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

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

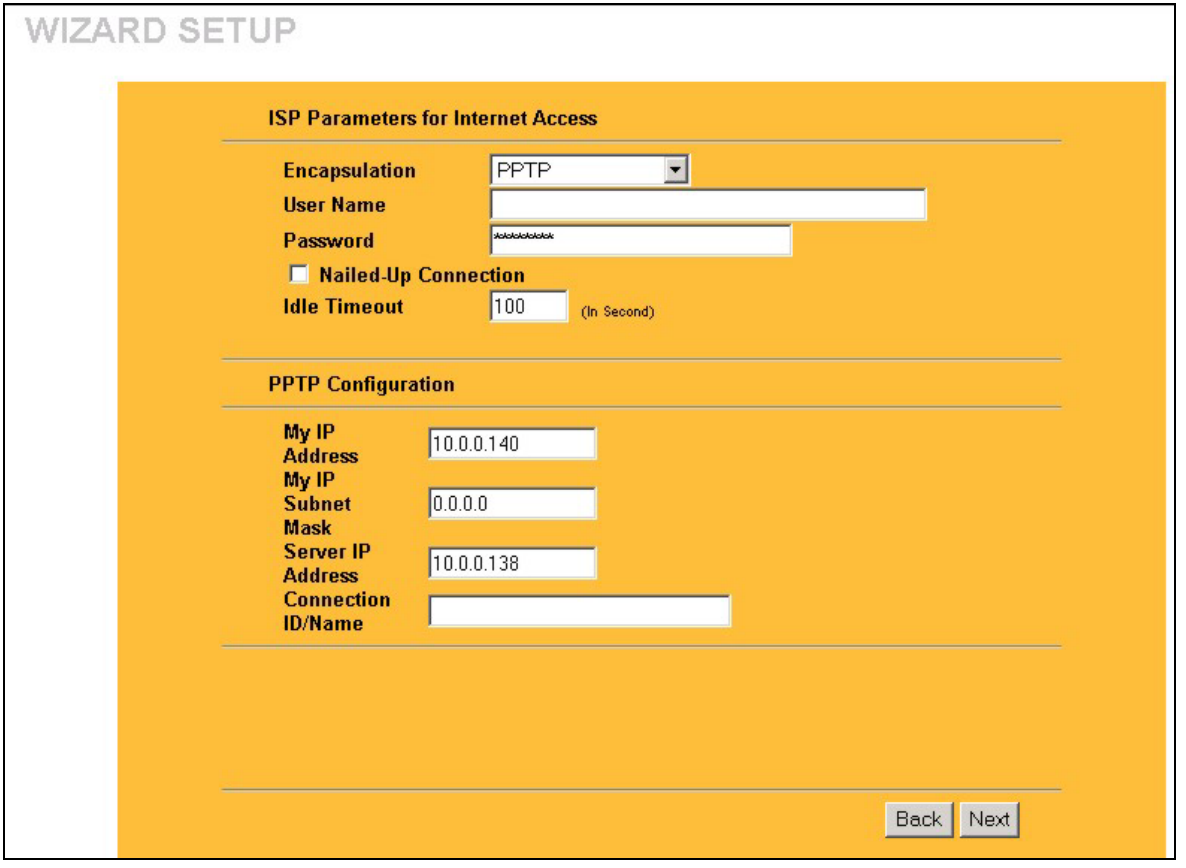


Figure 3-3 Wizard 2: PPTP Encapsulation

The following table describes the fields in this screen.

Table 3-2 PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select **PPTP** from the drop-down list box.
User Name	Type the user name given to you by your ISP.

Table 3-2 PPTP Encapsulation

LABEL	DESCRIPTION
Password	Type the password associated with the User Name above.
Nailed Up Connection	Select **Nailed Up Connection** 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. The default is 45 seconds.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your xDSL modem.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

3.3.3 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example xDSL, cable, wireless, etc.) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

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

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

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

Refer to the *Reference Guide* for more information on PPPoE.

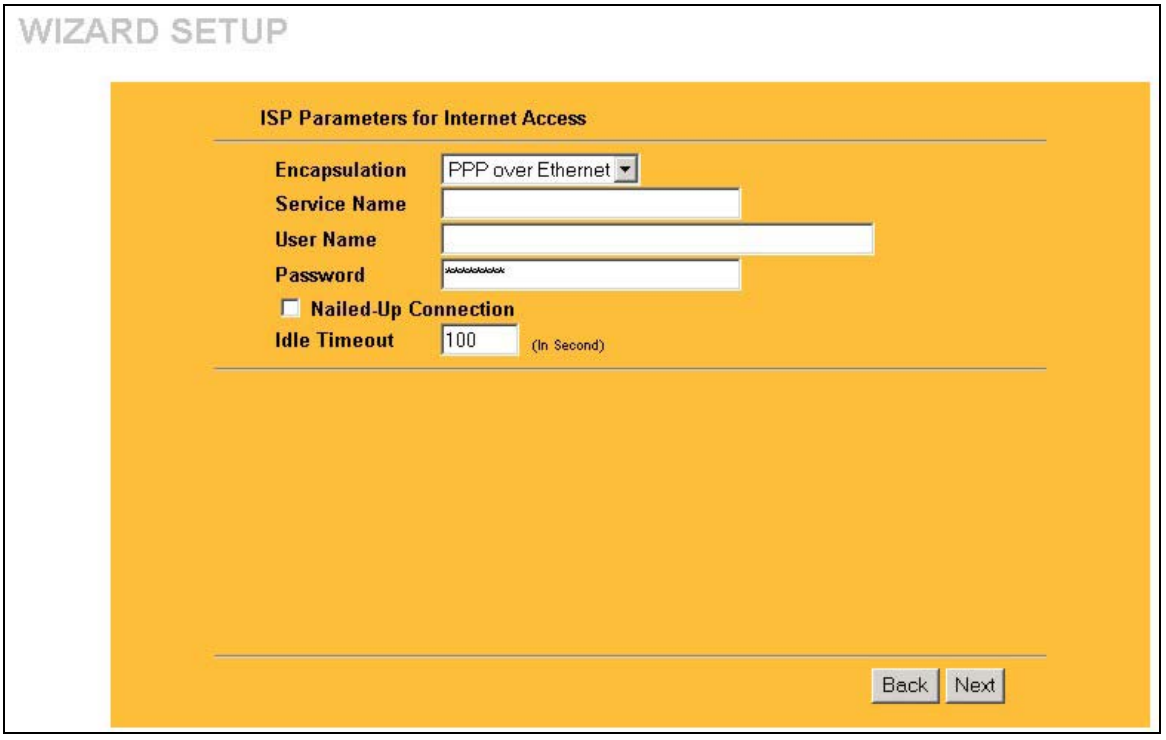


Figure 3-4 Wizard2: PPPoE Encapsulation

The following table describes the fields in this screen.

Table 3-3 PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose an encapsulation method from the pull-down list box. PPPoE forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Nailed Up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.

Table 3-3 PPPoE Encapsulation

LABEL	DESCRIPTION
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

3.4 Wizard Setup: Screen 3

The third wizard screen allows you to configure WAN IP address assignment, DNS server address assignment and the WAN MAC address.

3.4.1 WAN IP Address Assignment

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

Table 3-4 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

3.4.2 IP Address and Subnet Mask

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

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

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

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyWALL, but make sure that no other device on your network is using that IP address. The subnet mask specifies the network number portion of an IP address. Your ZyWALL will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyWALL unless you are instructed to do otherwise.

3.4.3 DNS Server Address Assignment

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

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

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.
2. If the ISP did not give you DNS server information, leave the DNS Server fields in DHCP Setup set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

3.4.4 WAN MAC Address

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

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

ZyXEL recommends you clone the MAC address from a computer on your LAN even if your ISP does not require MAC address authentication.

Your ZyWALL WAN Port is always set at half-duplex mode as most cable/DSL modems only support half-duplex mode. Make sure your modem is in half-duplex mode. Your ZyWALL supports full duplex mode on the LAN side.

Table 3-5 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(ZyWALL LAN IP)

The third wizard screen varies according to the type of encapsulation that you select in the second wizard screen.

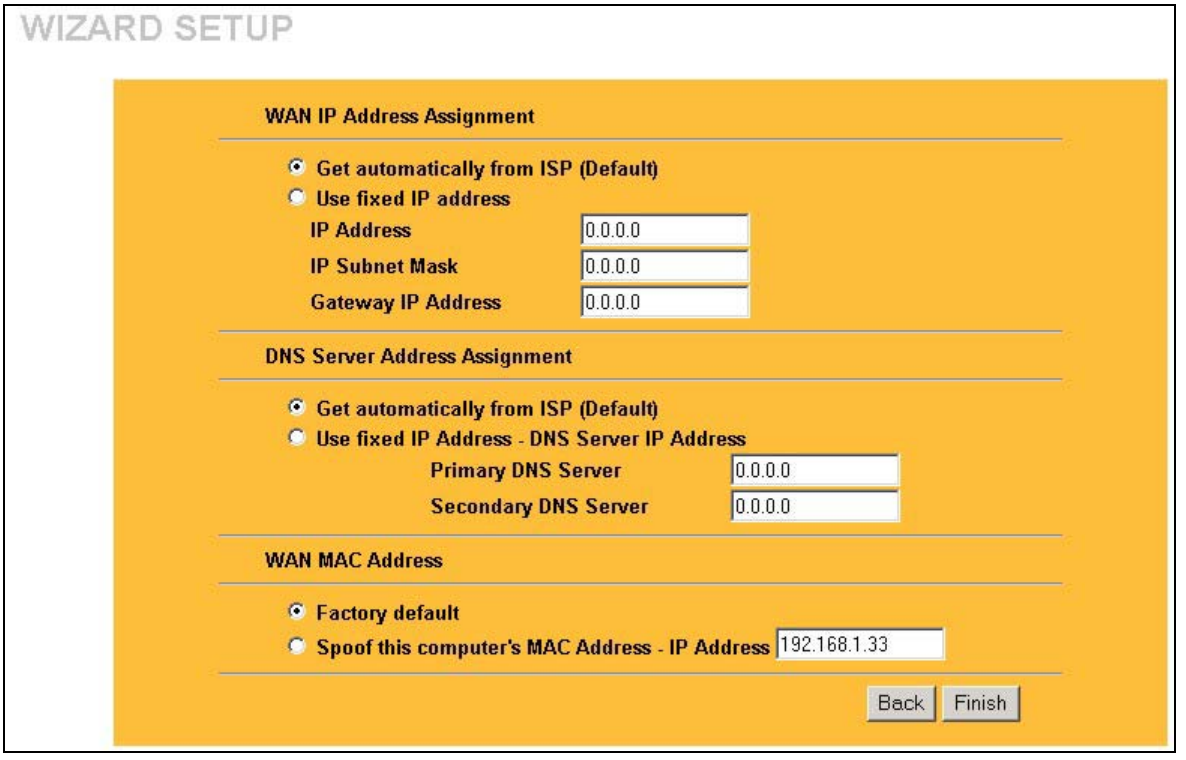


Figure 3-5 Wizard 3

The following table describes the fields in this screen.

Table 3-6 WAN Setup

LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
IP Subnet Mask	Enter the IP subnet mask in this field if you selected **Use Fixed IP Address**. This field is not available when you select PPPoE encapsulation in the previous wizard screen.

Table 3-6 WAN Setup

LABEL	DESCRIPTION
Gateway IP Address	Enter the gateway IP address in this field if you selected **Use Fixed IP Address**. This field is not available when you select PPPoE encapsulation in the previous wizard screen.
DNS Server Address Assignment	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.
Get automatically from ISP	Select this option if your ISP does not give you DNS server addresses. This option is selected by default.
Use fixed IP address - DNS Server IP Address	Select this option If your ISP provides you a DNS server address.
Primary/Secondary DNS Server	If you selected the **Use fixed IP address – Primary/Secondary DNS Server** option, enter the provided DNS addresses in these fields.
WAN MAC Address	The MAC address field allows you to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN.
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different rom file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to complete and save the wizard setup.

3.5 Basic Setup Complete

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

Part II:

System, LAN and Wireless LAN

This part covers configuration of the system, LAN, and wireless LAN screens.

Chapter 4
System Screens

This chapter provides information on the System screens.

4.1 System Overview

See the *Wizard Setup* chapter for more information on the next few screens.

4.2 Configuring General Setup

Click **SYSTEM** to open the **General** screen.

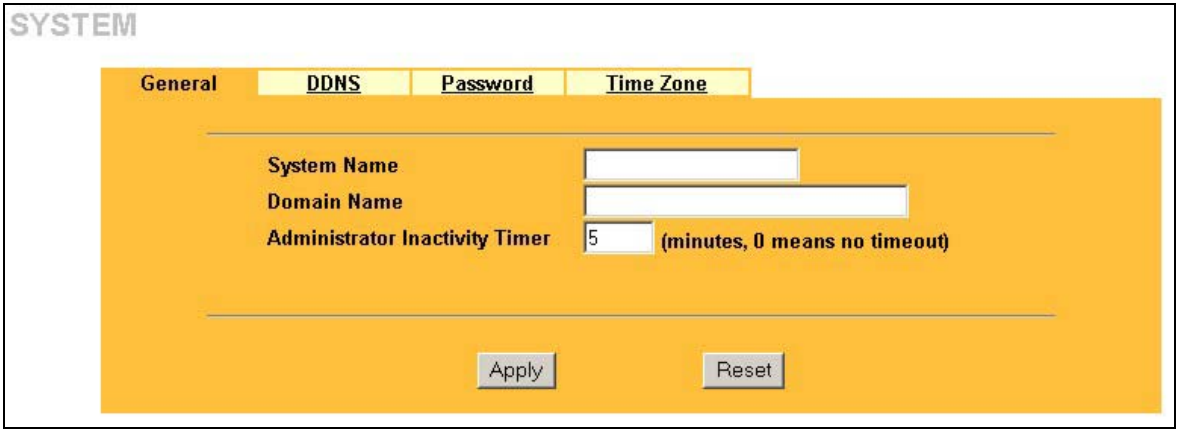


Figure 4-1 System General Setup

The following table describes the fields in this screen.

Table 4-1 System General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field (see the *Wizard Setup* chapter for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.

Table 4-1 System General Setup

LABEL	DESCRIPTION
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

4.3 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a DNS-like address (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name. The Dynamic DNS service provider will give you a password or key.

4.3.1 DYNDNS Wildcard

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

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

4.4 Configuring Dynamic DNS

To change your ZyWALL's DDNS, click **SYSTEM**, then the **DDNS** tab. The screen appears as shown.

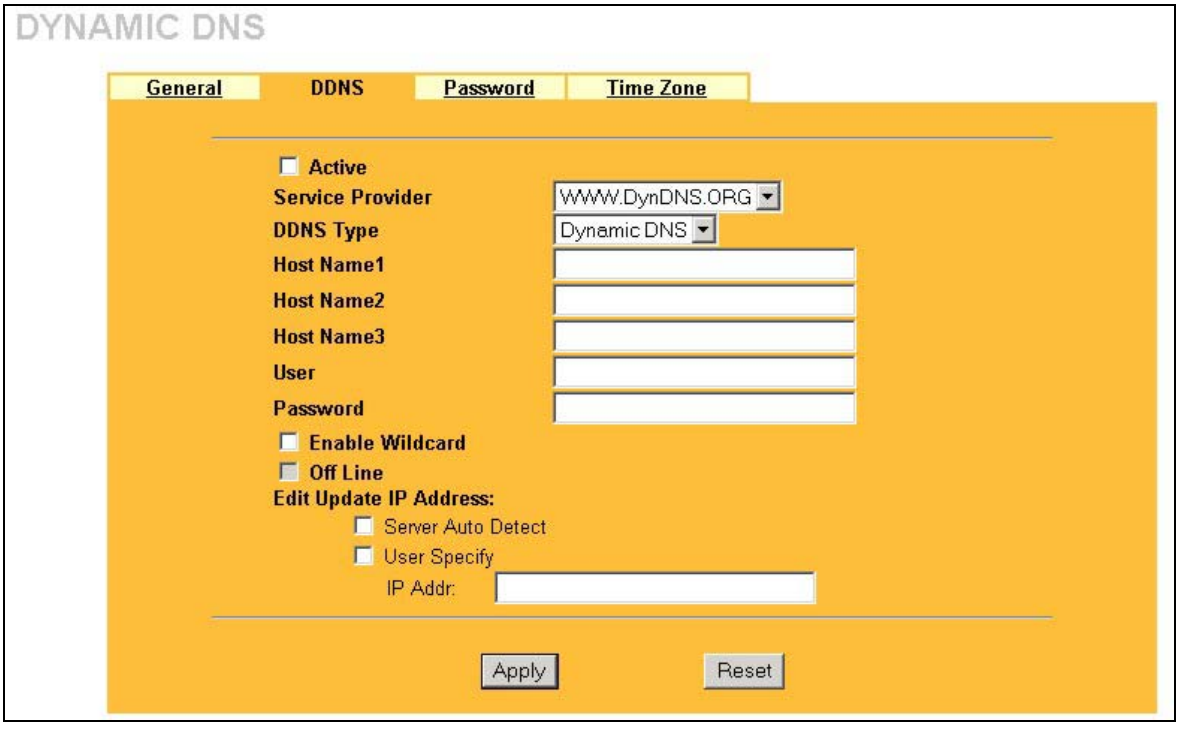


Figure 4-2 DDNS

The following table describes the fields in this screen.

Table 4-2 DDNS

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").
User	Enter your user name.
Password	Enter the password assigned to you.

Table 4-2 DDNS

LABEL	DESCRIPTION
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Off Line	This option is available when **CustomDNS** is selected in the **DDNS Type field**. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Edit Update IP Address:	
Server Auto Detect	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
User Specify	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.
IP Addr	Enter the IP address if you select the **User Specify** option.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

4.5 Configuring Password

To change your ZyWALL's password (recommended), click **SYSTEM**, then the **Password** tab. The screen appears as shown. This screen allows you to change the ZyWALL's password.

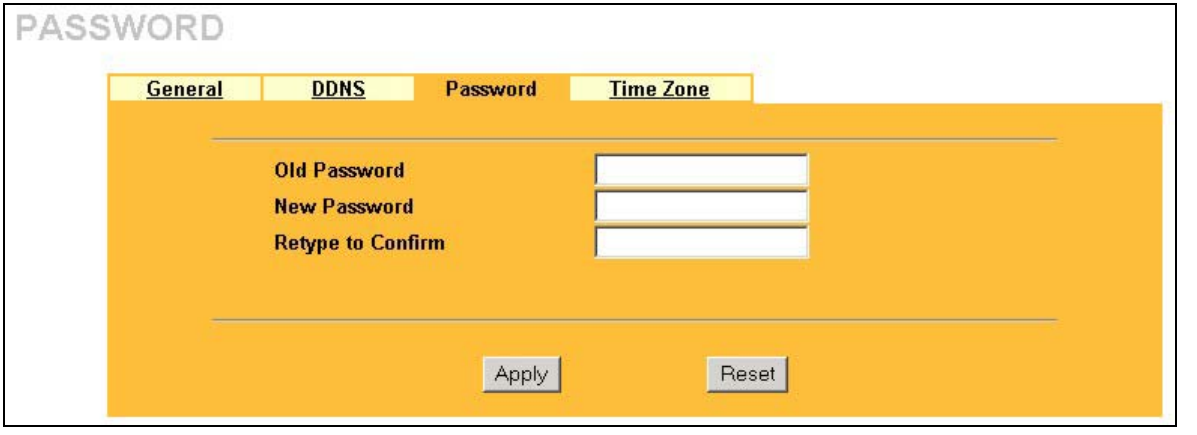


Figure 4-3 Password

The following table describes the fields in this screen.

Table 4-3 Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

4.6 Configuring Time Zone

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

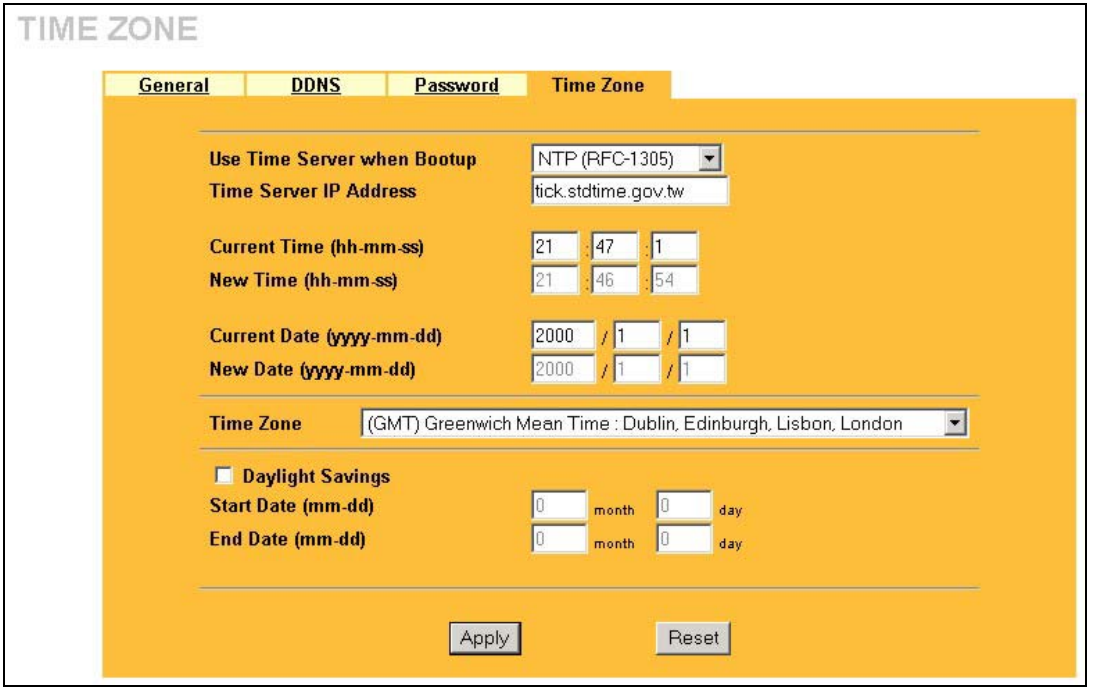


Figure 4-4 Time Zone

The following table describes the fields in this screen.

Table 4-4 Time Zone

LABEL	DESCRIPTION
Use Time Server when Bootup	Select the time service protocol that your time server sends when you turn on the ZyWALL. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305),** is similar to Time (RFC 868). Select **None** to enter the time and date manually.
Time Server IP Address	Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information (the default is tick.stdtime.gov.tw).
Current Time	This field displays the time of your ZyWALL. Each time you reload this page, the ZyWALL synchronizes the time with the time server.
New Time	This field displays the last updated time from the time server. When you select **None** in the **Use Time Server when Bootup** field, enter the new time in this field and then click **Apply**.
Current Date	This field displays the date of your ZyWALL. Each time you reload this page, the ZyWALL synchronizes the time with the time server.
New Date	This field displays the last updated date from the time server. When you select **None** in the **Use Time Server when Bootup** field, enter the new date in this field and then click **Apply**.
Time Zone	Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. 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.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**.

Table 4-4 Time Zone

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 5
LAN Screens

This chapter describes how to configure LAN settings.

5.1 LAN Overview

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

5.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyWALL as a DHCP server or disable it. When configured as a server, the ZyWALL provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

5.2.1 IP Pool Setup

The ZyWALL is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the ZyWALL itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

5.2.2 Primary and Secondary DNS Server

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter.

5.3 LAN TCP/IP

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

5.3.1 Factory LAN Defaults

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

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

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

5.3.2 IP Address and Subnet Mask

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter for this information.

5.3.3 RIP Setup

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

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

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

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

5.3.4 Multicast

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

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

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

5.4 Configuring IP

Click **LAN** to open the **IP** screen.

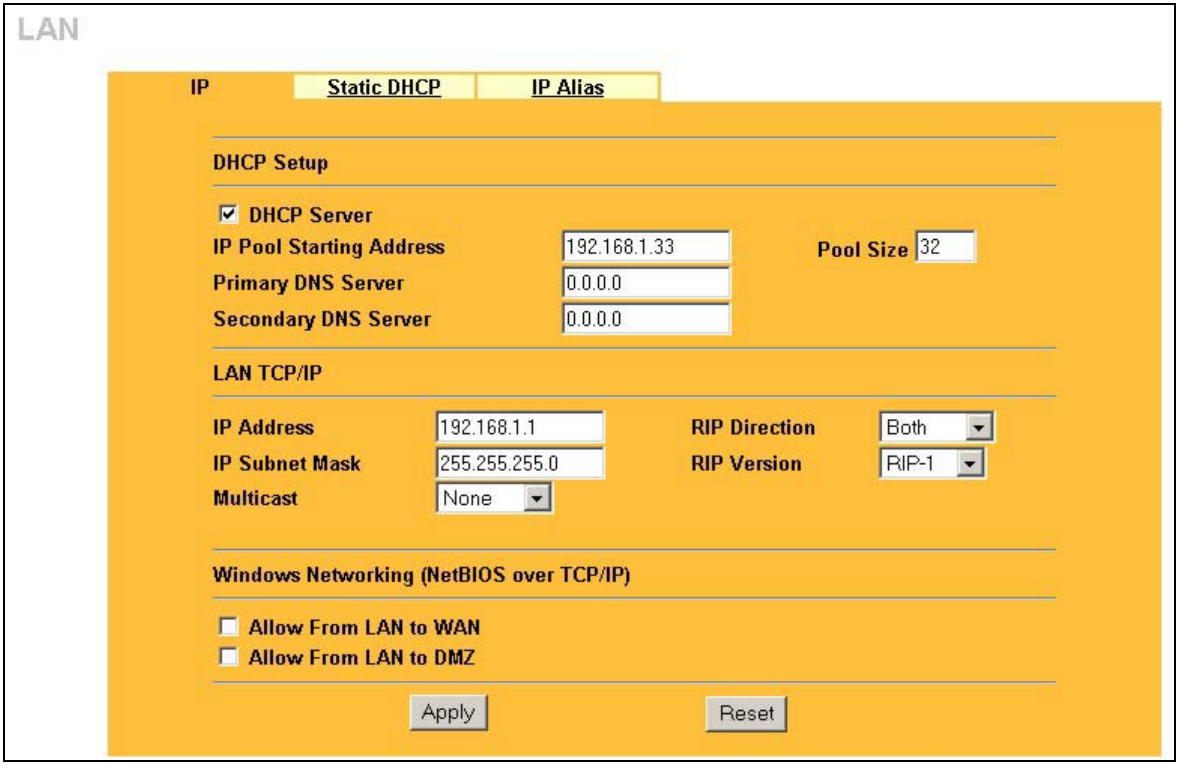


Figure 5-1 IP

The following table describes the fields in this screen.

Table 5-1 IP

LABEL	DESCRIPTION
DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave the **DHCP Server** check box selected. Clear it to disable the ZyWALL acting as a DHCP server. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the workstation must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask. Leave these entries at 0.0.0.0 if they are provided by a WAN DHCP server.
LAN TCP/IP	
IP Address	Type the IP address of your ZyWALL in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. **Both** is the default.

Table 5-1 IP

LABEL	DESCRIPTION
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow From LAN to WAN	Select this option to forward NetBIOS packets from the LAN port to the WAN port.
Allow From LAN to DMZ	Select this option to forward NetBIOS packets from the LAN port to the DMZ port. (Not all ZyWALL models have a DMZ port.)
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

5.5 Configuring Static DHCP

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

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

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

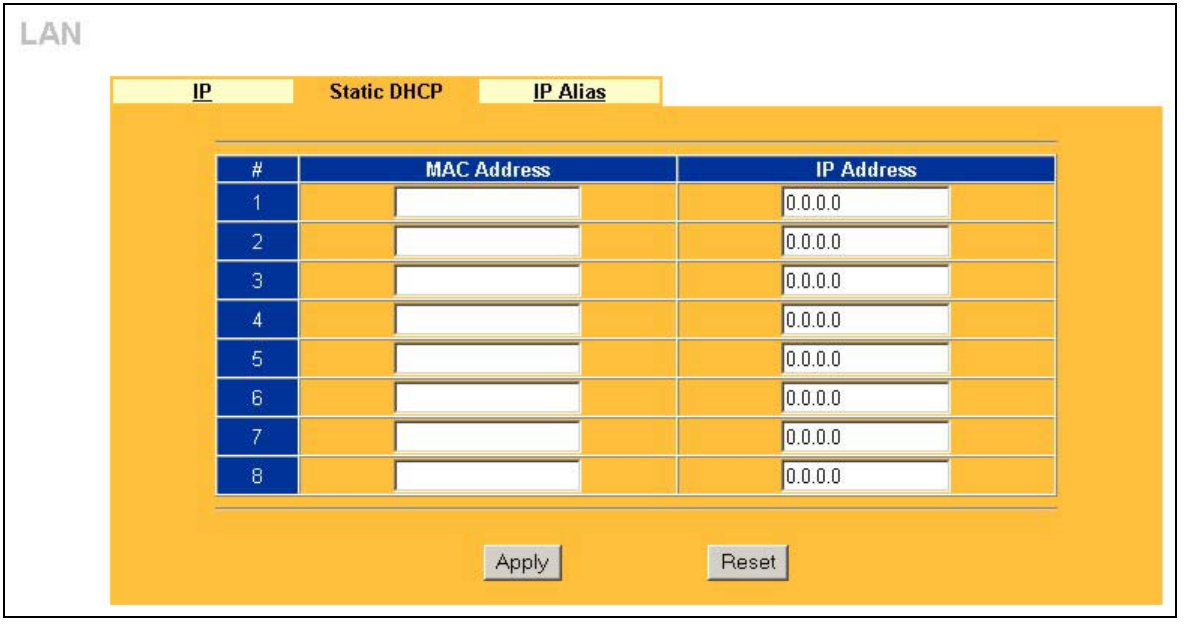


Figure 5-2 Static DHCP

The following table describes the fields in this screen.

Table 5-2 Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	This field specifies the size, or count of the IP address pool.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

5.6 Configuring IP Alias

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

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

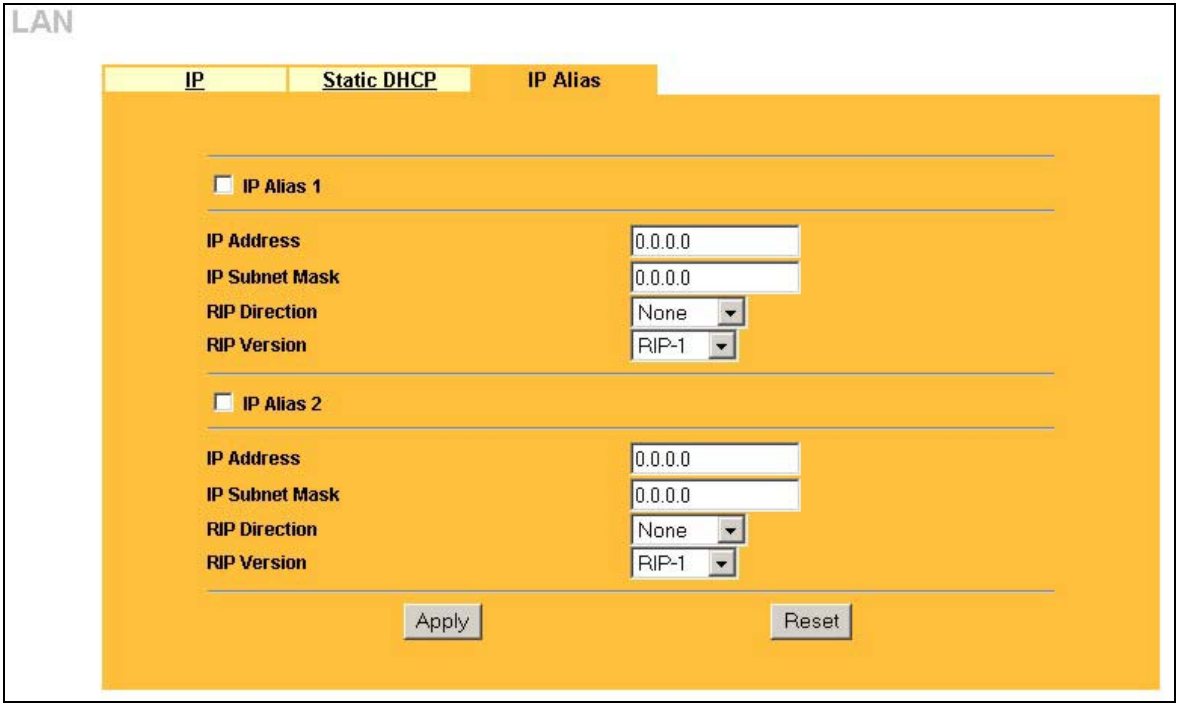


Figure 5-3 IP Alias

The following table describes the fields in this screen.

Table 5-3 IP Alias

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the ZyWALL.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.

Table 5-3 IP Alias

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

Chapter 6
Wireless LAN Screens

This chapter discusses how to configure Wireless LAN on the ZyWALL 10W, 30W and 100 models.

6.1 Wireless LAN Overview

This section introduces the wireless LAN (WLAN) and some basic scenarios.

6.1.1 Additional Installation Requirements for Using 802.1x

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

6.2 Wireless LAN Basics

This section provides background information on WLAN.

6.2.1 Channel

IEEE 802.11b wireless devices use ranges of radio frequencies called channels. Choose the radio channel depending on your geographical area. Adjacent Access Points (APs) should use different channels to reduce crosstalk. Crosstalk occurs when radio signals from access points overlap and cause interference that degrades performance.

6.2.2 ESS ID

Extended Service Set (ESS) is defined as one or more APs acting as a bridge between a wired LAN and the associated wireless clients. The ESS ID is a unique ID given to the APs and the wireless clients that participate in the same wireless network. You can think of the ESS ID as being similar to a workgroup name in a Microsoft network.

6.2.3 RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the

access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

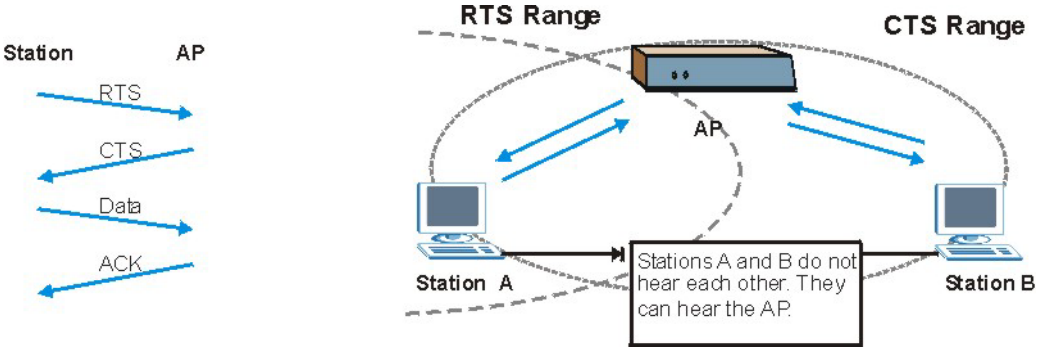


Figure 6-1 RTS Threshold

When station A sends data to the ZyWALL, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

6.2.4 Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the ZyWALL will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS Threshold** size.

6.3 Wireless Security

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

The figure below shows the possible wireless security levels on your ZyWALL. The highest security level is EAP (Extensible Authentication Protocol) authentication. It requires interaction with a RADIUS (Remote Authentication Dial In User Service) server either on the WAN or your LAN to provide authentication service for wireless clients.

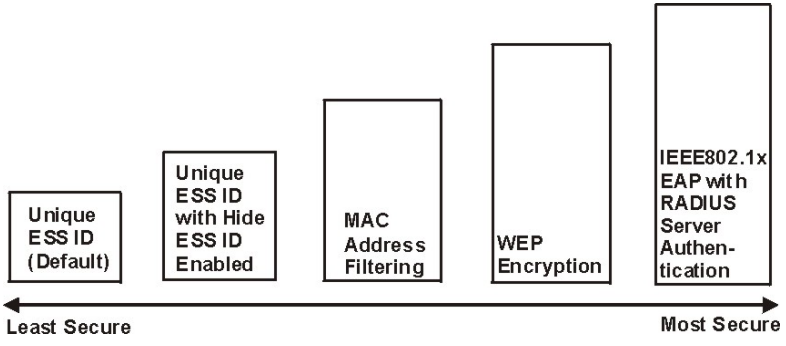


Figure 6-2 ZyWALL Wireless Security Levels

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

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

6.3.1 WEP

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

6.4 Configuring Wireless LAN

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

Click **WIRELESS LAN** to open the **Wireless** screen.

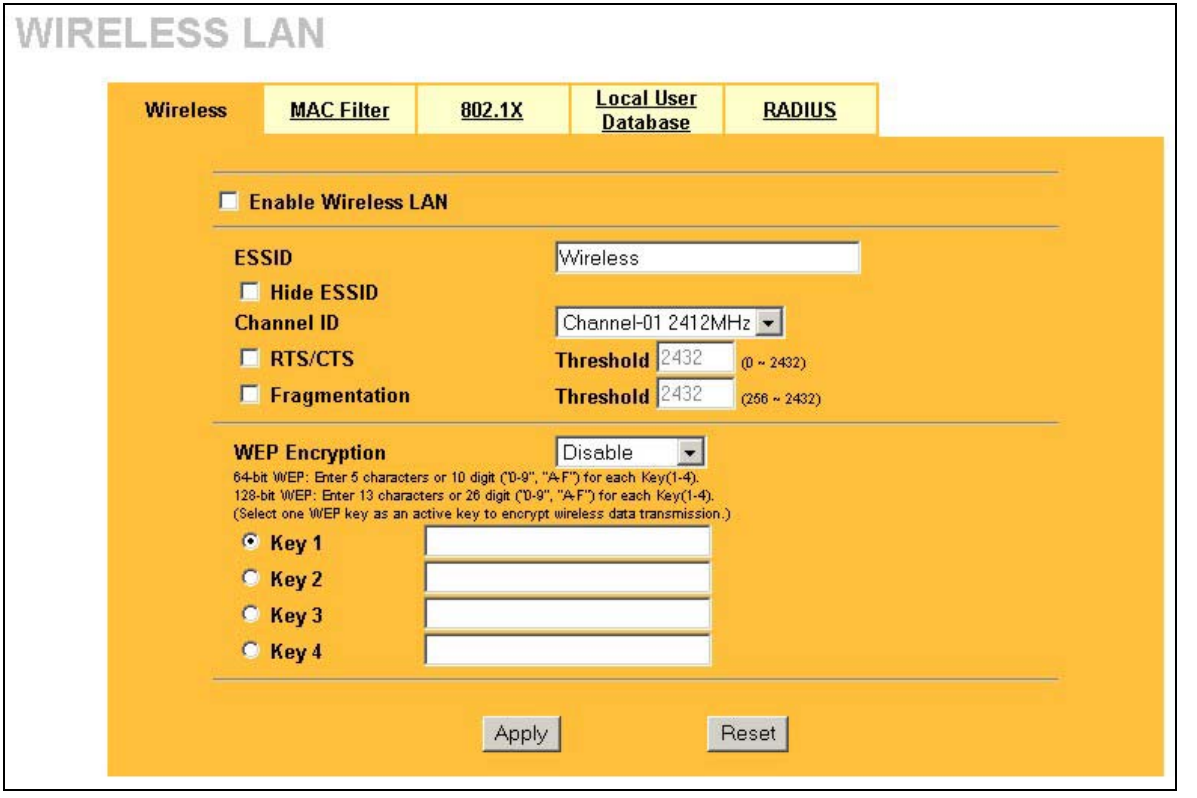


Figure 6-3 Wireless

The following table describes the fields in this screen.

Table 6-1 Wireless

LABEL	DESCRIPTION
Enable Wireless LAN	The wireless LAN is turned off (**No**) by default, before you enable the wireless LAN you should configure some security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN.
ESSID	(Extended Service Set IDentification) The ESSID identifies the Service Set the station is to connect to. Wireless clients associating to the Access Point must have the same ESSID. Enter a descriptive name (up to 32 characters) for the wireless LAN.
Hide ESSID	Select **Yes** to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.
Channel ID	This allows you to set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. CH01 2412 MHz / CH02 2417 MHz ~ CH11 2462 MHz (North America/FCC) CH01 2412 MHz / CH02 2417 MHz ~ CH13 2472 MHz (Europe CE/ ETSI) CH01 2412 MHz / CH02 2417 MHz ~ Ch14 2484 MHz (Japan) CH10 2457 MHz / CH11 2462 MHz (Spain) CH10 2457 MHz / CH11 2462 MHz ~ CH13 2472 MHz (France)
RTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **0** and **2432**.
Frag. Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **256** and **2432**.
WEP	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **Disable** to allow wireless clients to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Although WEP is functional at 5.5 and 11 Mbps, there is significant performance degradation when using WEP at these rates.

Table 6-1 Wireless

LABEL	DESCRIPTION
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless client computers.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.5 Configuring MAC Filter

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

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

.

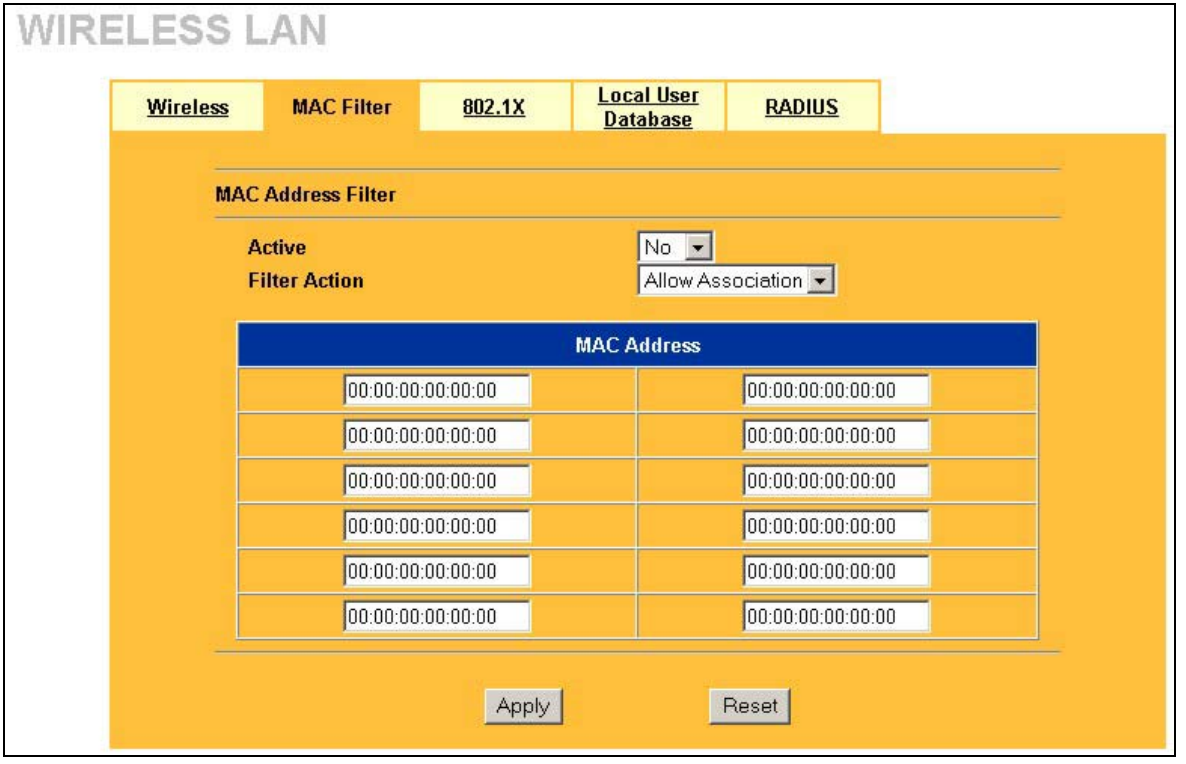


Figure 6-4 MAC Address Filter

The following table describes the fields in this menu.

Table 6-2 MAC Address Filter

LABEL	DESCRIPTION
Active	Use the drop down list box to enable or disable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the router.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyWALL in these address fields.

Table 6-2 MAC Address Filter

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.6 802.1x Overview

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

6.7 RADIUS

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

- **Authentication**

  Determines the identity of the users.

- **Accounting**

  Keeps track of the client's network activity.

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

Types of RADIUS Messages

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

- **Access-Request**

  Sent by an access point requesting authentication.

- **Access-Reject**

  Sent by a RADIUS server rejecting access.

- **Access-Accept**

  Sent by a RADIUS server allowing access.

- **Access-Challenge**

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

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

- **Accounting-Request**

  Sent by the access point requesting accounting.

- **Accounting-Response**

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

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

6.7.1 EAP Authentication Overview

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

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

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

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

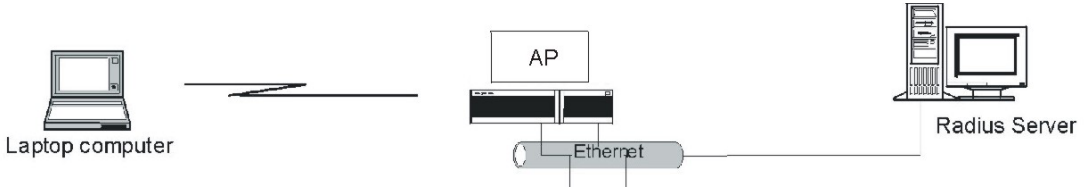


Figure 6-5 EAP Authentication

The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x chapter in the *Reference Guide*.

- The wireless station sends a “start” message to the ZyWALL.
- The ZyWALL sends a “request identity” message to the wireless station for identity information.

- The wireless station replies with identity information, including username and password.
- The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

6.8 Local User Database

By storing user profiles locally on the ZyWALL, your ZyWALL is able to authenticate wireless users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

6.9 Configuring 802.1X

To change your ZyWALL's Authentication settings, click **WIRELESS LAN**, then the **802.1X** tab. The screen appears as shown.

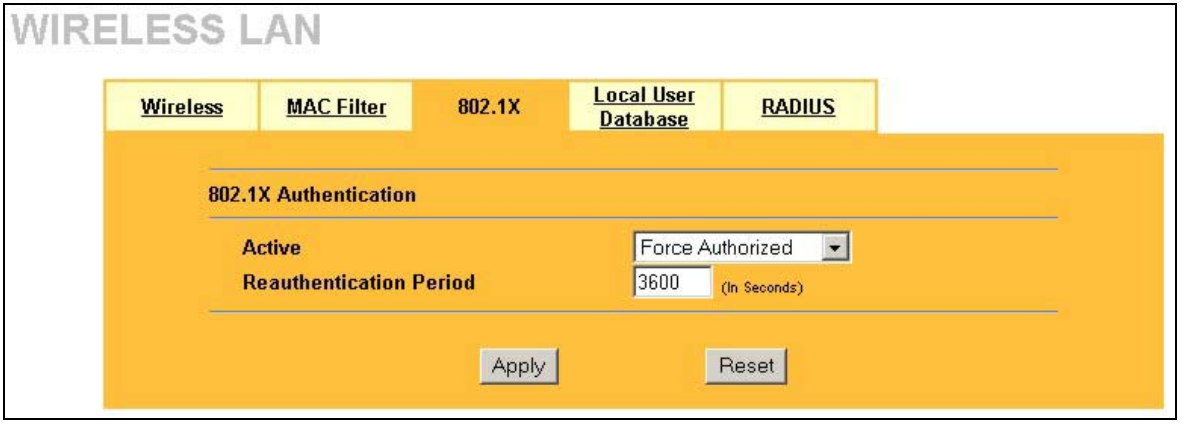


Figure 6-6 802.1X Authentication

The following table describes the fields in this screen.

Table 6-3 802.1X Authentication

LABEL	DESCRIPTION
Active	Select **Force Authorized**, **Force UnAuthorized** or **Auto** from the drop-down list box. Select **Auto** to authenticate all wireless clients before they can access the wired network. Select **Force Authorized** to allow all wireless clients to access your wired network without authentication. Select **Force UnAuthorized** to deny all wireless clients access to your wired network.
Reauthentication Period	Specify the time interval between the RADIUS server's authentication checks of wireless users connected to the network. This field is activated only when you select **Auto** authentication control.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.10 Configuring Local User Database

To change your ZyWALL's local user list, click **WIRELESS LAN**, then the **Local User Database** tab. The screen appears as shown (some of the screen's blank rows are not shown).

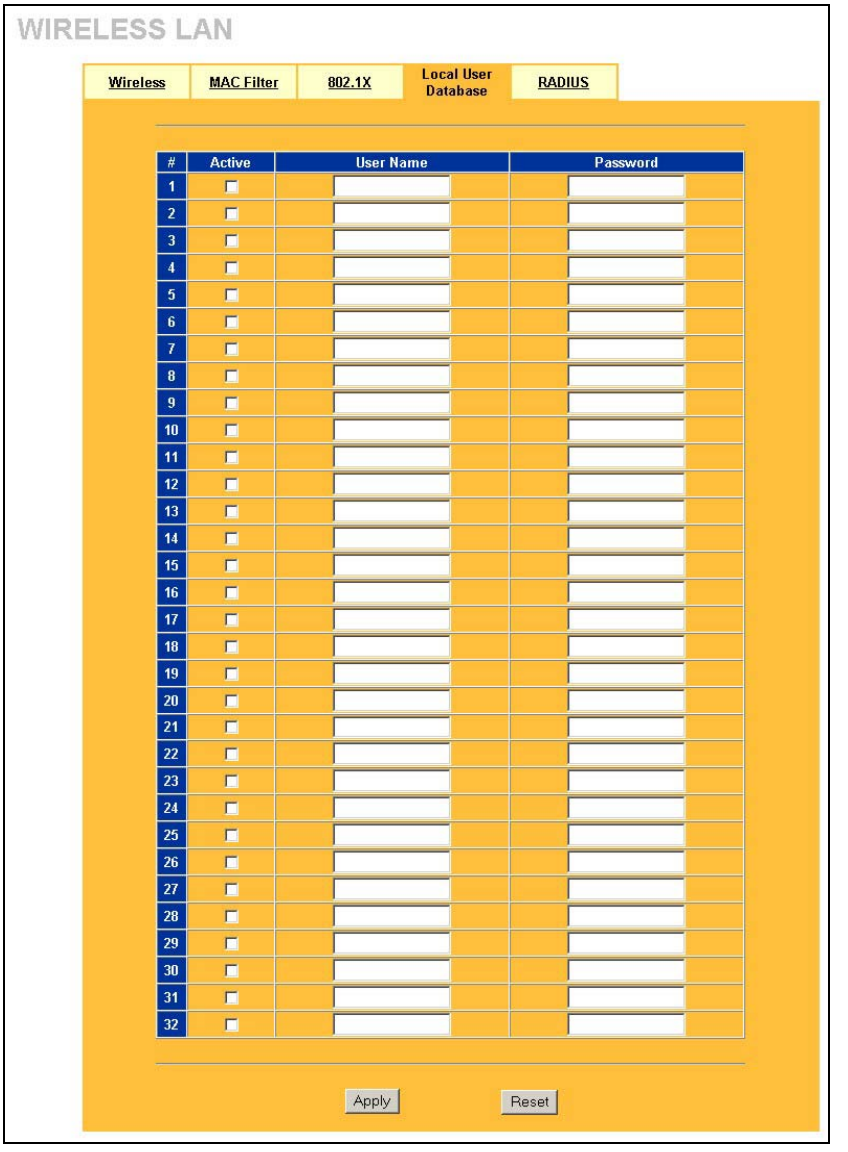


Figure 6-7 Local User Database

The following table describes the fields in this screen.

Table 6-4 Local User Database

LABEL	DESCRIPTION
Active	Select this check box to enable the user profile.
User Name	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.11 Configuring RADIUS

Use RADIUS if you want to authenticate wireless users using an external server.

To set up your ZyWALL's RADIUS Server settings, click **WIRELESS LAN**, then the **RADIUS** tab. The screen appears as shown.

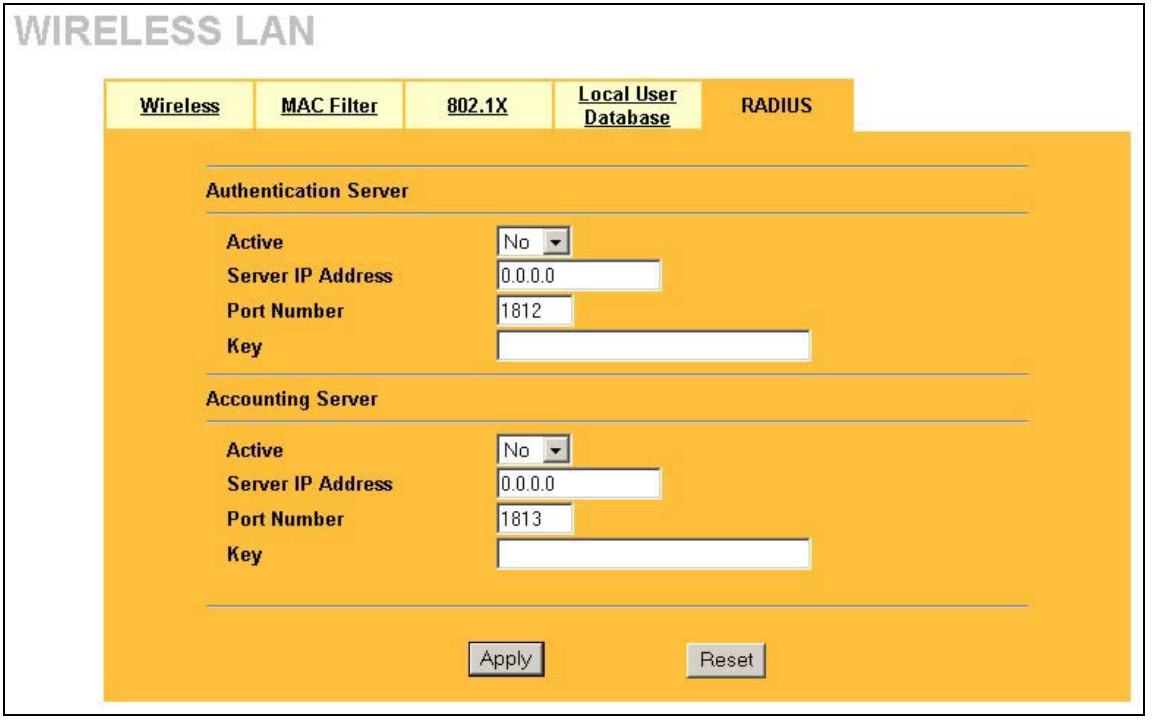


Figure 6-8 RADIUS

The following table describes the fields in this screen.

Table 6-5 RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select **Yes** from the drop-down list box to enable user authentication through an external authentication server. Select **No** to enable user authentication using the local user profile on the ZyWALL.
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	The default port of the RADIUS server for authentication is **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 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and ZyWALL.
Accounting Server	
Active	Select **Yes** from the drop-down list box to enable user authentication through an external accounting server.
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and ZyWALL.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

Part III:

DMZ and WAN

This part covers configuration of the DMZ and WAN screens.

Chapter 7
DMZ Screens

This chapter describes how to configure the ZyWALL 100's DMZ.

7.1 DMZ Overview

The DeMilitarized Zone (DMZ) auto-negotiating 10/100 Mbps Ethernet port provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

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

It is highly recommended that you connect all of your public servers to the DMZ port. If you have more than one public server, connect a hub to the DMZ port.

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

7.2 Configuring DMZ

From the **MAIN MENU**, click **DMZ**. The screen appears as shown next.

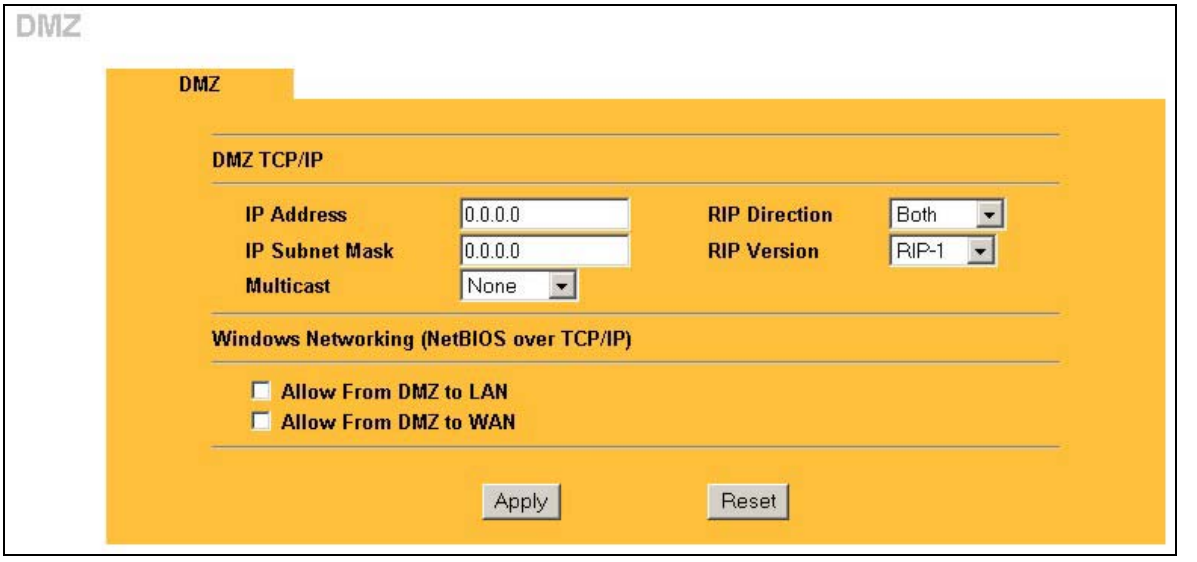


Figure 7-1 DMZ

The following table describes the fields in this screen.

Table 7-1 DMZ

LABEL	DESCRIPTION
DMZ TCP/IP	
IP Address	Type the IP address of your ZyWALL in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. Both is the default.

Table 7-1 DMZ

LABEL	DESCRIPTION
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*.
Windows Networking (NetBIOS over TCP/IP)	
Allow from DMZ to LAN	Click this option to forward NetBIOS packets from the DMZ port to the LAN port.
Allow from DMZ to WAN	Click this option to forward NetBIOS packets from the DMZ port to the WAN port.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 8
WAN Screens

This chapter describes how to configure WAN settings. Dial-backup applies to the ZyWALL 100, 30W and 10W (see Table 1-1 Model Specific Features). Traffic redirect applies to the ZyWALL 10W, 30W, 50 and 100 models.

8.1 WAN Overview

See the *Wizard Setup* chapter for more information on the fields in the WAN screens.

8.2 TCP/IP Priority (Metric)

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

The metric sets the priority for the ZyWALL's routes to the Internet. If any two of the default routes have the same metric, the ZyWALL uses the following pre-defined priorities:

1. Normal route: designated by the ISP (see *section 8.5*) or a static route (see the IP Static Route Setup chapter)
2. Traffic-redirect route (see *section 8.8*)
3. Dial-backup route (see *section 8.9*)

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

If you want the dial-backup route to take first priority over the traffic-redirect route or even the normal route, all you need to do is set the dial-backup route's metric to "1" and the others to "2" (or greater).

8.3 Configuring Route

Click **WAN** to open the **Route** screen.

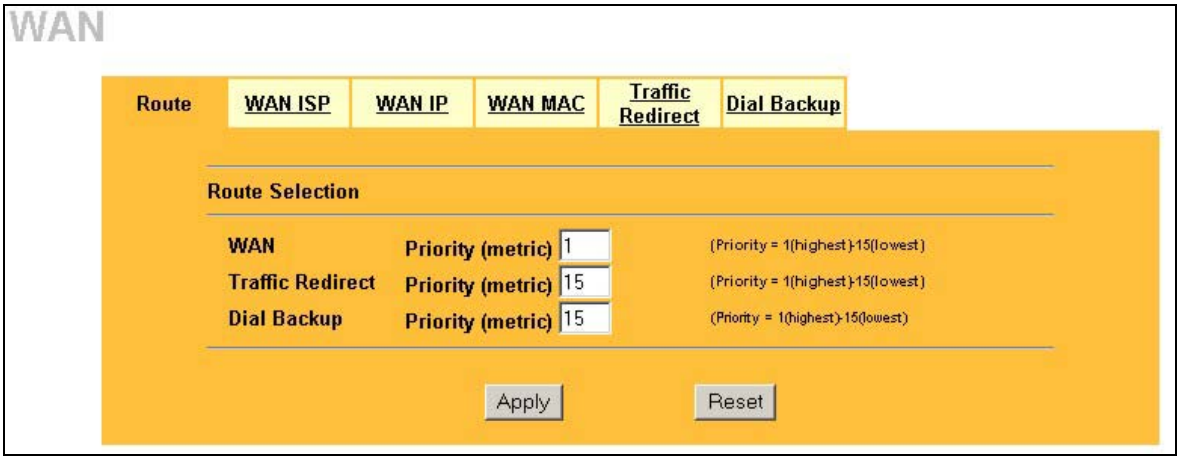


Figure 8-1 WAN Setup: Route

The following table describes the fields in this screen.

Table 8-1 WAN Setup: Route

LABEL	DESCRIPTION
WAN Traffic Redirect Dial Backup	The default WAN connection is "1' as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is **WAN**, **Traffic Redirect** and then **Dial Backup** (dial backup does not apply to all ZyWALL models): You have two choices for an auxiliary connection in the event that your regular WAN connection goes down. If **Dial Backup** is preferred to **Traffic Redirect**, then type "14" in the **Dial Backup Priority (metric)** field (and leave the **Traffic Redirect Priority (metric)** at the default of "15").
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4 Configuring WAN ISP

To change your ZyWALL's WAN ISP settings, click **WAN**, then the **WAN ISP** tab. The screen differs by the encapsulation.

8.4.1 Ethernet Encapsulation

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

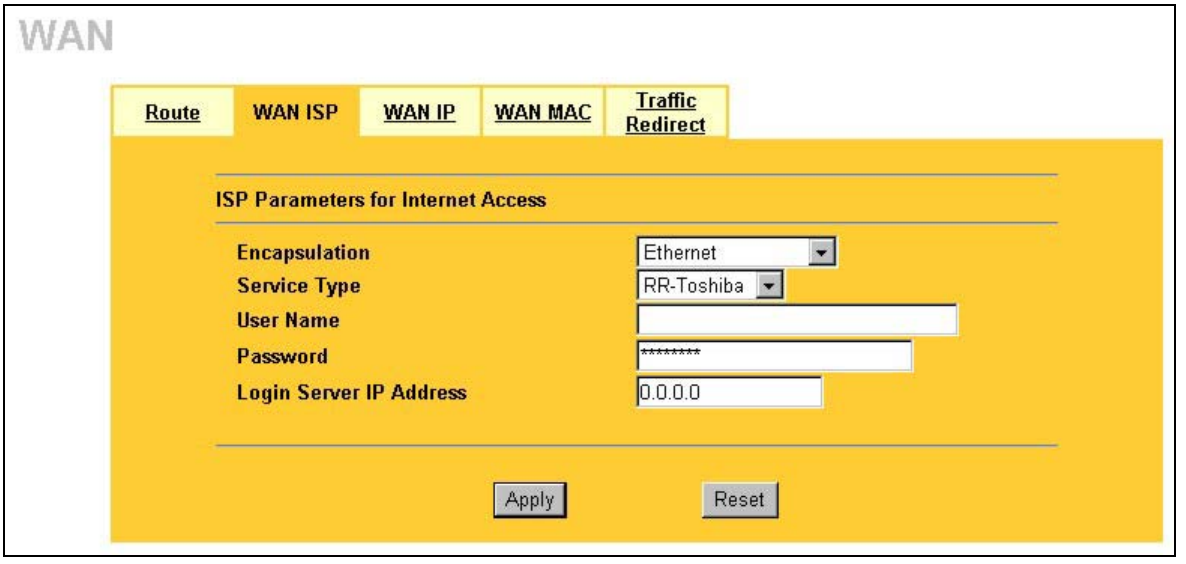


Figure 8-2 Ethernet Encapsulation

The following table describes the fields in this screen.

Table 8-2 Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from **Standard**, **Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**. The following fields do not appear with the **Standard** service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example “login1.telia.com”.

Table 8-2 Ethernet Encapsulation

LABEL	DESCRIPTION
Relogin Period (min) (Telia Login only)	The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyWALL to wait between logins.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.2 PPPoE Encapsulation

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

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

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

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

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

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

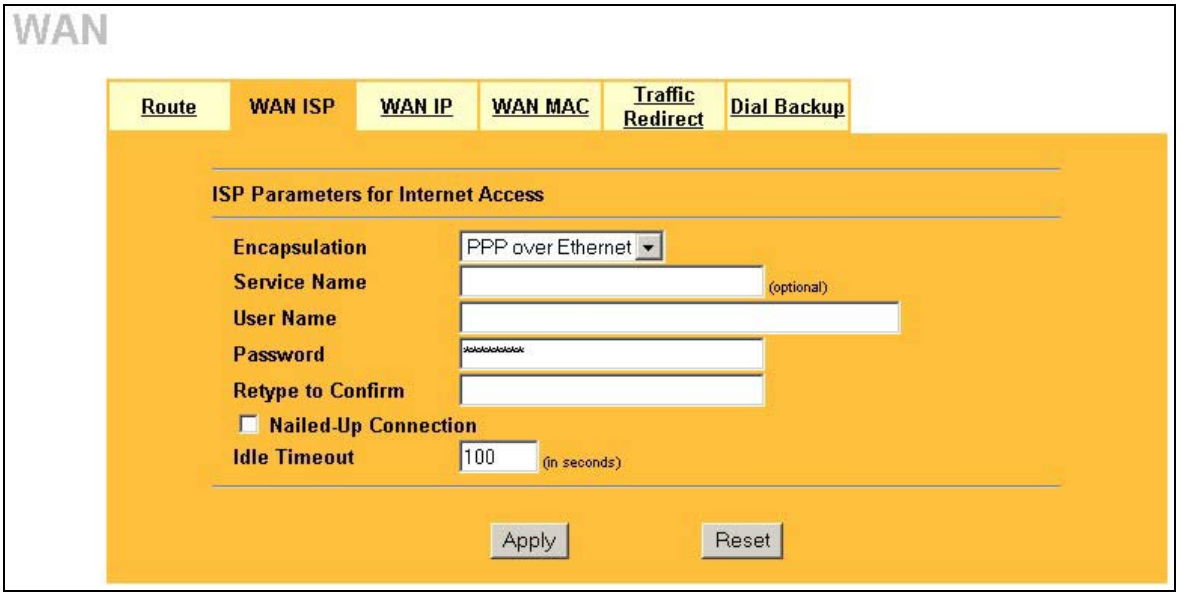


Figure 8-3 PPPoE Encapsulation

The following table describes the fields in this screen.

Table 8-3 PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the User Name given to you by your ISP.
Password	Type the password associated with the User Name above.

Table 8-3 PPPoE Encapsulation

LABEL	DESCRIPTION
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed Up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.3 PPTP Encapsulation

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

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

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

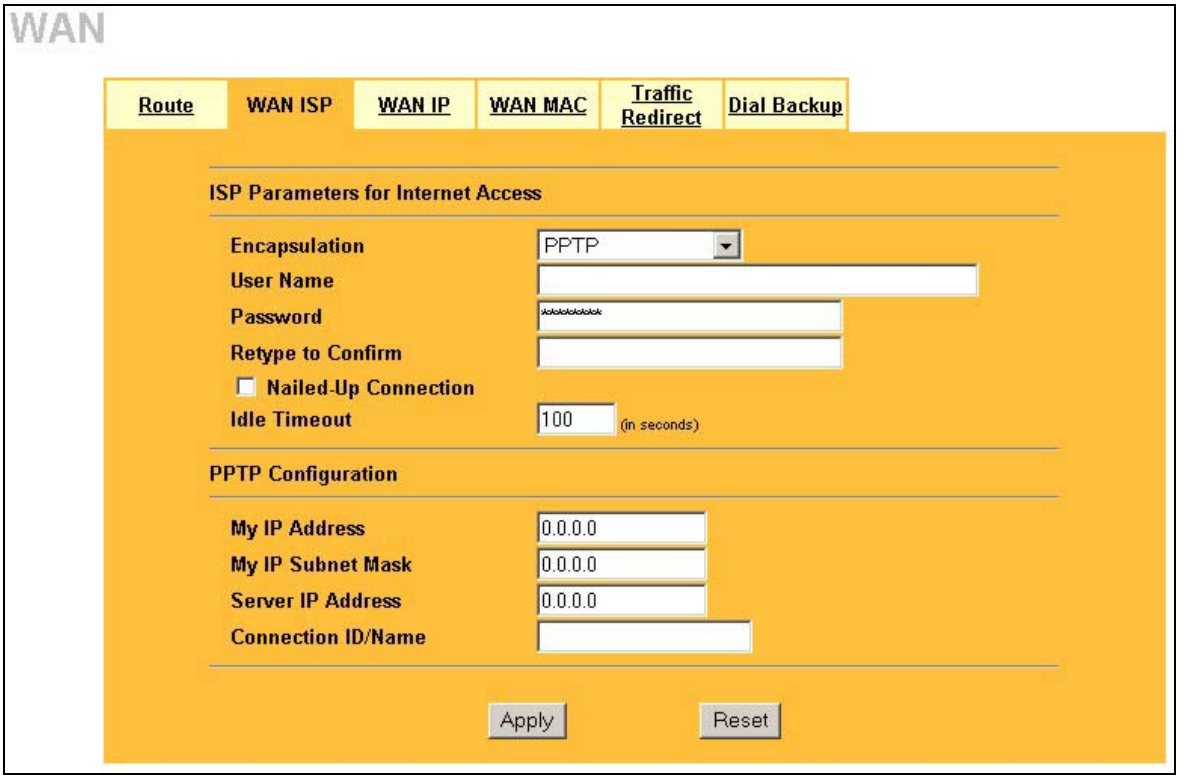


Figure 8-4 PPTP Encapsulation

The following table describes the fields in this screen.

Table 8-4 PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The ZyWALL supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the My Login and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the User Name given to you by your ISP.

Table 8-4 PPTP Encapsulation

LABEL	DESCRIPTION
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.4 Service Type

The screen shown next is for **RR- Service Type**.

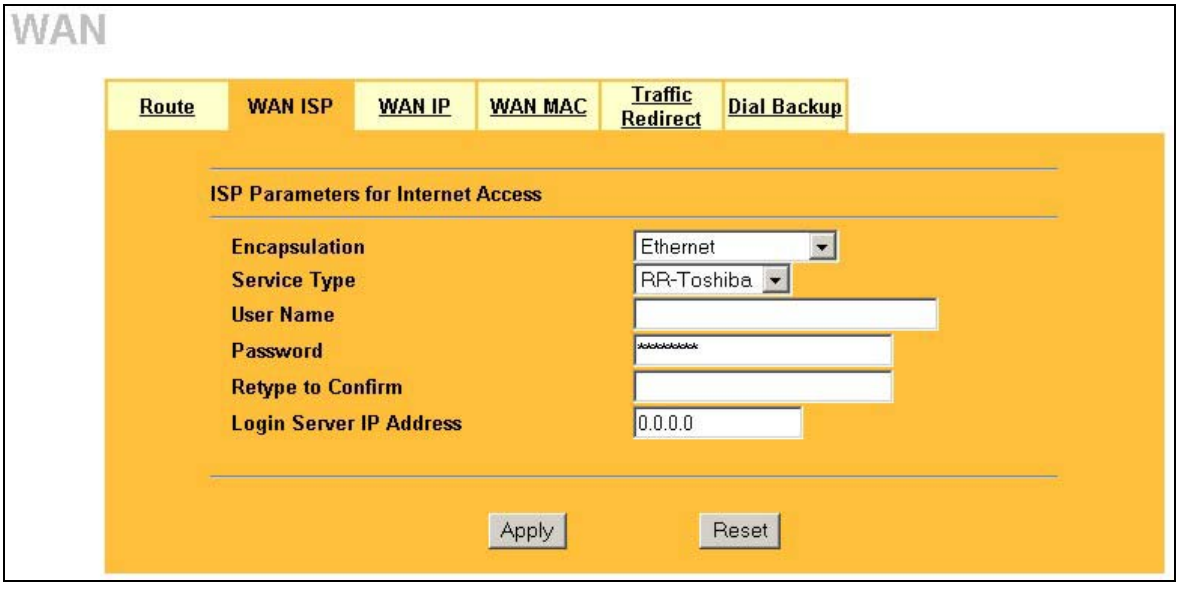


Figure 8-5 RR Service Type

The following table describes the fields in this screen.

Table 8-5 RR Service Type

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (Roadrunner Manager authentication method) or **RR-Telstra**. Choose a Roadrunner service type if your ISP is Time Warner's Roadrunner; otherwise choose **Standard**.
User Name	Enter the username given to you by your ISP.
Password	Enter the password associated with the login name above.
Login Server IP Address	The ZyWALL will find the Roadrunner Server IP address if this field is left blank. If it does not, then you must enter the authentication server IP address.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.5 Configuring WAN IP

To change your ZyWALL's WAN IP settings, click **WAN**, then the **WAN IP** tab. This screen varies according to the type of encapsulation you select.

If your ISP did *not* assign you a fixed IP address, click **Get automatically from ISP (Default)**;otherwise click **Use fixed IP Address** and enter the IP address in the following field.

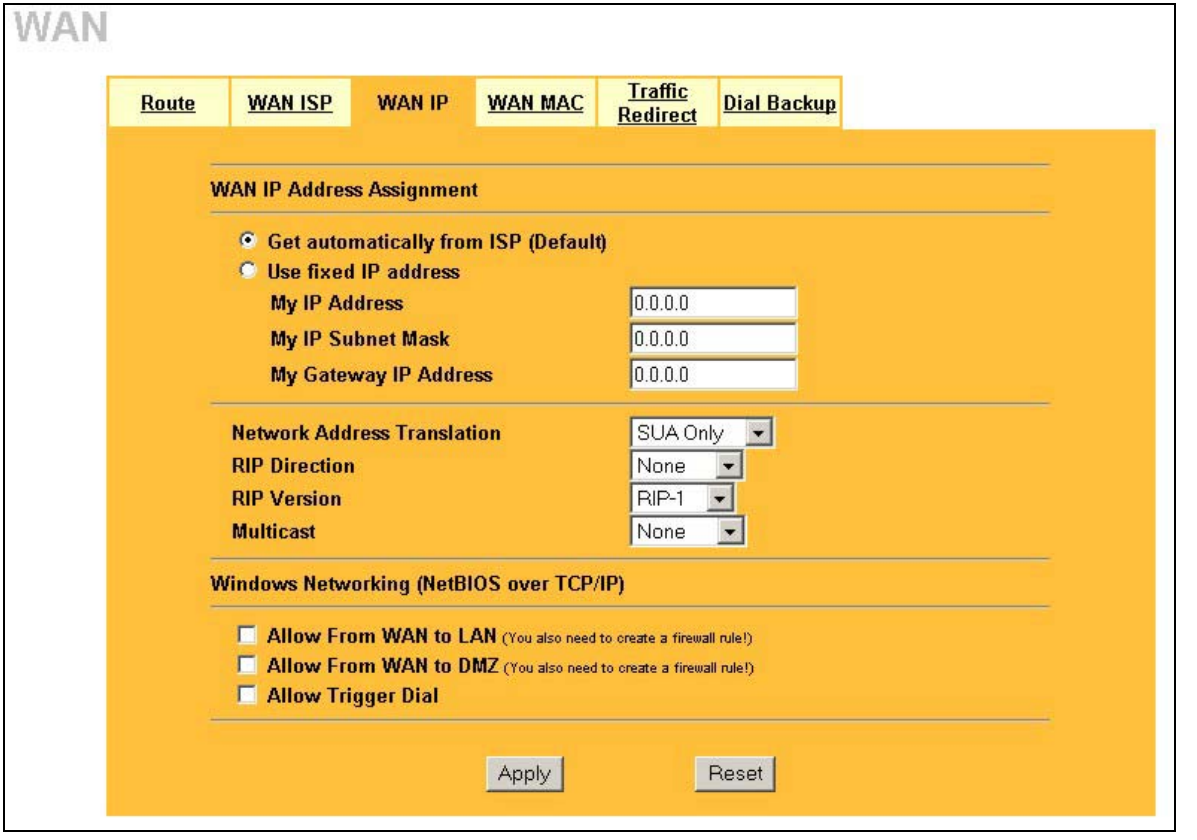


Figure 8-6 IP Setup

The following table describes the fields in this screen.

Table 8-6 IP Setup

LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
IP Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT**.** Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set! For more information about NAT refer to the *NAT* chapter in this *User's Guide*.
Metric (PPPoE and PPTP only)	This field sets this route's priority among the routes the ZyWALL uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Private (PPPoE and PPTP only)	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.

Table 8-6 IP Setup

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives. When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received. By default, **RIP Direction** is set to **Both**.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**.
Multicast	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.	
Allow From WAN to LAN	Select this option to forward NetBIOS packets from the WAN port to the LAN port.

Table 8-6 IP Setup

LABEL	DESCRIPTION
Allow From WAN to DMZ	Select this option to forward NetBIOS packets from the WAN port to the DMZ port. (Not all ZyWALL models have a DMZ port.)
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.6 Configuring WAN MAC

To change your ZyWALL's WAN MAC settings, click **WAN**, then the **WAN MAC** tab. The screen appears as shown.

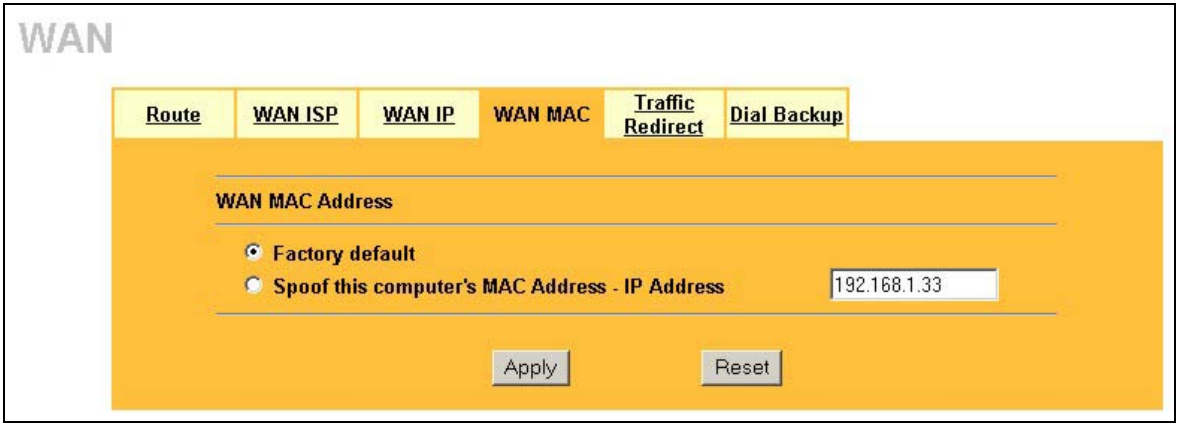


Figure 8-7 MAC Setup

The MAC address screen allows users to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Spoof this computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.

8.7 Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the ZyWALL cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyWALL still provides firewall protection. This feature is not available on all models.

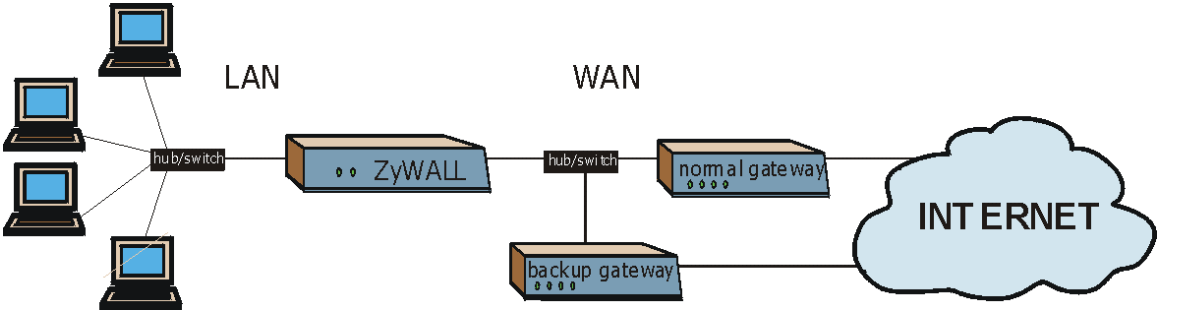


Figure 8-8 Traffic Redirect WAN Setup

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

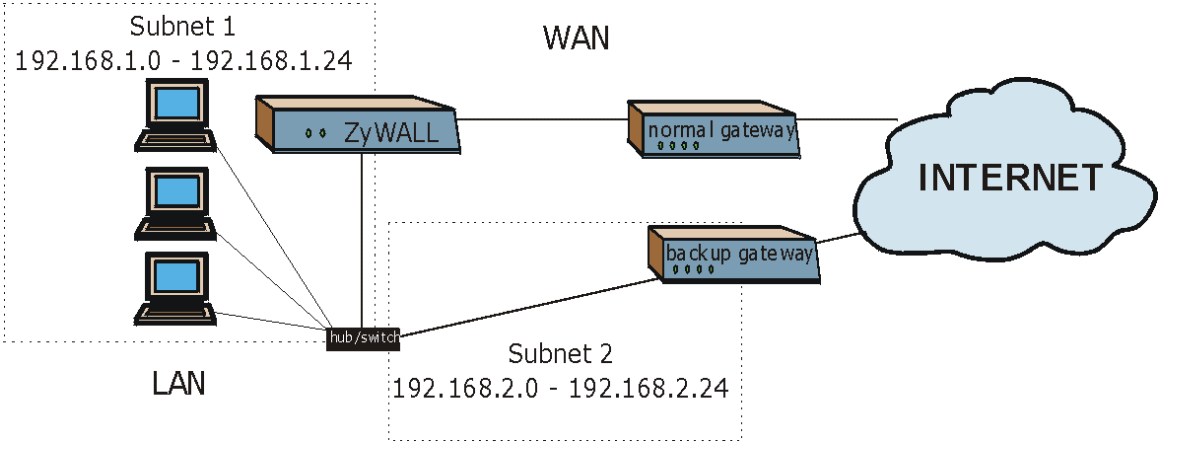


Figure 8-9 Traffic Redirect LAN Setup

8.8 Configuring Traffic Redirect

To change your ZyWALL's Traffic Redirect settings, click **WAN**, then the **Traffic Redirect** tab. The screen appears as shown.

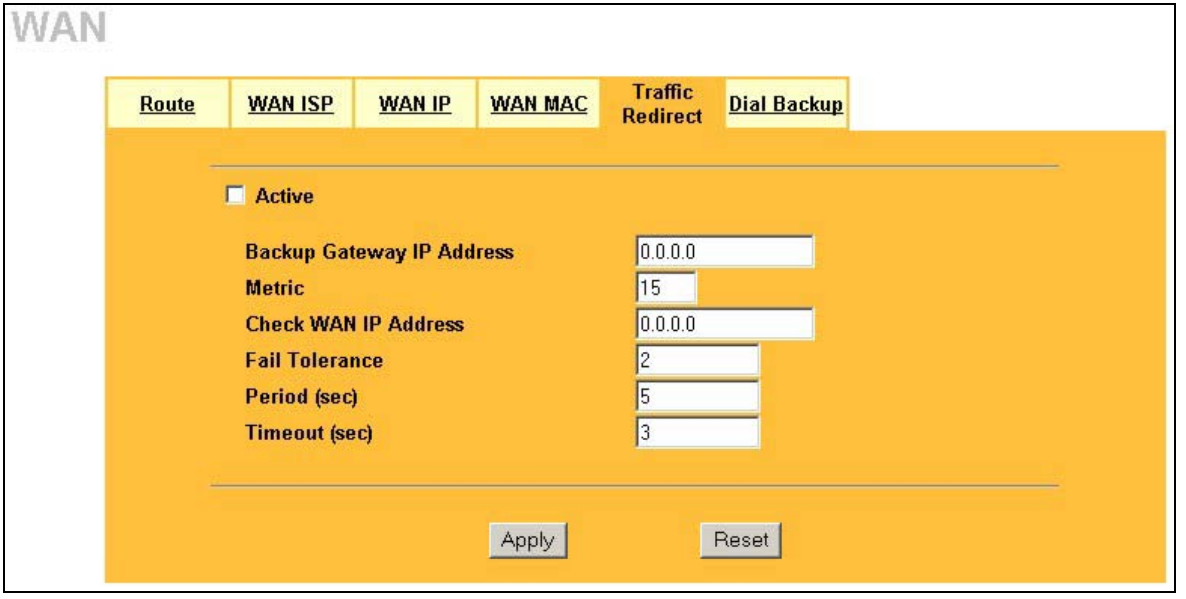


Figure 8-10 Traffic Redirect

The following table describes the fields in this screen.

Table 8-7 Traffic Redirect

LABEL	DESCRIPTION
Active	Select this check box to have the ZyWALL use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates.
Metric	This field sets this route's priority among the routes the ZyWALL uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

Table 8-7 Traffic Redirect

LABEL	DESCRIPTION
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the ZyWALL will use the default gateway IP address. Configure this field to test your ZyWALL's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you are using PPTP or PPPoE Encapsulation, type "0.0.0.0" to configure the ZyWALL to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Type the number of times your ZyWALL may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
Period (sec)	Type the number of seconds for the ZyWALL to wait between checks to see if it can connect to the WAN IP address (**Check WAN IP Address** field) or default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout (sec)	Type the number of seconds for your ZyWALL to wait for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The WAN connection is considered "down" after the ZyWALL times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.9 Configuring Dial Backup

To change your ZyWALL's Dial Backup settings, click **WAN**, then the **Dial Backup** tab. The screen appears as shown.

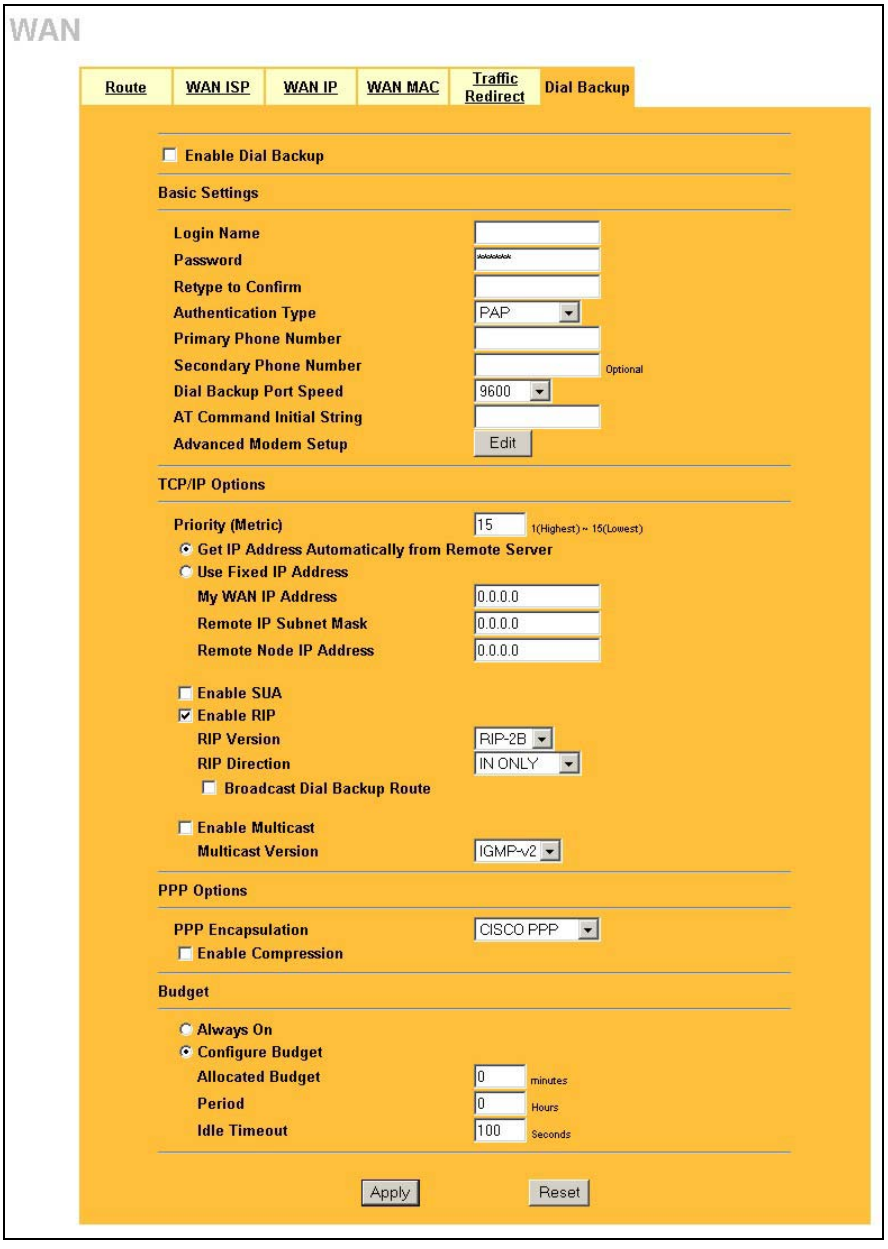


Figure 8-11 Dial Backup Setup

The following table describes the fields in this screen.

Table 8-8Dial Backup Setup

LABEL	DESCRIPTION
Enable Dial Backup	Select this check box to turn on dial backup.
Basic Settings	
Login Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your ZyWALL accepts CHAP only. **PAP** - Your ZyWALL accept PAP only.
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Dial Backup Port Speed	Use the drop-down list box to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Advanced Modem Setup	Click this button to display the **Advanced Setup** screen and edit the details of your dial backup setup.
TCP/IP Options	
Priority (Metric)	This field sets this route's priority among the three routes the ZyWALL uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority. If the three routes have the same metrics, the priority of the routes is as follows: **WAN**, **Traffic Redirect**, **Dial Backup**.

Table 8-8Dial Backup Setup

LABEL	DESCRIPTION
Get IP Address Automatically from Remote Server	Type the login name assigned by your ISP for this remote node.
Used Fixed IP Address	Select this check box if your ISP assigned you a fixed IP address, then enter the IP address in the following field.
ZyWALL WAN IP Address	Leave the field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Type your WAN IP address here if you know it (static). This is the address assigned to your local ZyWALL, not the remote router.
Remote IP Subnet Mask	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Type the remote gateway's subnet mask here if you know it (static).
Remote Node IP Address	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Type the remote gateway's IP address here if you know it (static).
ZyWALL Operating Mode	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network. Select **SUA Only** or **None**. **SUA** (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the ZyWALL will use Address Mapping Set 255 (see your *User's Guide* for more information). Select **None** to disable NAT.
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

Table 8-8Dial Backup Setup

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives.
Broadcast Dial Backup Route	Select this check box to forward the backup route broadcasts to the WAN.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*.
Budget	
Always On	Select this check box to have the dial backup connection on all of the time.
Configure Budget	Select this check box to have the dial backup connection on during the time that you select.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).
Idle Timeout	Type the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) for the ZyWALL to wait before it automatically disconnects the dial backup connection. This option applies only when the ZyWALL initiates the call. The dial backup connection never times out if you set this field to "0" (it is the same as selecting **Always On**).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.10 Advanced Modem Setup

8.10.1 AT Command Strings

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

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

8.10.2 DTR Signal

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

8.10.3 Response Strings

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

8.11 Configuring Advanced Modem Setup

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

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

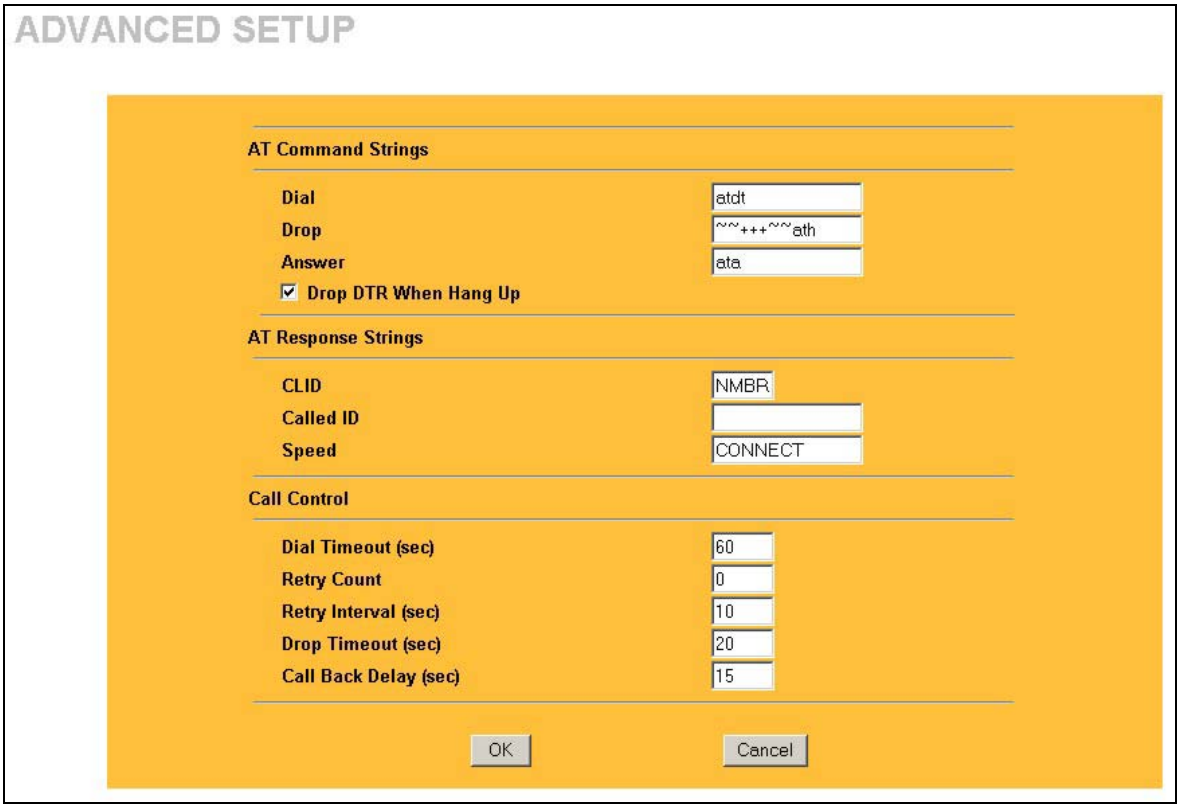


Figure 8-12 Advanced Setup

The following table describes the fields in this screen.

Table 8-9 Advanced Setup

LABEL	DESCRIPTION	EXAMPLE
AT Command Strings		
Dial	Type the AT Command string to make a call.	atdt
Drop	Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~~+++~~ath" can be used if your modem has a slow response time.	~~+++~~ath
Answer	Type the AT Command string to answer a call.	ata

Table 8-9 Advanced Setup

LABEL	DESCRIPTION	EXAMPLE
Drop DTR When Hang Up	Select this check box to have the ZyWALL drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out.	
AT Response Strings		
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyWALL capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR
Called ID	Type the keyword preceding the dialed number.	
Speed	Type the keyword preceding the connection speed.	CONNECT
Call Control		
Dial Timeout (sec)	Type a number of seconds for the ZyWALL to try to set up an outgoing call before timing out (stopping).	60
Retry Count	Type a number of times for the ZyWALL to retry a busy or no-answer phone number before blacklisting the number.	0
Retry Interval (sec)	Type a number of seconds for the ZyWALL to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	10
Drop Timeout (sec)	Type the number of seconds for the ZyWALL to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20
Call Back Delay (sec)	Type a number of seconds for the ZyWALL to wait between dropping a callback request call and dialing the corresponding callback call.	15
Apply	Click **Apply** to save your changes back to the ZyWALL.	
Reset	Click **Reset** to begin configuring this screen afresh.	

Part IV:

NAT and Static Route

This part covers Network Address Translation and setting up static routes.

Chapter 9
Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the ZyWALL.

9.1 NAT Overview

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

9.1.1 NAT Definitions

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

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

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

Table 9-1 NAT Definitions

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

NAT never changes the IP address (either local or global) of an outside **host.**

9.1.2 What NAT Does

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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyWALL filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

9.1.3 How NAT Works

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

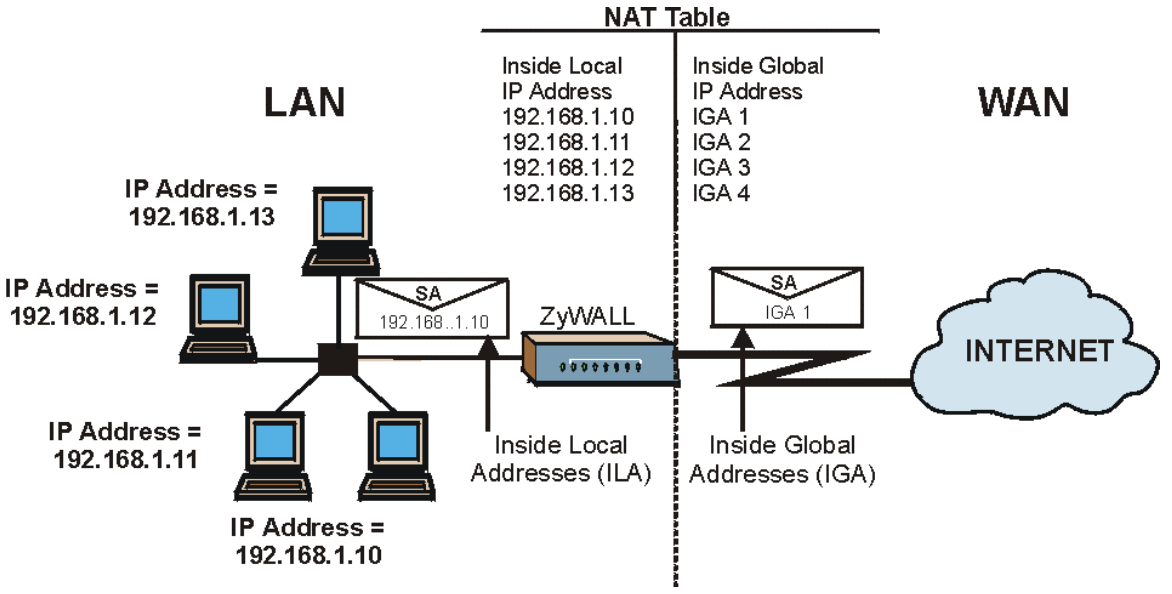


Figure 9-1 How NAT Works

9.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyWALL can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

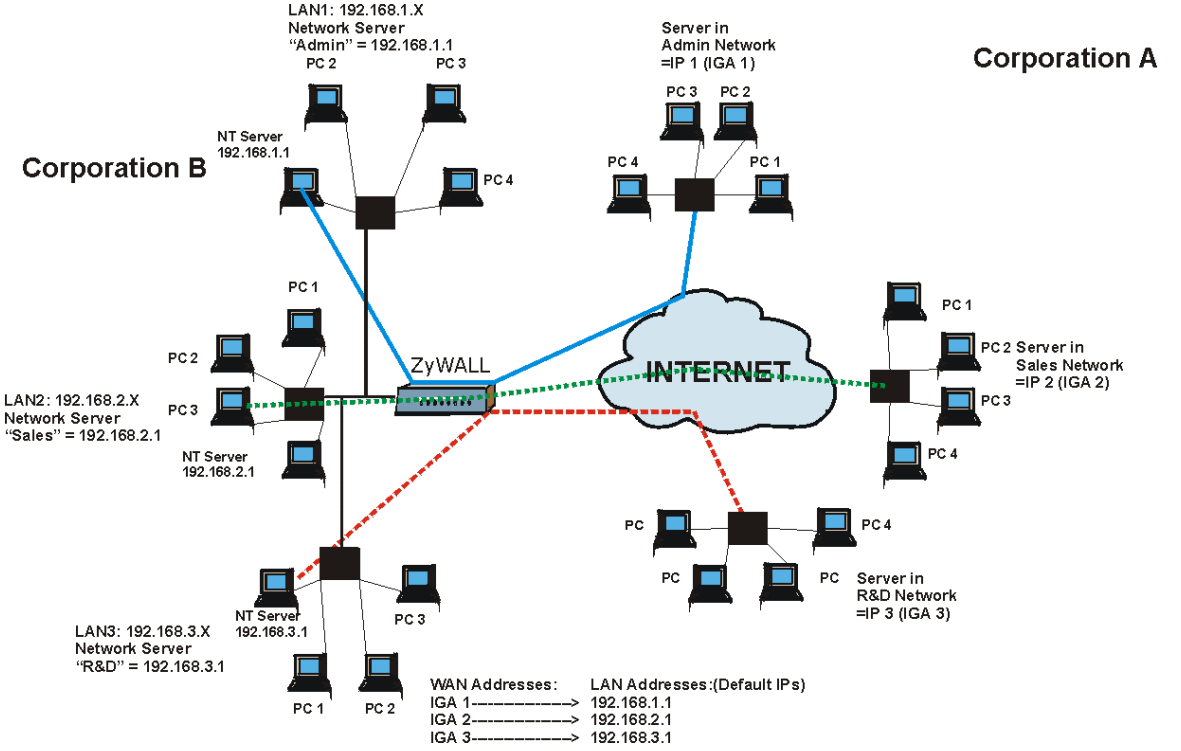


Figure 9-2 NAT Application With IP Alias

9.1.5 NAT Mapping Types

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

- **One to One**: In One-to-One mode, the ZyWALL maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyWALL maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the SUA Only option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyWALL maps the multiple local IP addresses to shared global IP addresses.

- **Many One to One**: In Many-One-to-One mode, the ZyWALL maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

Port numbers do not **change for** One-to-One **and** Many-One-to-One **NAT mapping types.**

The following table summarizes these types.

Table 9-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1-1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M-1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M-M Ov
Many-One-to-One	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M-1-1
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

9.2 Using NAT

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyWALL.

9.2.1 SUA (Single User Account) Versus NAT

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

9.3 SUA Server

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

If you do not assign a Default Server IP Address, then all packets received for ports not specified in this screen will be discarded.

9.3.1 Port Forwarding: Services and Port Numbers

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world. The ZyWALL 100 provides the additional safety of a DMZ port for connecting your publicly accessible servers. This makes the LAN more secure by physically separating it from your public servers.

Use the **SUA Server** page to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the

desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

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

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on SUA/NAT.

Table 9-3 Services and Port Numbers

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

9.3.2 Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35 as shown in the next figure.

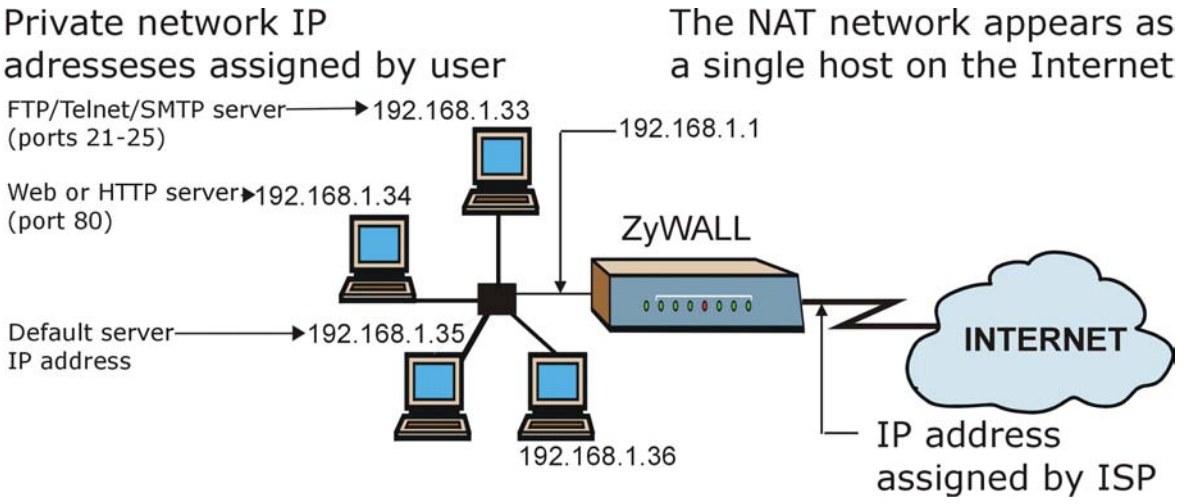


Figure 9-3 Multiple Servers Behind NAT Example

9.4 Configuring SUA Server

If you do not assign a Default Server **IP Address, then all packets received for ports not specified in this screen will be discarded.**

Click **SUA/NAT** to open the **SUA Server** screen.

Refer to the firewall chapters for port numbers commonly used for particular services.

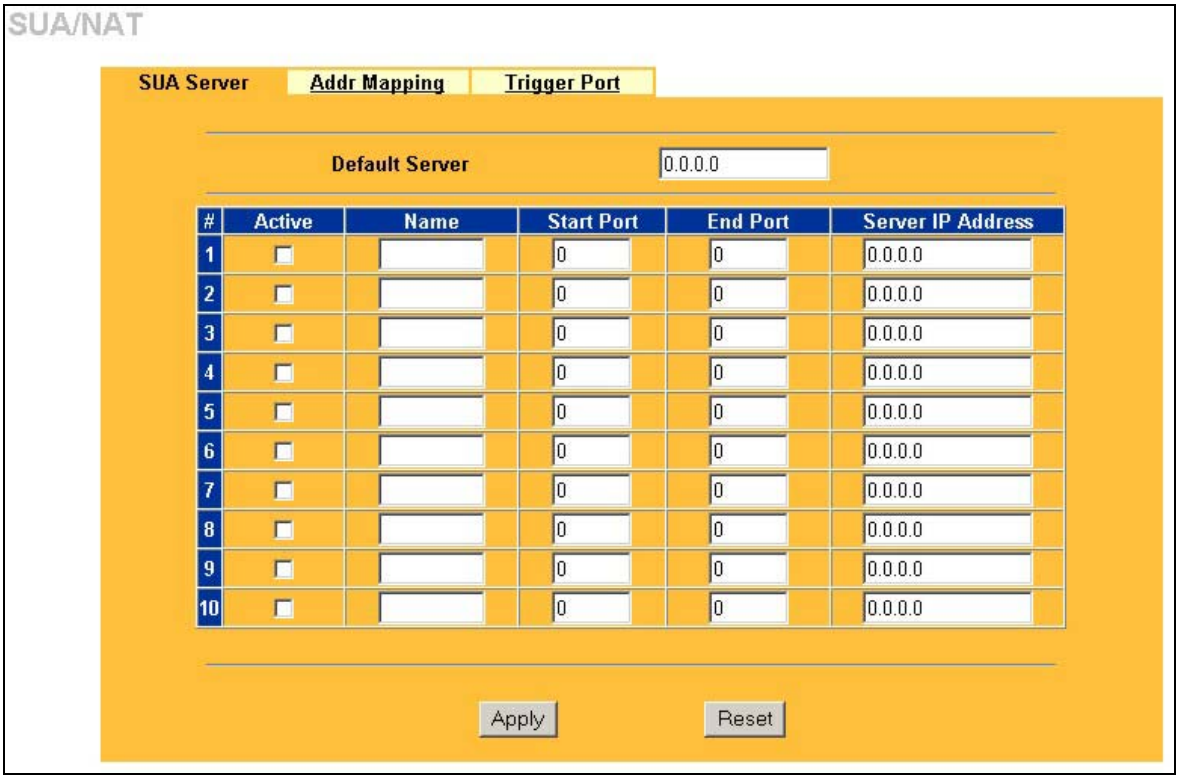


Figure 9-4 SUA/NAT Setup

The following table describes the fields in this screen.

Table 9-4 SUA/NAT Setup

LABEL	DESCRIPTION
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen will be discarded.
#	Number of an individual SUA server entry.
Active	Select this check box to enable the SUA server entry. Clear this checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.

Table 9-4 SUA/NAT Setup

LABEL	DESCRIPTION
Start Port	Enter a port number here. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field
End Port	
Server IP Address	Enter the inside IP address of the server here.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

9.5 Configuring Address Mapping

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

To change your ZyWALL's Address Mapping settings, click **SUA/NAT**, then the **Address Mapping** tab. The screen appears as shown.

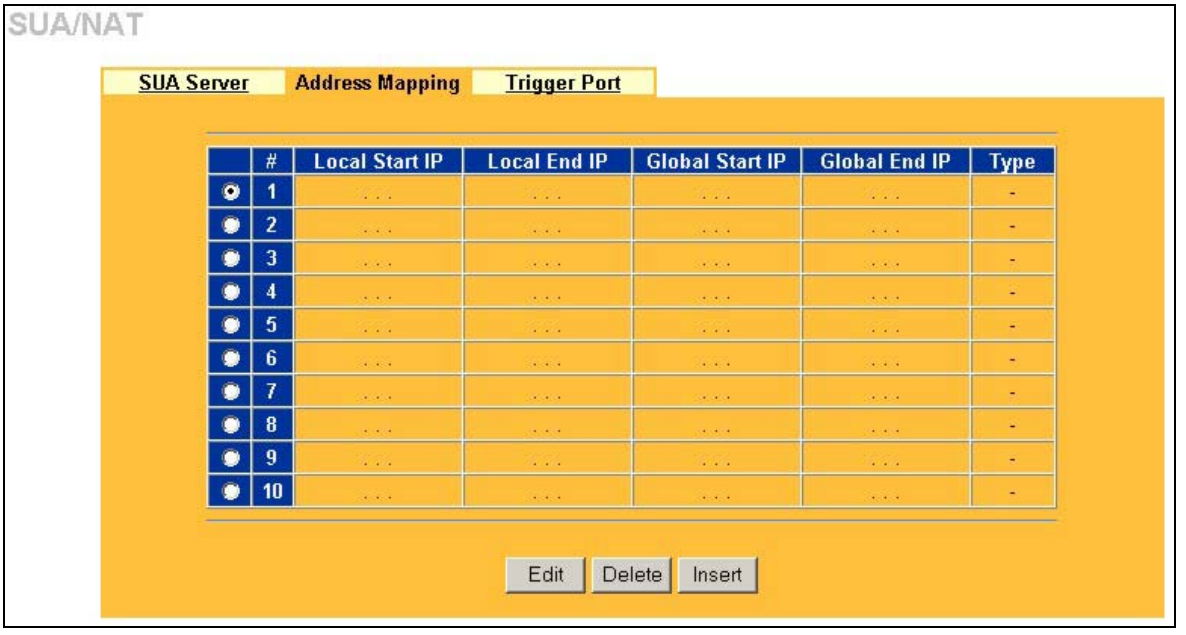


Figure 9-5 Address Mapping

The following table describes the fields in this screen.

Table 9-5 Address Mapping

LABEL	DESCRIPTION
Local Start IP	This refers to the Inside Local Address (ILA), that is the starting local IP address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global Address (IGA), that is the starting global IP address. This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.

Table 9-5 Address Mapping

LABEL	DESCRIPTION
Type	1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. 2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. 3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One** mode maps each local IP address to unique global IP addresses. 5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Edit	Click **Edit** to go to the **Address Mapping Rule** screen.
Delete	Click **Delete** to delete an address mapping rule.
Insert	Click **Insert** to insert a new mapping rule before an existing one.

Configuring Address Mapping

To edit an Address Mapping rule, click the **Edit** button to display the screen shown next.

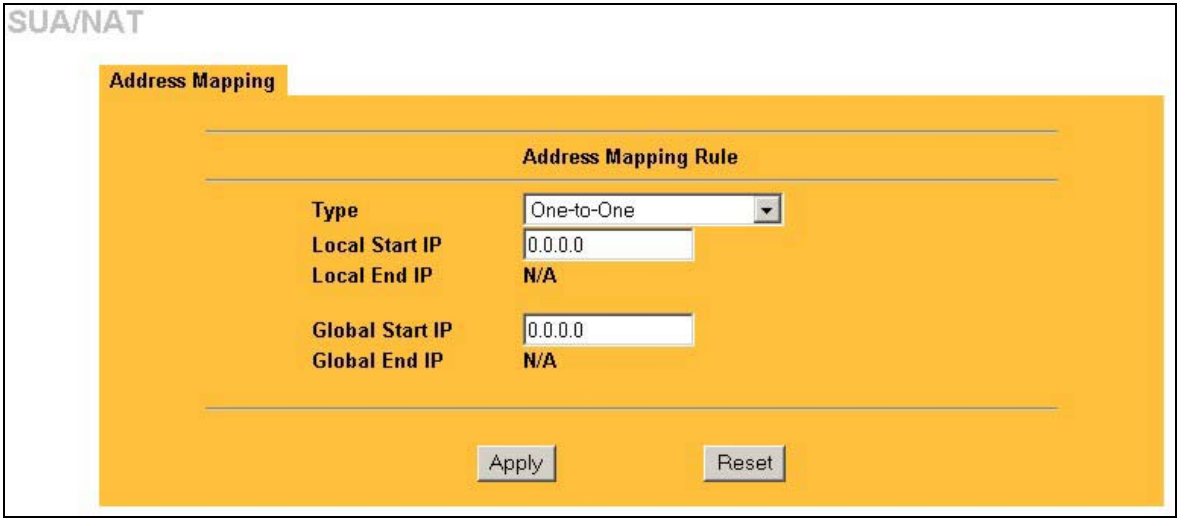


Figure 9-6Address Mapping Edit

The following table describes the fields in this screen.

Table 9-6 Address Mapping Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. 1. **One-to-One**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature. 3. **Many-to-Many Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One**: Many One-to-one mode maps each local IP address to unique global IP addresses. 5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

9.6 Configuring Trigger Port

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to

request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

1. Jane requests a file from the Real Audio server (port 7070).

2. Port 7070 is a "trigger" port and causes the ZyWALL to record Jane's computer IP address. The ZyWALL associates Jane's computer IP address with the "incoming" port range of 6970-7170.

3. The Real Audio server responds using a port number ranging between 6970-7170.

4. The ZyWALL forwards the traffic to Jane's computer IP address.

5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyWALL times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

To change your ZyWALL's trigger port settings, click **SUA/NAT** and the **Trigger Port** tab. The screen appears as shown.

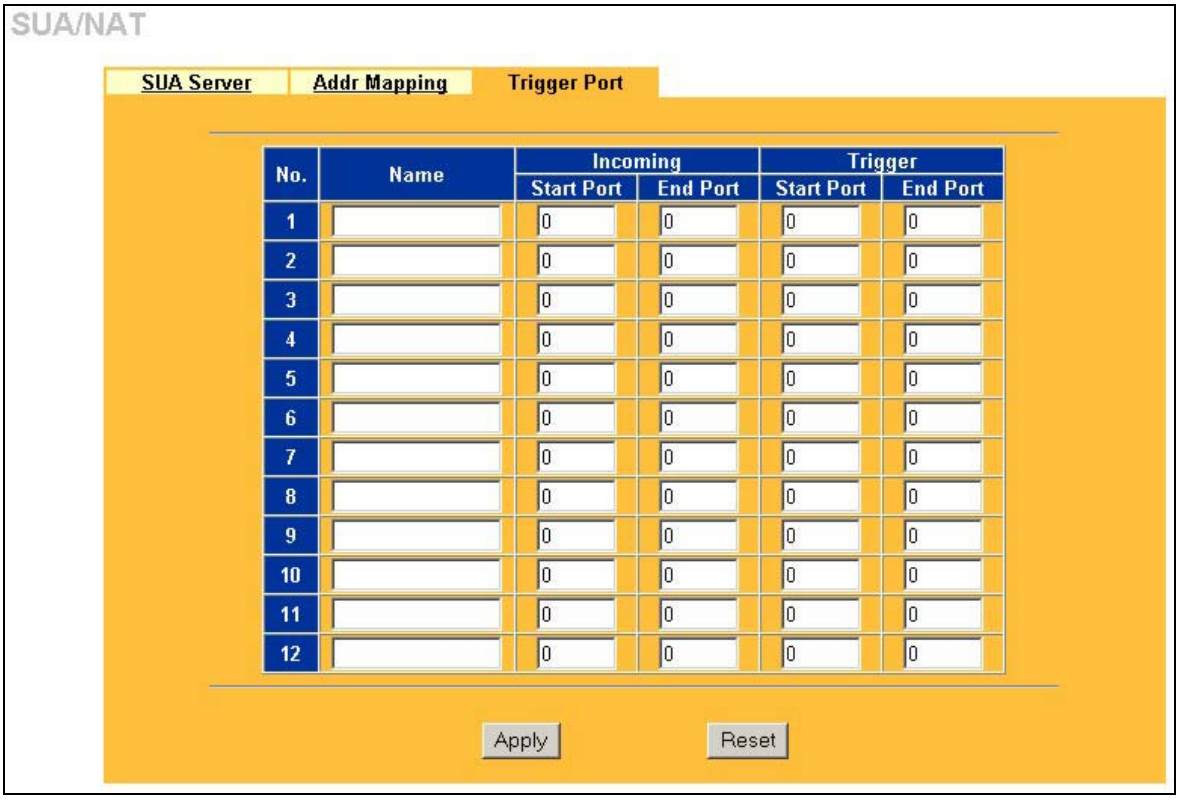


Figure 9-7 Trigger Port

The following table describes the fields in this screen.

Table 9-7 Trigger Port

LABEL	DESCRIPTION
No.	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.

Table 9-7 Trigger Port

LABEL	DESCRIPTION
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 10
Static Route Screens

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

10.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the ZyWALL has no knowledge of the networks beyond. For instance, the ZyWALL knows about network N2 in the following figure through remote node Router 1. However, the ZyWALL is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyWALL about the networks beyond the remote nodes.

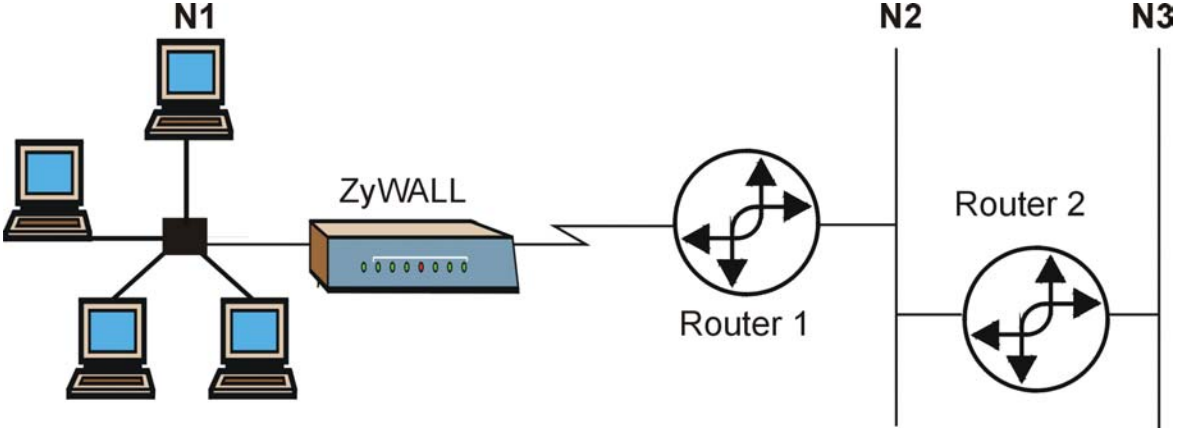


Figure 10-1 Example of Static Routing Topology

10.2 Configuring IP Static Route

Click **STATIC ROUTE** to open the **Route Entry** screen.

The following table describes the fields in this screen.

Table 10-1 IP Static Route Summary

LABEL	DESCRIPTION
#	Number of an individual static route.
Name	Name that describes or identifies this route.

Table 10-1 IP Static Route Summary

LABEL	DESCRIPTION
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyWALL; over the WAN, the gateway must be the IP address of one of the remote nodes.
Edit	Click a static route index number and then click **Edit** to set up a static route on the ZyWALL.

10.2.1 Configuring Route Entry

Select a static route index number and click **Edit**. The screen shown next appears. Fill in the required information for each static route.

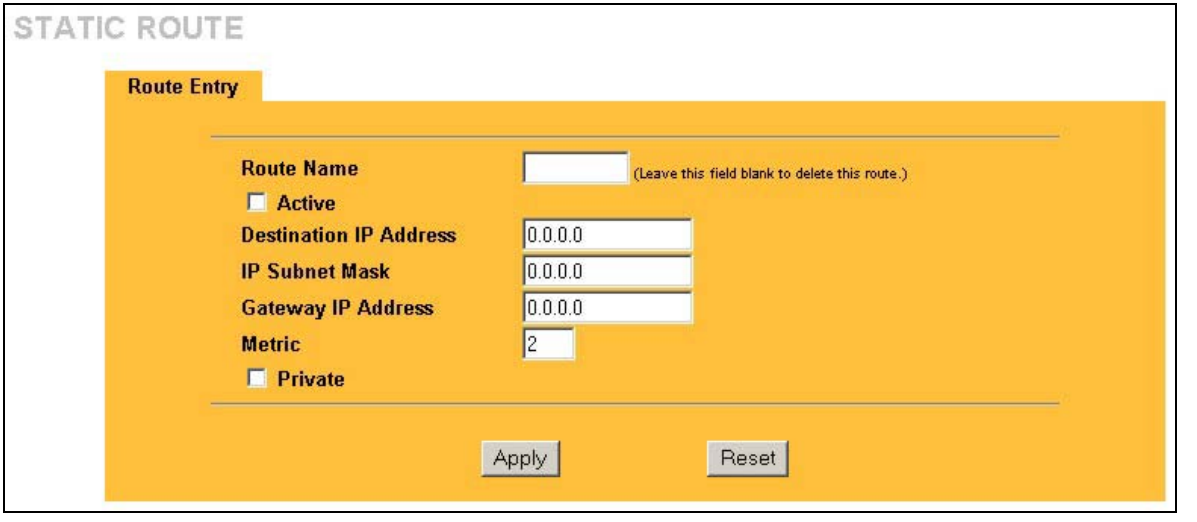


Figure 10-2 Edit IP Static Route

The following table describes the fields in this screen.

Table 10-2 Edit IP Static Route

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyWALL; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyWALL will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

Part V:

Firewall and Content Filters

This part introduces firewalls in general and the ZyWALL firewall. It also explains how to configure the ZyWALL firewall and content filtering.

Chapter 11
Firewalls

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

11.1 Firewall Overview

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

11.2 Types of Firewalls

There are three main types of firewalls:

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

11.2.1 Packet Filtering Firewalls

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

11.2.2 Application-level Firewalls

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

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

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

11.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. See *section 11.5* for more information on Stateful Inspection.

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

11.3 Introduction to ZyXEL's Firewall

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

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

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

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

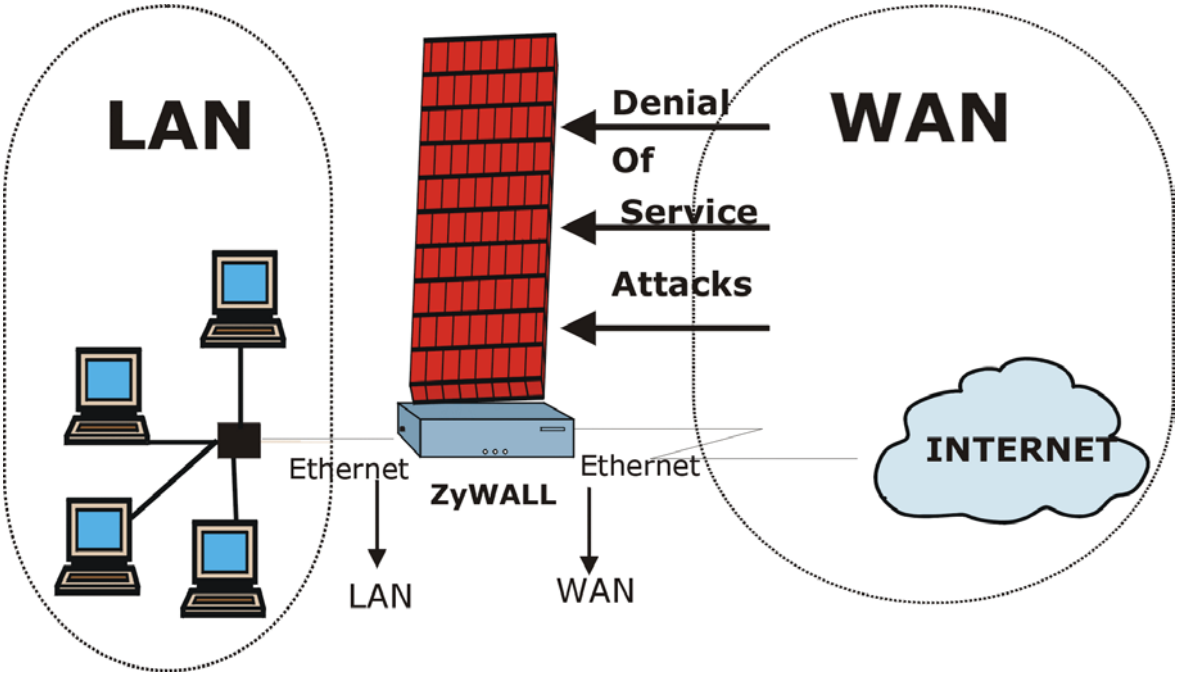


Figure 11-1 ZyWALL Firewall Application

11.4 Denial of Service

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

11.4.1 Basics

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

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended

for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 11-1 Common IP Ports

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

11.4.2 Types of DoS Attacks

There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.
4. IP Spoofing.

1. "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

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

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

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

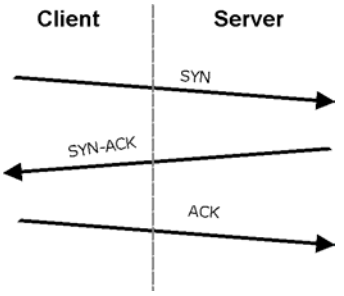


Figure 11-2 Three-Way Handshake

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

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

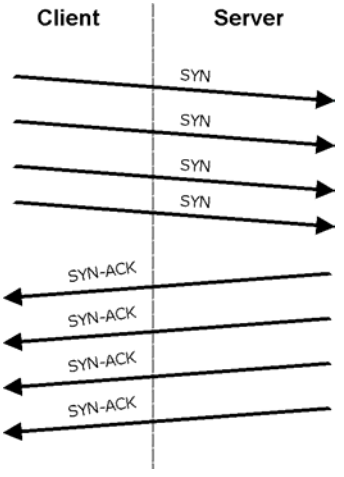


Figure 11-3 SYN Flood

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

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

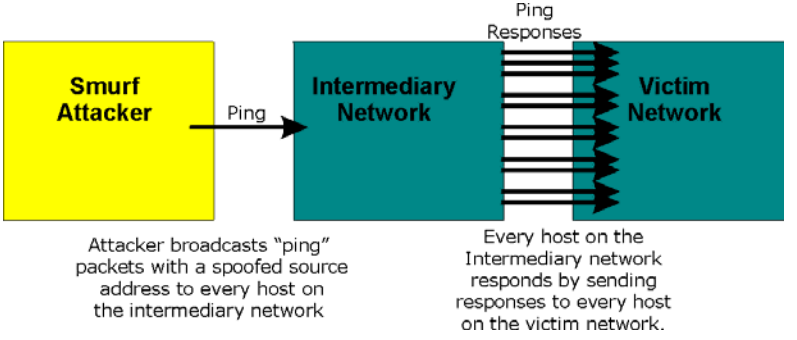


Figure 11-4 Smurf Attack

- ICMP Vulnerability

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

Table 11-2 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- Illegal Commands (NetBIOS and SMTP)

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

Table 11-3 Legal NetBIOS Commands

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

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

Table 11-4 Legal SMTP Commands

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

- Traceroute

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

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

11.5 Stateful Inspection

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

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

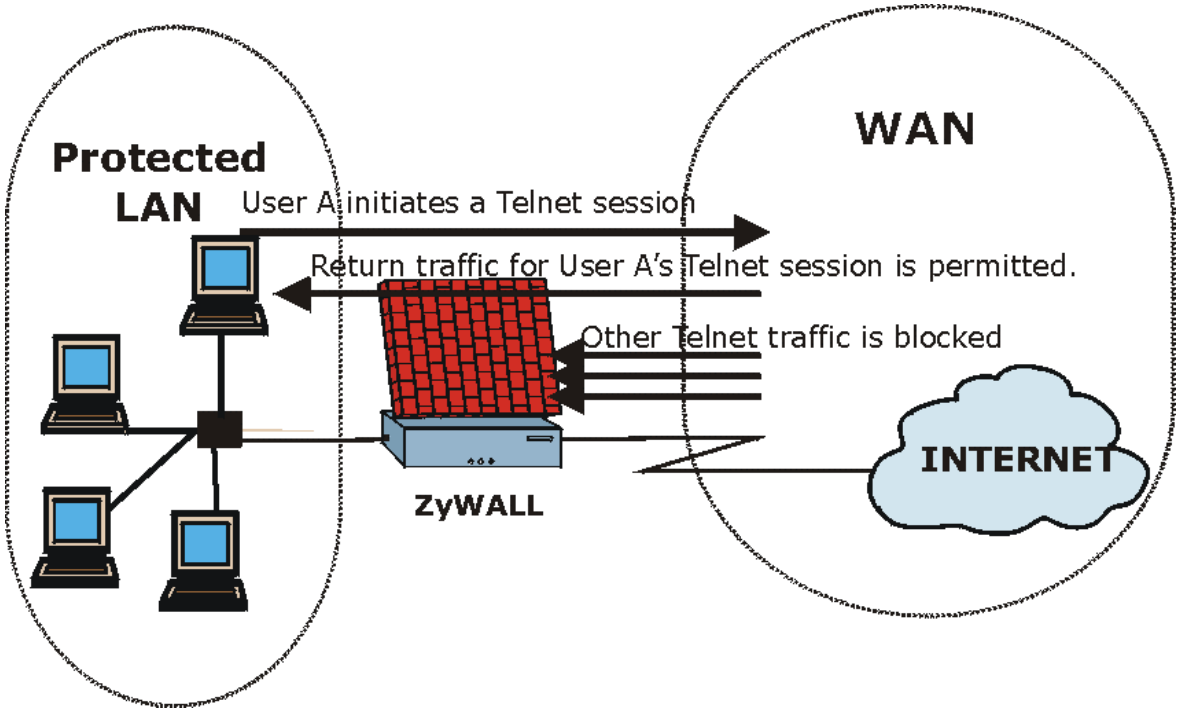


Figure 11-5 Stateful Inspection

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

11.5.1 Stateful Inspection Process

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

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).

3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **The default action for packets not matching following rules** field determines the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

11.5.2 Stateful Inspection and the ZyWALL

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

i. Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.

ii. Allow certain types of traffic from the Internet to specific hosts on the LAN.

iii. Allow access to a Web server to everyone but competitors.

iv. Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

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

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

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

11.5.3 TCP Security

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

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

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

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

11.5.4 UDP/ICMP Security

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

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

A similar situation exists for ICMP, except that the ZyWALL is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too

little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

11.5.5 Upper Layer Protocols

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

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

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

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

11.6 Guidelines For Enhancing Security With Your Firewall

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

11.7 Packet Filtering Vs Firewall

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

11.7.1 Packet Filtering:

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

When To Use Filtering

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

11.7.2 Firewall

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

When To Use The Firewall

1. To prevent DoS attacks and prevent hackers cracking your network.

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

Chapter 12
Firewall Screens

This chapter shows you how to configure your ZyWALL firewall.

12.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyWALL has to offer. For this reason, it is recommended that you configure your firewall using the web configurator. SMT screens allow you to activate the firewall. CLI commands provide limited configuration options and are only recommended for advanced users, please refer to the *Reference Guide* for firewall CLI commands.

12.2 Firewall Policies Overview

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

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

DMZ is not available on all models.

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

- LAN to LAN/ZyWALL

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

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

- WAN to LAN
- WAN to WAN/ZyWALL

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

- DMZ to LAN
- DMZ to DMZ/ZyWALL

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

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

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

For example, you may create rules to:

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

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

12.3 Rule Logic Overview

Study these points carefully before configuring rules.

12.3.1 Rule Checklist

1. State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."
2. Is the intent of the rule to forward or block traffic?
3. What direction of traffic does the rule apply to (refer to *12.2*)?
4. What IP services will be affected?

5. What computers on the LAN or DMZ are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

12.3.2 Security Ramifications

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

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

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

12.3.3 Key Fields For Configuring Rules

Action

Should the action be to **Block** or **Forward**?

"Block" means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See *section 12.7* for more information on predefined services.

Source Address

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

Destination Address

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

12.4 Connection Direction Examples

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

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

12.4.1 LAN to WAN Rules

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

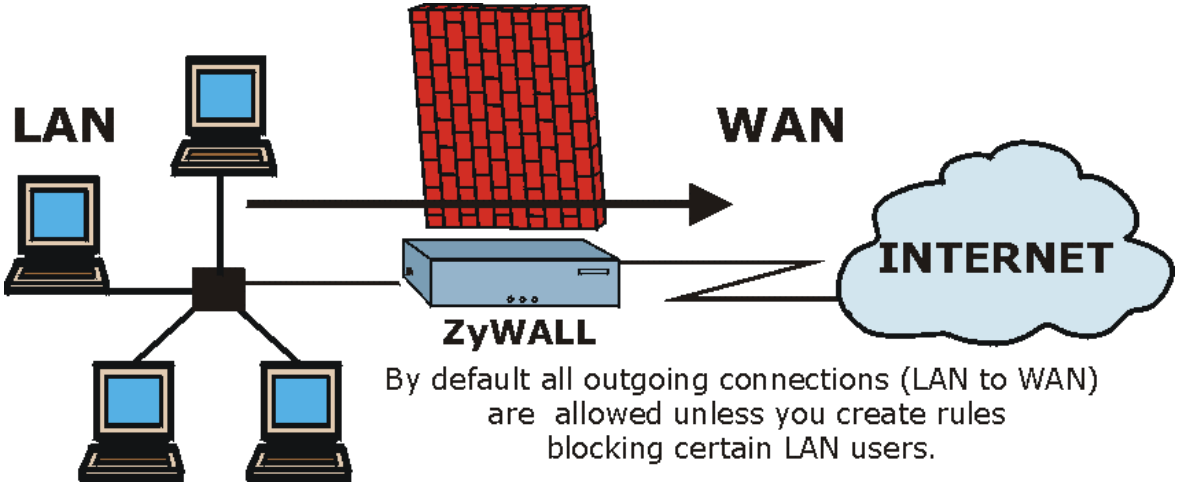


Figure 12-1 LAN to WAN Traffic

12.4.2 WAN to LAN Rules

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

See the following figure.

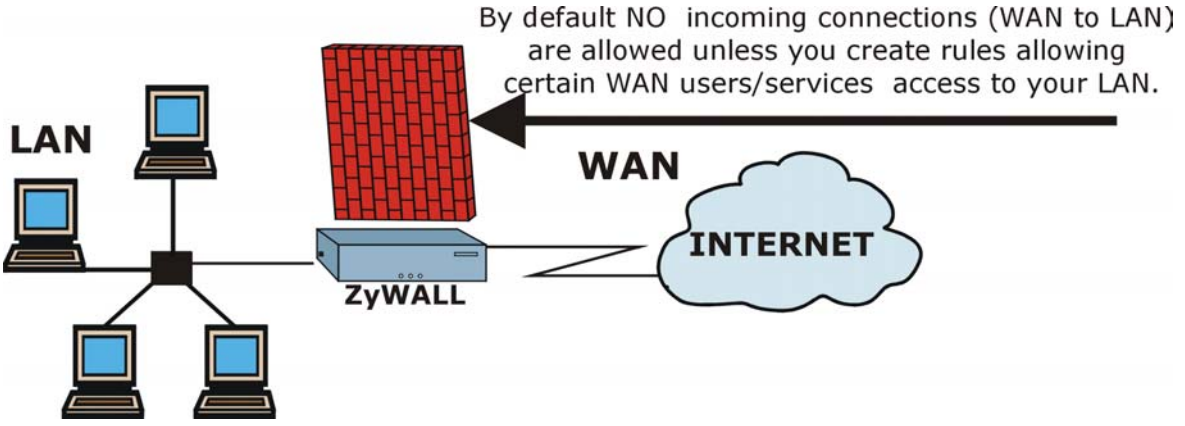


Figure 12-2 WAN to LAN Traffic

12.5 Configuring Firewall

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

Click **FIREWALL** to open the **Summary** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box as seen in the following screen.

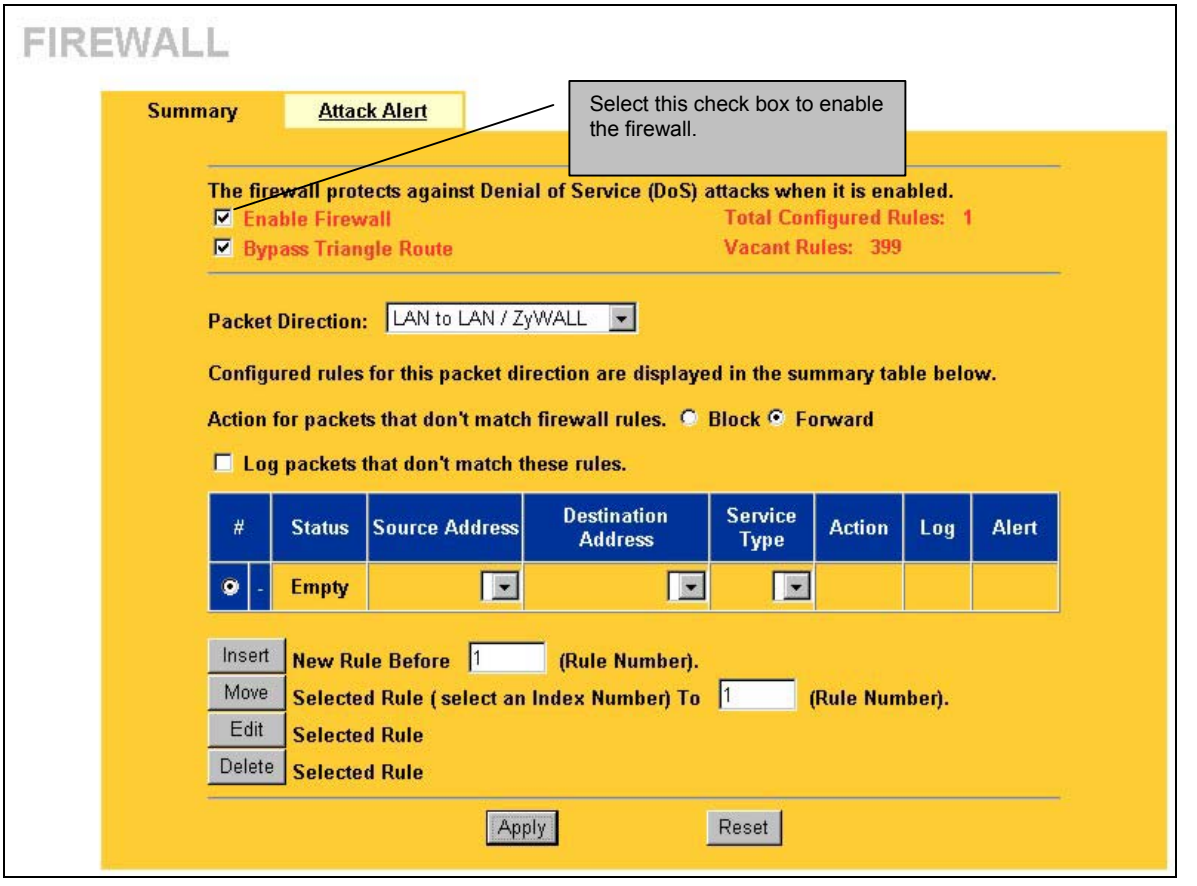


Figure 12-3 Enabling the Firewall (ZyWALL 100)

The following table describes the fields in this screen.

Table 12-1 Firewall Rules Summary: First Screen

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the ZyWALL firewall ignore the use of triangle route topology on the network. See the *Reference Guide* for more on triangle route topology.

Table 12-1 Firewall Rules Summary: First Screen

LABEL	DESCRIPTION
Total Configured Rules	This read-only number is the total number of rules that have been configured for the ZyWALL (the combined total for all packet directions). The ZyWALL allows you to configure up to 30 firewall rules total.
Vacant Rules	This read-only number is the number of rules that can still be configured for the ZyWALL (the combined total available for all packet directions).
Packet Direction	Use the drop-down list box to select a direction of travel of packets (**LAN to LAN/ZyWALL**, **LAN to WAN**, **LAN to DMZ**, **WAN to WAN/ZyWALL**, **WAN to LAN**, **WAN to DMZ, DMZ to DMZ/ZyWALL**, **DMZ to LAN** or **DMZ to WAN**) for which you want to configure firewall rules.
Block/ Forward	Use the option buttons to select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that are traveling in the selected direction.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.	
Index	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The **Move** field below allows you to reorder your rules.
Status	This field displays whether a firewall is turned on (**Active**) or not (**Inactive**). Rules that have not been configured display **Empty**.
Source Address	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Destination Address	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Service Type	This drop-down list box displays the services to which this firewall rule applies. Please note that a blank service type is equivalent to **Any**. See *Table 12-5* for more information.
Action	This is the specified action for that rule, either **Block** or **Forward**. Note that **Block** means the firewall silently discards the packet.
Log	This field shows you if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**).

Table 12-1 Firewall Rules Summary: First Screen

LABEL	DESCRIPTION
Alert	This field tells you whether this rule generates an alert (**Yes**) or not (**No**) when the rule is matched.
Insert	Type the index number for where you want to put a rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. Click **Insert** to display this screen and refer to the following table for information on the fields.
Move	Select a rule's Index option button and type a number for where you want to put that rule. Click **Move** 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.
Rule to (Rule Number)	Click a rule's option button and type the number for where you want to put that rule.
Edit	Click **Edit** to create or edit a rule.
Delete	Click **Delete** to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

12.5.1 Configuring Firewall Rules

Follow these directions to create a new rule.

Step 1. In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

Step 2. Click **Insert** to display this screen and refer to the following table for information on the fields.

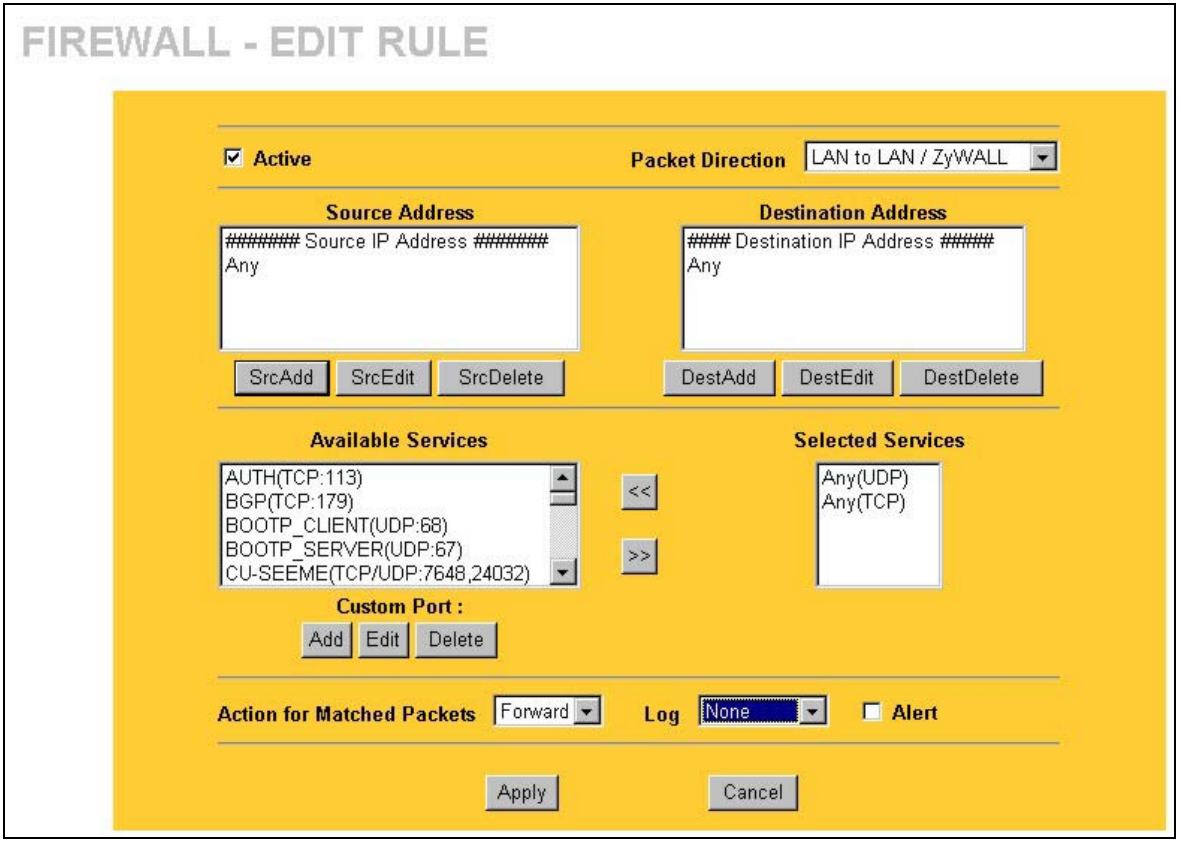


Figure 12-4 Creating/Editing A Firewall Rule (ZyWALL100)

The following table describes the fields in this screen.

Table 12-2 Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
Active	Check the **Active** check box to have the ZyWALL use this rule. Leave it unchecked if you do not want the ZyWALL to use the rule after you apply it
Packet Direction	Use the drop-down list box to select the direction of packet travel to which you want to apply this firewall rule.

Table 12-2 Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
Source Address	Click **SrcAdd** to add a new address, **SrcEdit** to edit an existing one or **SrcDelete** to delete one. Please see the next section for more information on adding and editing source addresses.
Destination Address	Click **DestAdd** to add a new address, **DestEdit** to edit an existing one or **DestDelete** to delete one. Please see the following section on adding and editing destination addresses.
Services Available/ Selected Services	Please see *Table 12-5* for more information on services available. Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **<<**.
Custom Port	
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Edit	Select a custom service (denoted by an "*") from the **Available Services** list and click this button to edit the service.
Delete	Select a custom service (denoted by an "*") from the **Available Services** list and click this button to remove the service.
Action for Matched Packets	Use the drop down list box to select whether to discard (**Block**) or allow the passage of (**Forward**) packets that match this rule.
Log	This field determines if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**). Go to the **Log Settings** page and select the **Access Control** logs category to have the ZyWALL record these logs.
Alert	Check the **Alert** check box to determine that this rule generates an alert when the rule is matched.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving,

12.5.2 Configuring Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen**.** Either action displays the following screen.

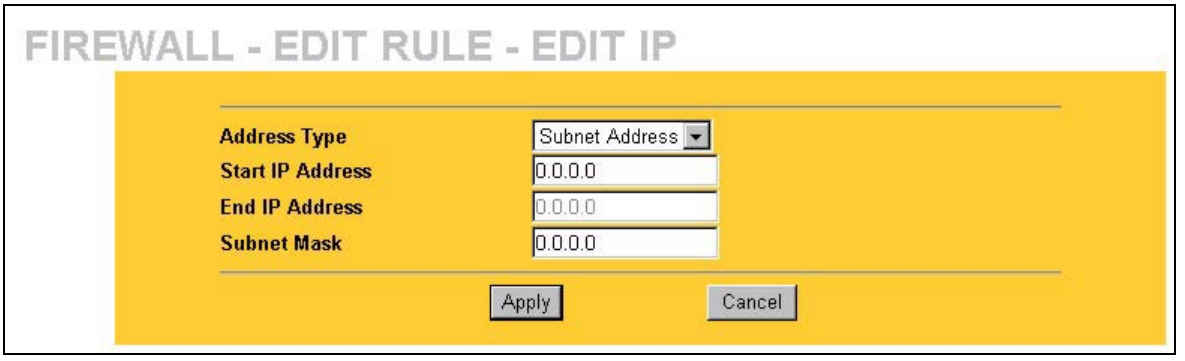


Figure 12-5 Adding/Editing Source and Destination Addresses

The following table describes the fields in this screen.

Table 12-3 Adding/Editing Source and Destination Addresses

LABEL	DESCRIPTION
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving,

12.5.3 Configuring Custom Ports

Configure customized ports for services not predefined by the ZyWALL (see *section 12.7* for a list of predefined services). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

Click the **Add** button under **Custom Port** while editing a firewall to configure a custom port. This displays the following screen.

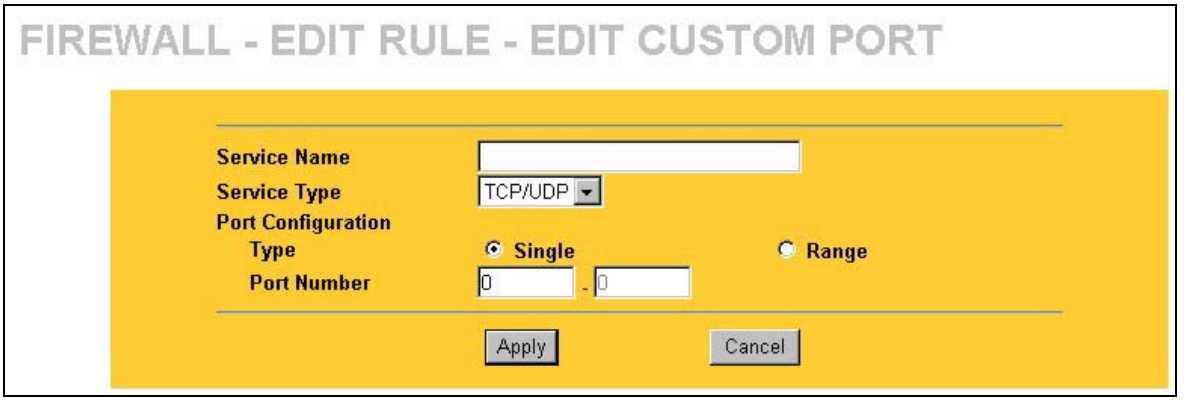


Figure 12-6 Creating/Editing A Custom Port

The following table describes the fields in this screen.

Table 12-4 Creating/Editing A Custom Port

LABEL	DESCRIPTION
Service Name	Enter a unique name for your custom port.
Service Type	Choose the IP port (**TCP**, **UDP** or **Both**) that defines your customized port from the drop down list box.
Port Configuration Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.
Port Number	Enter a single port number or the range of port numbers that define your customized service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving,

12.6 Example Firewall Rule

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

Step 1. Click the **Firewall** link and then the **Summary** tab.

Step 2. In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

Step 3. Click **Insert** to display the firewall rule configuration screen.

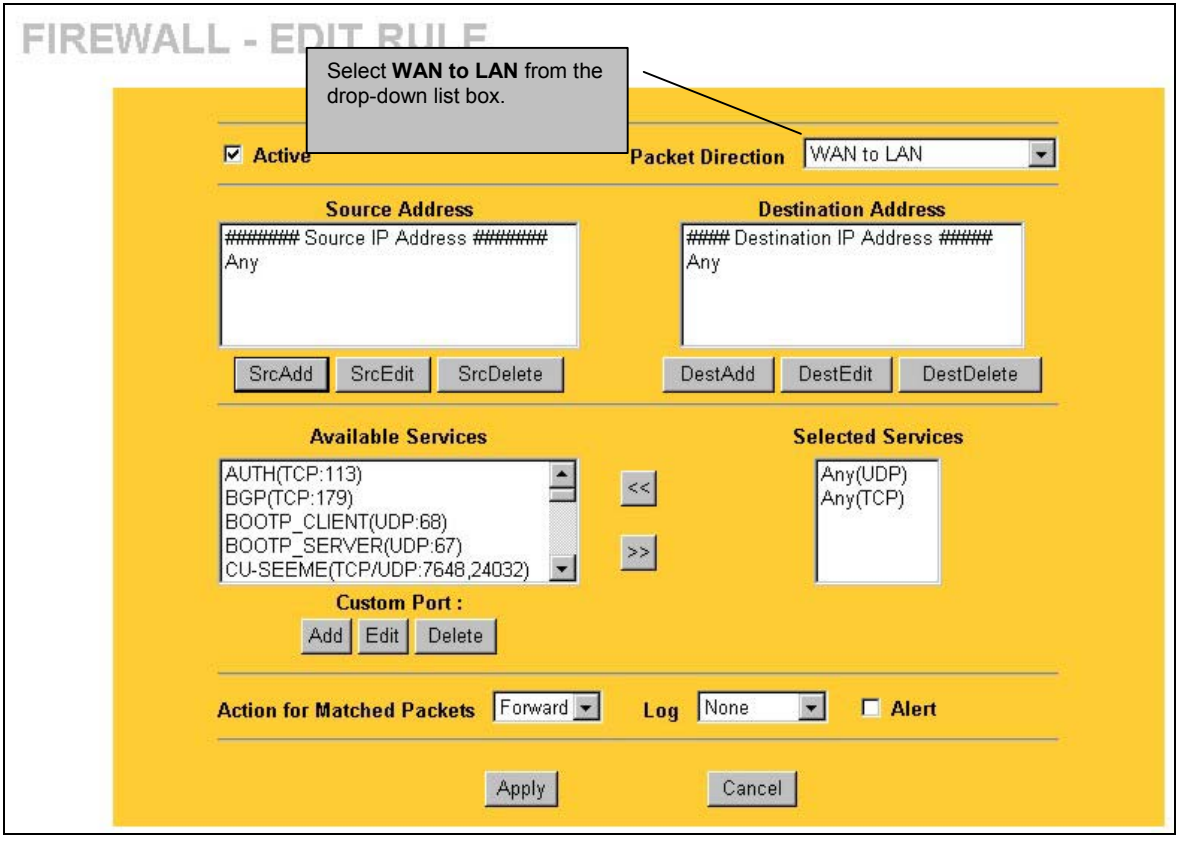


Figure 12-7 Firewall IP Config Screen

Step 4. Select **Any** in the Source Address box and then click **ScrDelete**.

Step 5. Click **ScrAdd** under the Source Address box.

Step 6. Configure the **Firewall Rule Edit IP** screen as follows and click **Apply**.

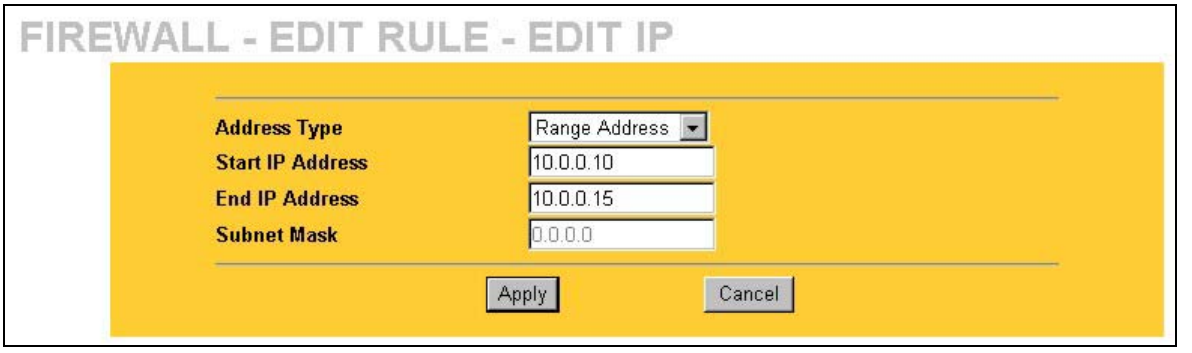


Figure 12-8 Firewall Rule Edit IP Example

Step 7. In the firewall rule configuration screen, click **Add** under **Custom Port** to open the **Edit Custom Port** screen. Configure it as follows and click **Apply**.

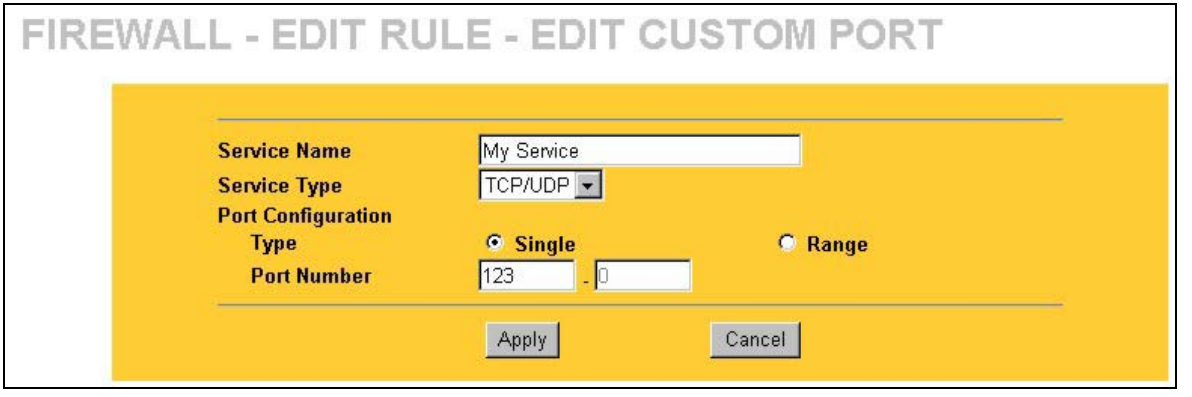


Figure 12-9 Edit Custom Port Example

Step 8. The firewall rule configuration screen displays, use the arrows between **Available Services** and **Selected Services** to configure it as follows. Click **Apply** when you are done.

Custom ports show up with an "*" before their names in the Services **list box and the Rule Summary list box. Click** Apply **after you've created your custom port.**

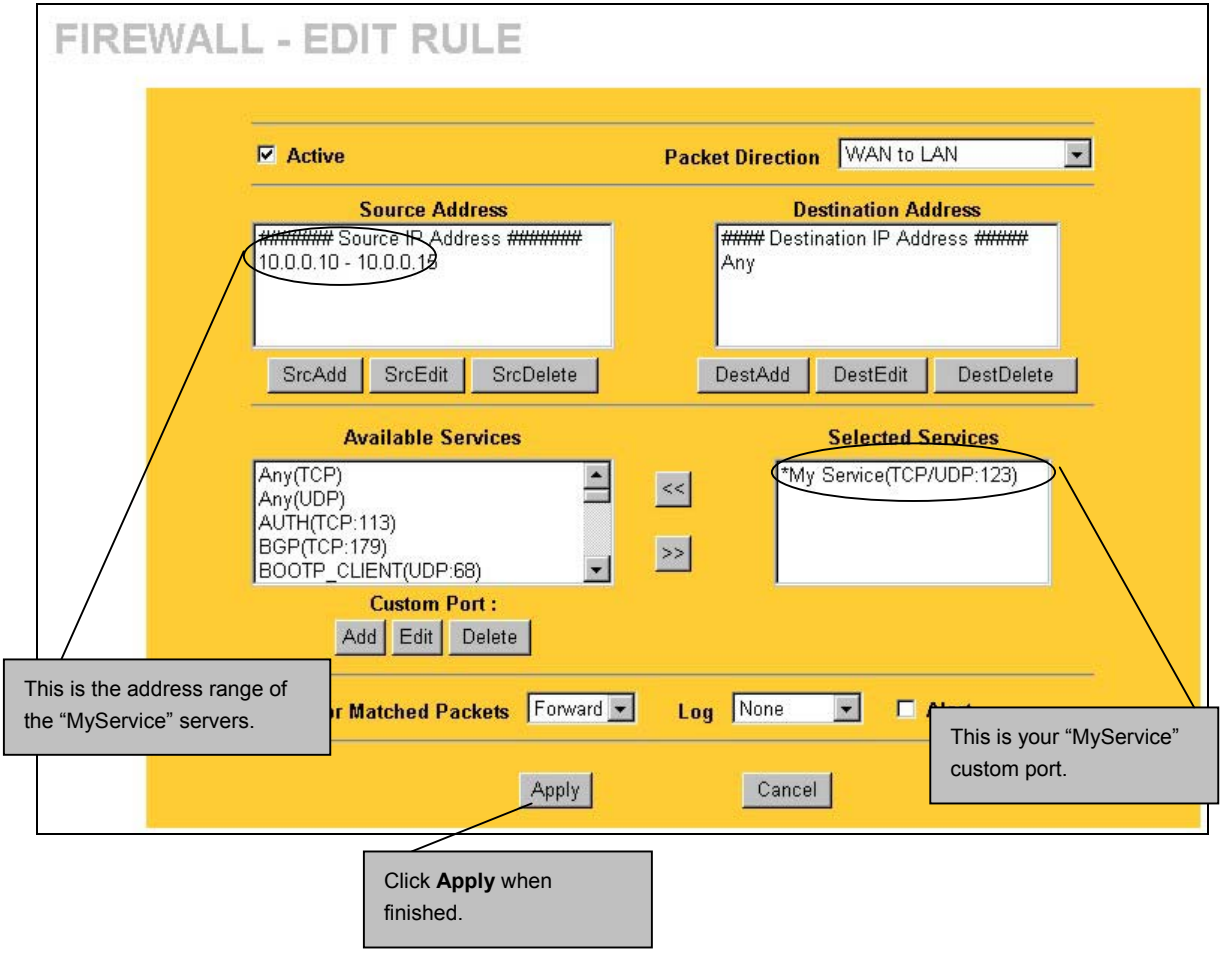


Figure 12-10 MyService Rule Configuration (ZyWALL100)

On completing the configuration procedure for this Internet firewall rule, the **Rule Summary** screen should look like the following. Remember to click **Apply** when you have finished configuring your rule(s) to save your settings back to the ZyWALL.

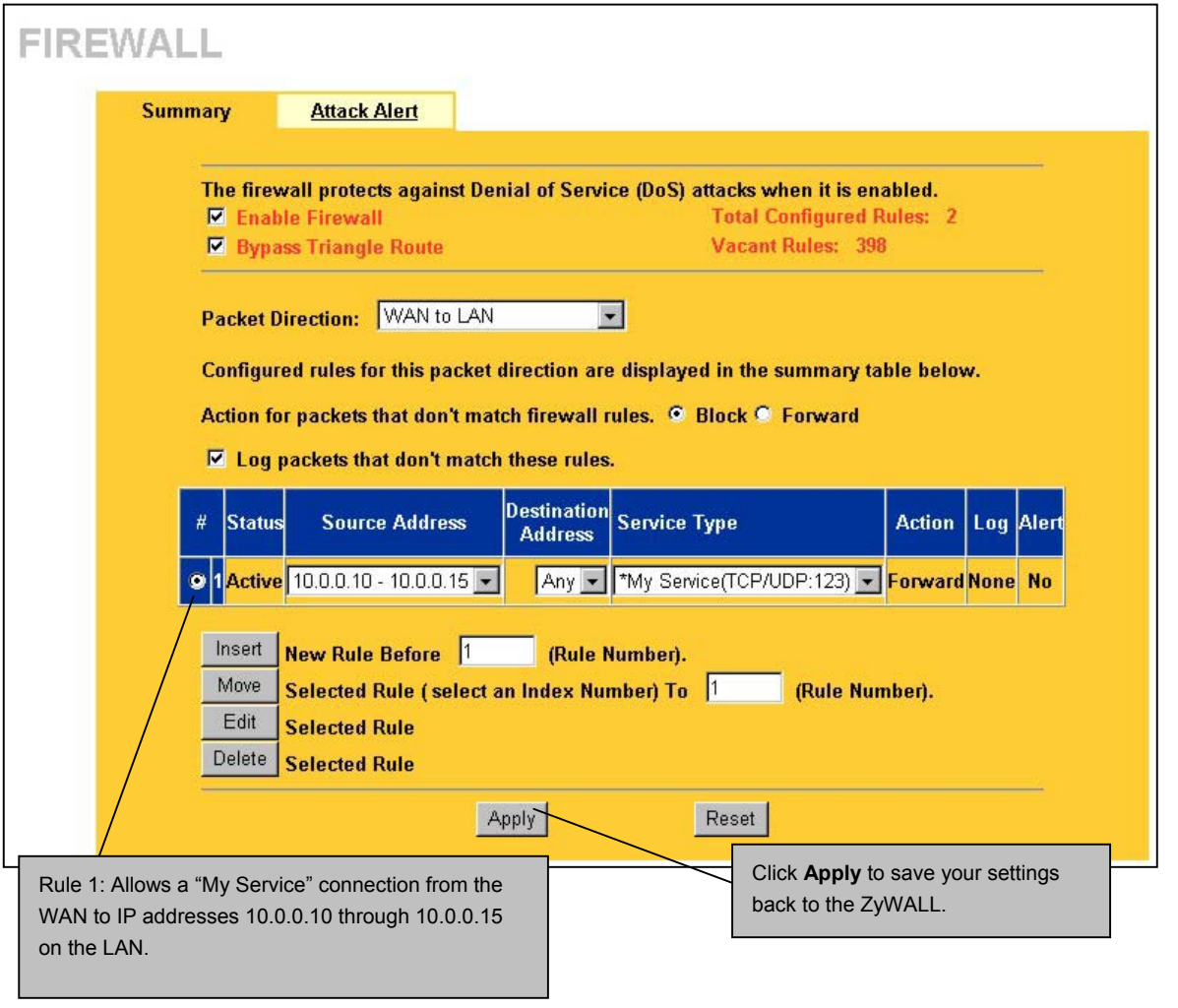


Figure 12-11 My Service Example Rule Summary (ZyWALL100)

12.7 Predefined Services

The **Available Services** list box in the **Rule Config**(uration) screen (see *Figure 12-4*) displays all predefined services that the ZyWALL already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Custom services may also be configured using the **Custom Ports** function discussed later.

Table 12-5 Predefined Services

SERVICE	DESCRIPTION
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.

Table 12-5 Predefined Services

SERVICE	DESCRIPTION
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
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(ICMP:0)	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:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.

Table 12-5 Predefined Services

SERVICE	DESCRIPTION
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.

12.8 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Attack Alert** screen *(Figure 12-12* - check the **Generate alert when attack detected** checkbox) or when a rule is matched in the **Rule Config** screen (see *Figure 12-4)*. When an event generates an alert, a message is immediately sent to an e-mail account specified by you. Enter the complete e-mail address to which alert messages will be sent in the **E-mail Alerts To** field and schedule times for sending alerts in the **Log Timer** fields in the **E-mail** screen (following screen).

12.9 Configuring Attack Alert

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

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

12.9.1 Threshold Values

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

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

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.
You should make any changes to the threshold values before you continue configuring firewall rules.

12.9.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see *Figure 11-2*). For UDP, "half-open" means that the firewall has detected no return traffic.

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

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

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

TCP Maximum Incomplete and Blocking Time

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

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

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

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

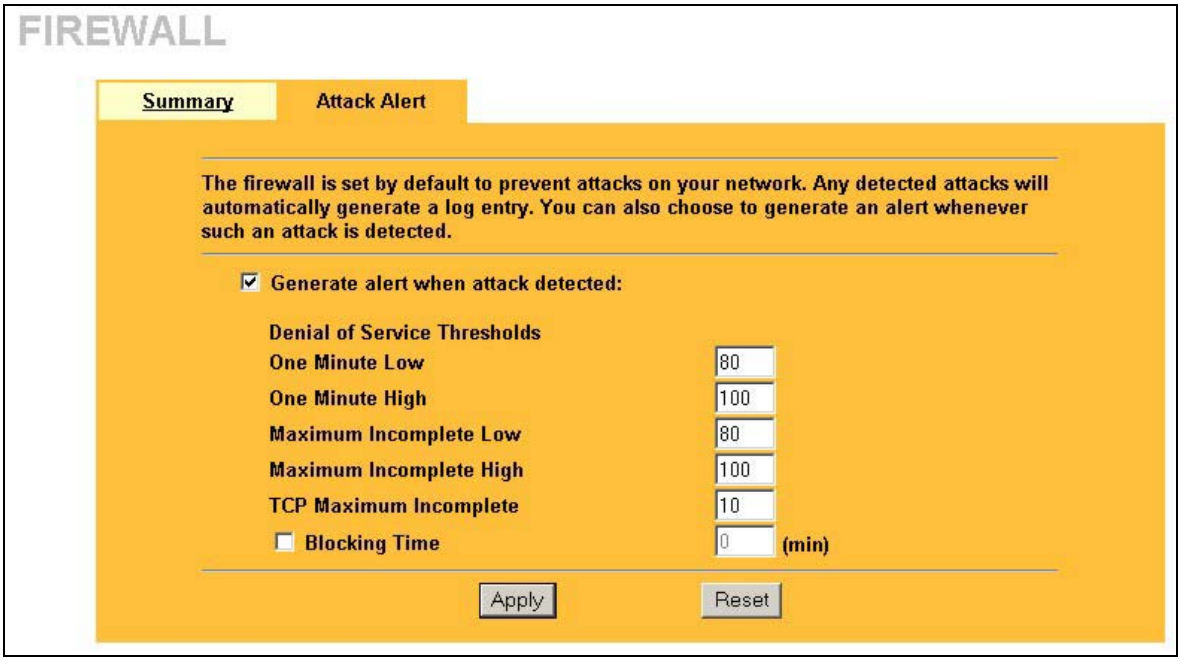


Figure 12-12 Attack Alert

The following table describes the fields in this screen.

Table 12-6 Attack Alert

LABEL	DESCRIPTION	DEFAULT VALUES
Generate alert when attack detected	A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected. See the chapter on logs for more information on logs and alerts.	
Denial of Service Thresholds		
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.

Table 12-6 Attack Alert

LABEL	DESCRIPTION	DEFAULT VALUES
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the ZyWALL to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum** I**ncomplete Low** number.	100 existing half-open sessions. The above values causes the ZyWALL to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	10 existing half-open TCP sessions.

Table 12-6 Attack Alert

LABEL	DESCRIPTION	DEFAULT VALUES
Blocking Time	When **TCP Maximum Incomplete** is reached you can choose if the next session should be allowed or blocked. If you check **Blocking Time** any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.	Select this check box to specify a number in minutes (min) text box.
(min)	Enter the length of **Blocking Time** in minutes.	0
Apply	Click **Apply** to save your changes back to the ZyWALL.	
Reset	Click **Reset** to begin configuring this screen afresh.	

Chapter 13
Content Filtering Screens

This chapter provides a brief overview of content filtering.

13.1 Content Filtering Overview

Internet content filtering allows schools and businesses to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URLs and should not be confused with packet filtering via SMT menu 21.1.

13.1.1 Restrict Web Features

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

13.1.2 Filter List

You can select categories, such as pornography or racial intolerance, to block or monitor from a pre-defined list. There is a period of free use of the list when you register the ZyWALL. After this period, you must subscribe to the list periodically.

13.1.3 Days and Times

The ZyWALL also allows you to define time periods and days during which content filtering should be enabled.

13.2 Configuring Categories

Click **CONTENT FILTER** to open the **Categories** screen.

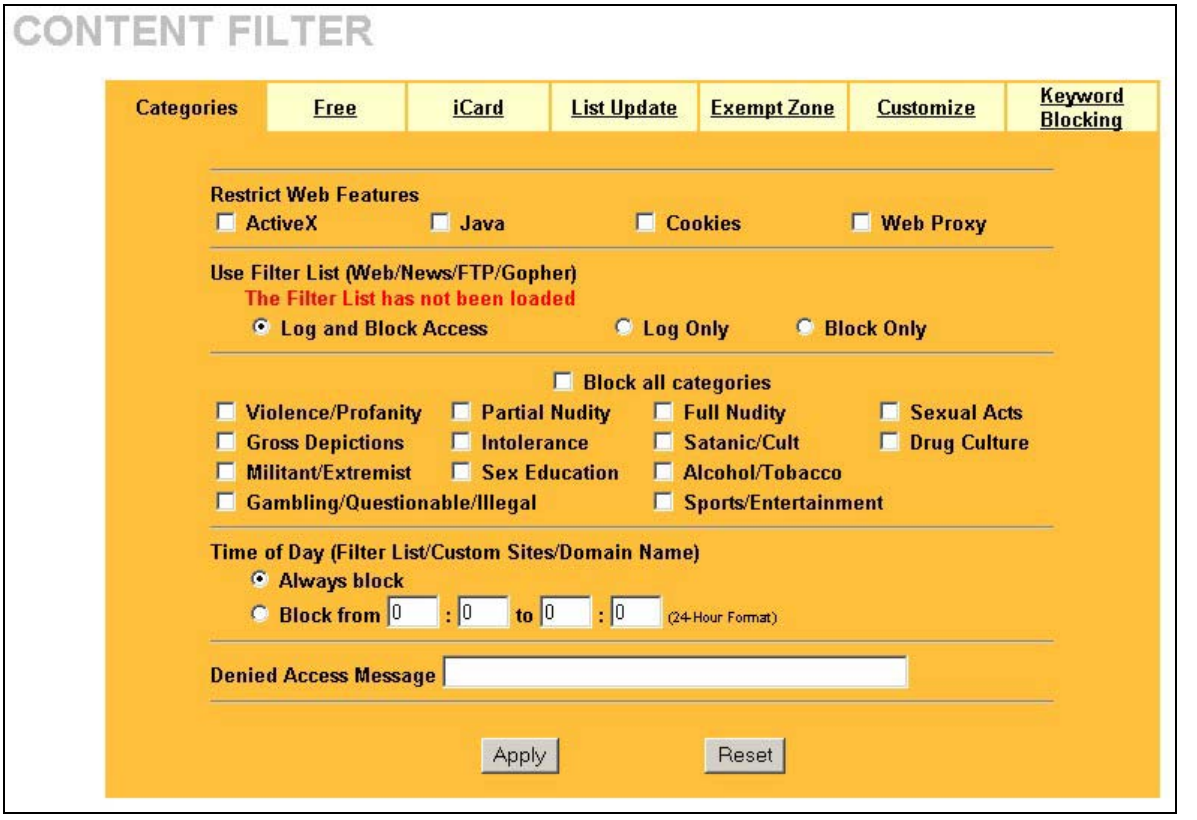


Figure 13-1Content Filter: Categories

The following table describes the fields in this screen.

Table 13-1 Content Filter: Categories

LABEL	DESCRIPTION
Restricted Web Features	Restricted Web Features Select the 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.
ActiveX	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.

Table 13-1 Content Filter: Categories

LABEL	DESCRIPTION
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers 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.
Use Filter List (Web/News/FTP/Gopher) You will see the message "The Filter List has not been loaded" if you have not yet downloaded the filter list or your subscription has expired.	
Log and Block Access	Click this option button to record attempts to access prohibited sites (as defined below) and prevent users from accessing these sites.
Log Only	Click this option button to just log user attempts to access prohibited sites (as defined below).
Block Only	Click this option button to prevent users from accessing prohibited sites (as defined below), but have no record made of attempts to access these sites.
Block all categories	Select this box to restrict access to all site categories listed below.
Violence/ Profanity	Selecting this category excludes pictures or text exposing extreme cruelty, or physical or emotional acts against any animal or person, which are primarily intended to hurt or inflict pain. Obscene words, phrases, and profanity are defined as text that uses, but is not limited to, George Carlin's seven censored words more often than once every 50 messages (Newsgroups) or once a page (Web sites).
Partial Nudity	Selecting this category excludes pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia.
Full Nudity	Selecting this category excludes pictures exposing any or all portions of the human genitalia.
Sexual Acts	Selecting this category excludes pictures or text exposing anyone or anything involved in explicit sexual acts and or lewd and lascivious behavior. Also includes phone sex ads, dating services, and adult personals, CD-ROM's and videos.
Gross Depictions	Selecting this category excludes pictures or descriptive text of anyone or anything which are crudely vulgar or grossly deficient in civility or behavior, or which show scatological impropriety. Includes such depictions as maiming, bloody figures, or indecent depiction of bodily functions.

Table 13-1 Content Filter: Categories

LABEL	DESCRIPTION
Intolerance	Selecting this category excludes pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Also includes intolerant jokes or slurs.
Satanic/Cult	Selecting this category excludes pictures or text advocating devil worship, an affinity for evil or wickedness, or the advocacy to join a cult. A cult is defined as a closed society headed by a single individual where loyalty is demanded and leaving is punishable.
Drug Culture	Selecting this category excludes pictures or text advocating the illegal use of drugs for entertainment. Includes substances used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This would exclude currently illegal drugs legally prescribed for medicinal purposes.
Militant/ Extremist	Selecting this category excludes pictures or text advocating extremely aggressive and combative behaviors, or advocacy of unlawful political measures. Topics include groups that advocate violence as a means to achieve their goals. Includes "how to" information on weapons making, ammunition making or the making or use of pyrotechnics materials. Also includes the use of weapons for unlawful reasons.
Sex Education	Selecting this category excludes pictures or text advocating the proper use of contraceptives. In addition, this category will include discussion sites on discussing diseases with a partner, pregnancy and respecting boundaries. Excluded from this category are commercial sites wishing to sell sexual paraphernalia.
Alcohol/Tobacco	Selecting this category excludes pictures or text advocating the sale, consumption, or production of alcoholic beverages and tobacco products.
Gambling/ Questionable/ Illegal	Selecting this category excludes pictures or text advocating materials or activities of a dubious nature which may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using someone's phone lines without permission) and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, on-line sports or financial betting, including non-monetary dares.
Sports/ Entertainment	Selecting this category excludes pictures or text of leisure, sports, or other similar sites not considered applicable to the primary business function.
Time of Day allows the administrator to define time periods content filtering is enabled.	
Time of Day (Filter List/Custom Sites/Domain Name)	Time of Day restrictions only apply to the Filter List (sites checked above), Customized sites and Keywords. Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected.

Table 13-1 Content Filter: Categories

LABEL	DESCRIPTION
Always Block	Click this option button to have content filtering always active with Time of Day limitations not enforced. This is enabled by default.
Block from	Click this option button to have content filtering only active during the time interval specified. Enter the time period, in 24-hour format, during which content filtering will be enforced.
Denied Access Message	Enter a message to be displayed when a user tries to access a restricted web site.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

13.3 Configuring Free

Use this screen to register the ZyWALL. Registering the ZyWALL allows you to install and activate the Content Filter List, and to receive a free subscription to updated Content Filter Lists for a limited period. You may register your ZyWALL for the initial free subscription in this page by filling in your personal information in the fields and then clicking **Apply**. You must fill in all required fields (denoted by an asterisk).

To register your ZyWALL, click **CONTENT FILTER**, then the **Free** tab. The screen appears as shown.

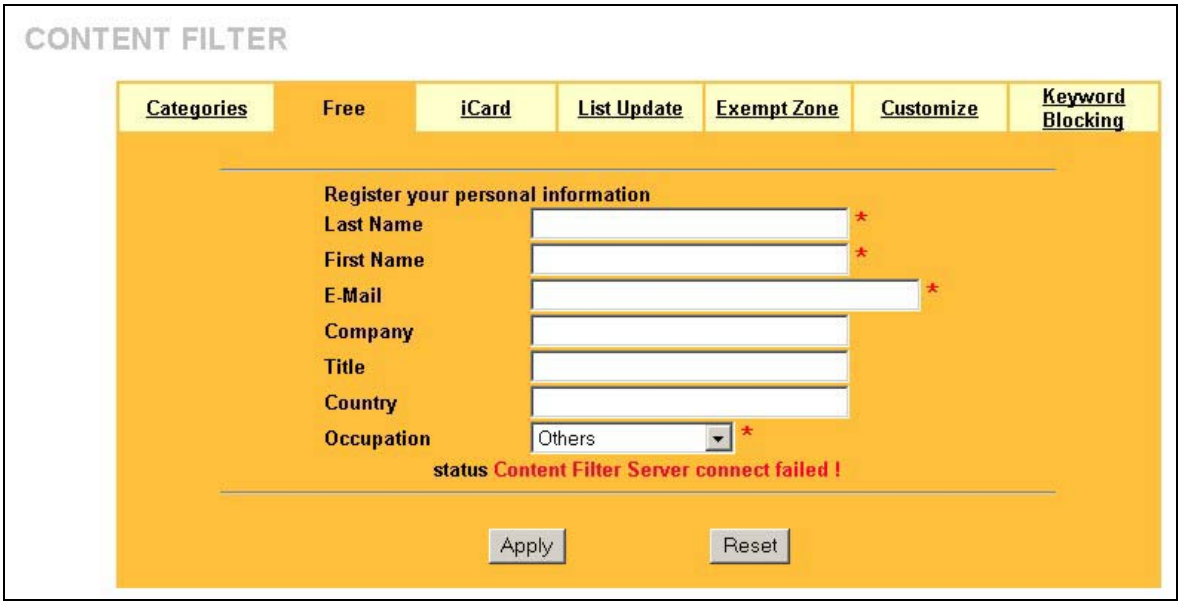


Figure 13-2 Content Filter: Free

The following table describes the fields in this screen.

Table 13-2 Content Filter: Free

LABEL	DESCRIPTION
Last Name	Type your last name. You may enter up to 31 characters. This is a required field.
First Name	Type your first name. You may enter up to 31 characters. This is a required field.
E-mail	Type your e-mail address. You may enter up to 40 characters. This is a required field.
Company	Type the name of your company. You may enter up to 31 characters.
Title	Type your job title. You may enter up to 31 characters.
Country	Type your country name. You may enter up to 31 characters.
Occupation	Select the industry you work in from this drop-down list box. This is a required field.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

13.4 Configuring iCard

Use this screen to re-register the ZyWALL after the initial free subscription period expires (see 13.3). Update your subscription in this page by filling in your personal information in the fields as shown, and then click **Apply**. You must fill in all required fields (marked with an asterisk).

To re-register your ZyWALL, click **CONTENT FILTER**, then the **iCARD** tab. The screen appears as shown.

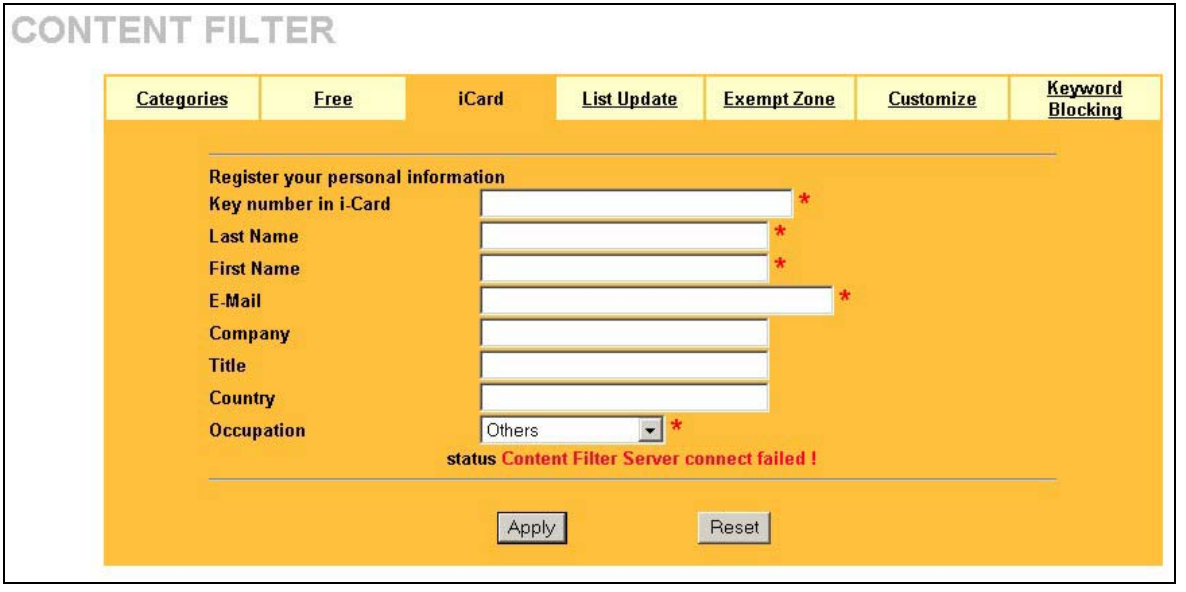


Figure 13-3 Content Filter: iCard

The following table describes the fields in this screen.

Table 13-3 Content Filter: iCard

LABEL	DESCRIPTION
Key number in I-Card	Type the key from your subscription card (required field).
Last Name	Type your last name. You may enter up to 31 characters (required field).
First Name	Type your first name. You may enter up to 31 characters (required field).
E-mail	Type your e-mail address. You may enter up to 40 characters (required field).

Table 13-3 Content Filter: iCard

LABEL	DESCRIPTION
Company	Type the name of your company. You may enter up to 31 characters.
Title	Type your job title. You may enter up to 31 characters.
Country	Type your country name. You may enter up to 31 characters.
Occupation	Select the industry you work in from this drop-down list box (required field).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

13.5 Configuring List Update

To update the list of filters on your ZyWALL, click **CONTENT FILTER**, then the **List Update** tab. The screen appears as shown.

The "The Filter List has not been loaded" message displays if you have not yet downloaded the filter list or your subscription has expired.

Content on the Internet is constantly changing, so the content filter list should be updated on a weekly basis.

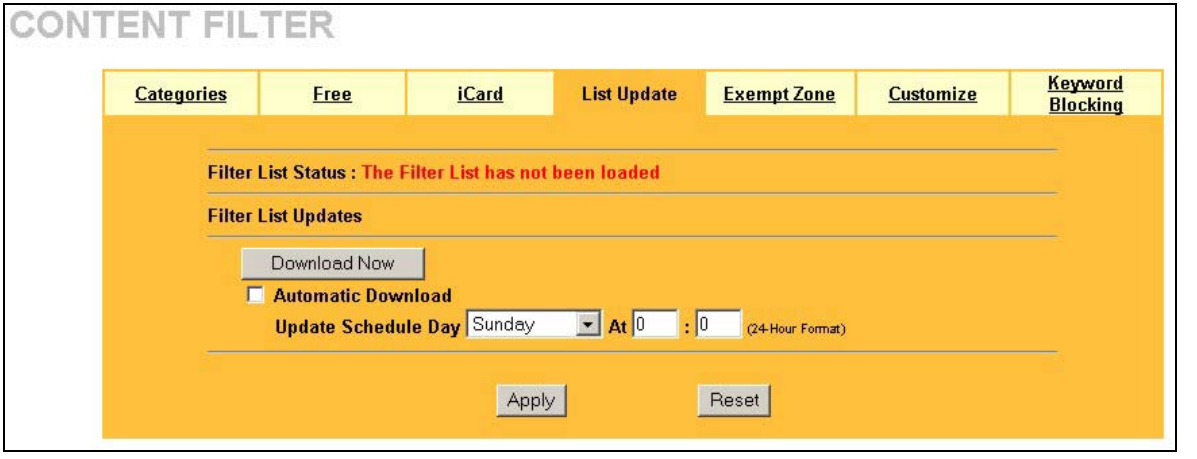


Figure 13-4 Content Filter: List Update

The following table describes the fields in this screen.

Table 13-4 Content Filter: List Update

LABEL	DESCRIPTION
Download Now	Click **Download Now** to download and install a new Content Filter List. This process may take a couple of minutes, depending on Internet traffic conditions and requires a current subscription to the Content Filter List. It is a good idea to download new lists when LAN access to the Internet is at a minimum.
Automatic Download	Select this check box to enable automatic weekly downloads of the Content Filter List.
Update Schedule Day	Select the day of the week, from the drop-down menu, that the new list should be retrieved. A current subscription to the Content Filter List updates is required.
At	Type the time in 24-hour format when the new Content Filter List should be retrieved. It is a good idea to choose a day and time when LAN traffic to the Internet is at a minimum.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

13.6 Configuring Exempt Computers

To include or exclude a range of users on the LAN from content filtering on your ZyWALL, click **CONTENT FILTER**, then the **Exempt Zone** tab. The screen appears as shown.

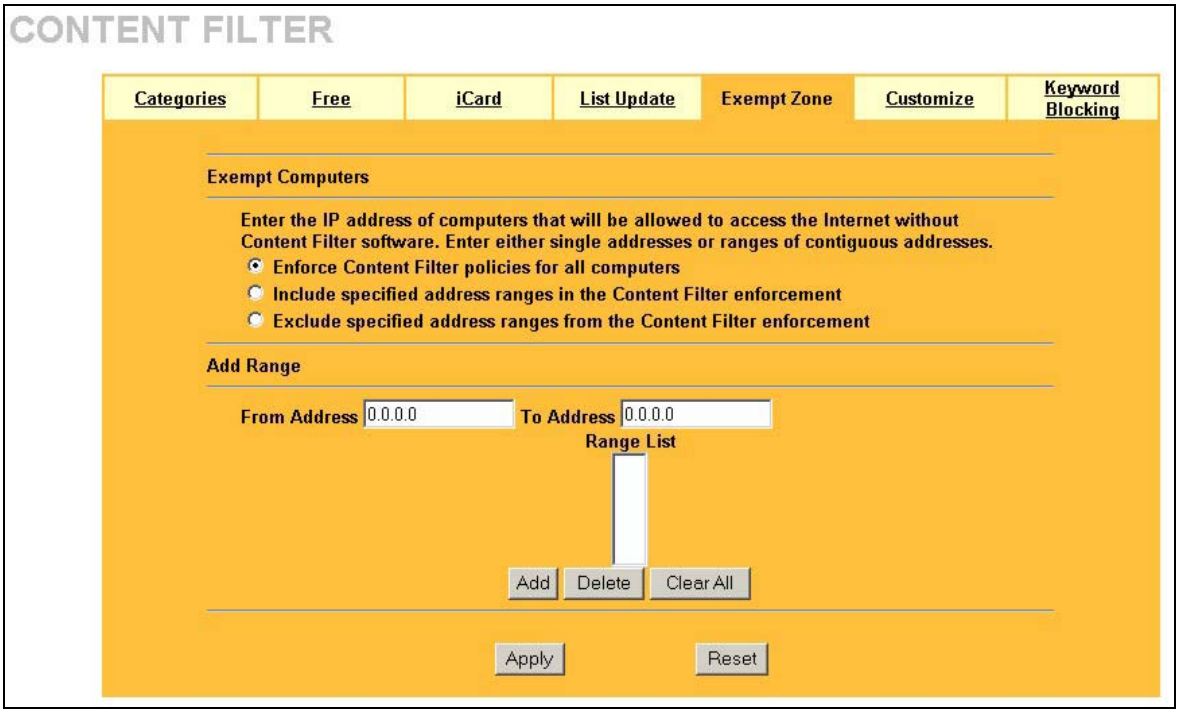


Figure 13-5 Content Filter: Exempt Zone

The following table describes the fields in this screen.

Table 13-5 Content Filter: Exempt Zone

LABEL	DESCRIPTION
Enforce Content Filter policies for all computers	Select to have all users on your LAN follow Content Filter policies (default).
Include specified address ranges in the Content Filter enforcement	Select to have a specific range of users on your LAN follow Content Filter policies.
Exclude specified address ranges from the Content Filter enforcement	Select to exempt a specific range of users on your LAN from Content Filter policies.
Add Range	Fill in the two fields below if you selected one of the last two options above.

Table 13-5 Content Filter: Exempt Zone

LABEL	DESCRIPTION
From Address	Type the beginning IP address of the specific range of users on your LAN.
To Address	Type the ending IP address of the specific range of users on your LAN, then click **Add Range**.
Add Range	Click **Add Range** after you have filled in the From Address and To Address fields above.
Delete Range	Click **Delete Range** after you select the range of addresses you wish to delete.
Clear All	Click **Clear All** to remove all of the IP addresses from the list.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

13.7 Configuring Customize

To customize the content filter list by adding or removing specific sites from the filter list on your ZyWALL, click **CONTENT FILTER**, then the **Customize** tab. The screen appears as shown.

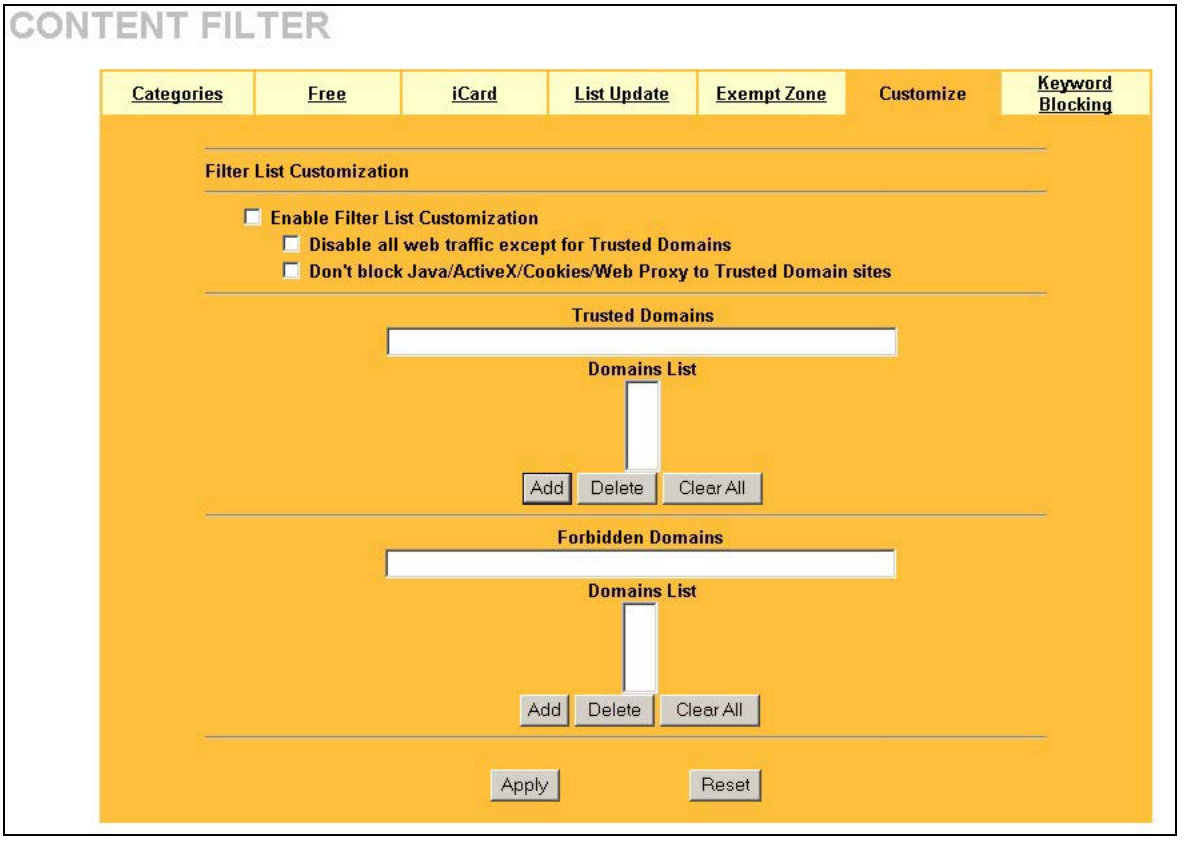


Figure 13-6 Content Filter: Customize

The following table describes the fields in this screen.

Table 13-6 Content Filter: Customize

LABEL	DESCRIPTION
Filter List Customization	Make sure the **Enable Filter List Customization** check box is selected to make this feature available. Add or remove sites from the Filter List to customize the Content Filter List.
Enable Filter List Customization	Select this check box to allow **Trusted Domain** web sites and block **Forbidden Domain** web sites. Content Filter List Customization may be enabled and disabled without re-entering all site names. Sites also do not have to be re-entered when the Content Filter List is updated each week.

Table 13-6 Content Filter: Customize

LABEL	DESCRIPTION
Disable all web traffic except for Trusted Domains	When this box is selected, ZyWALL only allows Web access to sites on the **Trusted Domains** list. If **Trusted Domains** are chosen carefully, this is the most effective way to block objectionable material.
Don't block Java/ActiveX/Cookies/Web Proxy to Trusted Domains sites	When this box is selected, ZyWALL will permit Java, ActiveX and Cookies from sites on the **Trusted Domains** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted.
Add or delete a Trusted Domain to the Content Filter List. Up to 256 entries are supported in this list.	
Trusted Domains	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.
Add	Click **Add Trusted Domain** when you have finished adding the host name in the text field above.
Delete	Select a domain name from the Trusted Domain list, and then click **Delete Trusted Domain** to delete it from that list.
Forbidden Domains Sites that are not objectionable (not in the Content Filter List), but are considered inappropriate may be blocked by adding them to the Forbidden Domains list. Up to 256 entries are supported in this list.	
Forbidden Domains	Enter its host name, 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.
Add	Click **Add Forbidden Domain** when you have finished adding the host name in the text field above.
Delete	Select a domain name from the **Forbidden Domain** list, and then click **Delete Forbidden Domain** to delete it from that list.
Clear All	Click **Clear All** to remove all of the domain names from the list.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

13.8 Configuring Keyword Blocking

Use this screen to block sites containing certain keywords. For example, if you enable the keyword "bad", the ZyWALL blocks all sites containing this keyword including the URL http://www.website.com/bad.html, even if it is not included in the Filter List. This functions as a second line of defense against objectionable material.

To block Web sites containing keywords in their URLs on your ZyWALL, click **CONTENT FILTER**, then the **Keyword Blocking** tab. The screen appears as shown.

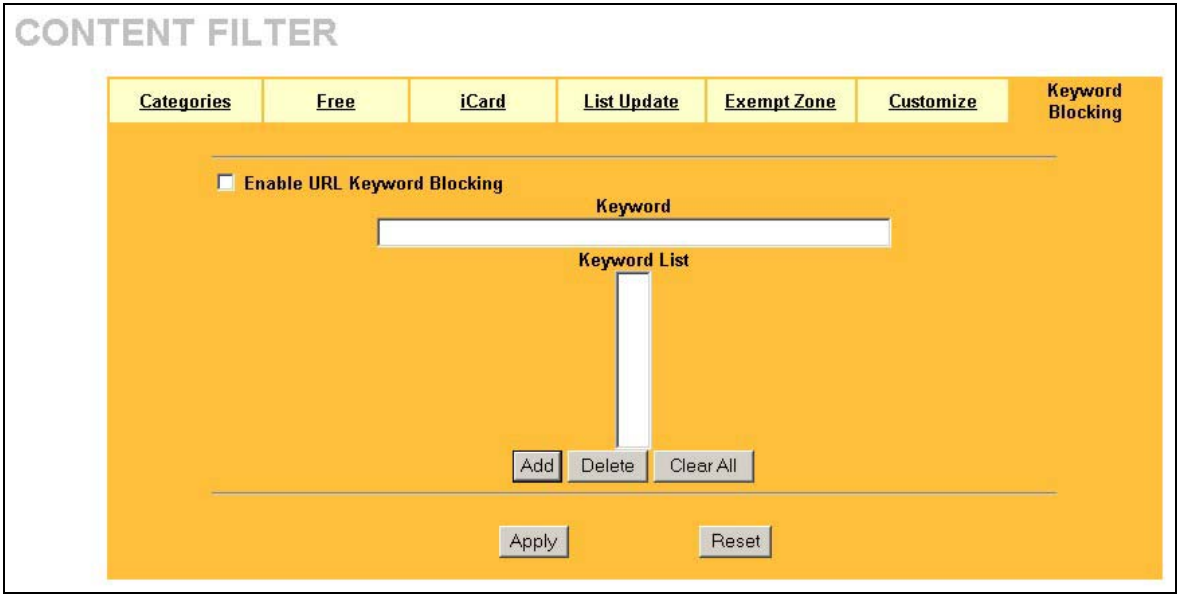


Figure 13-7 Content Filter: Keyword Blocking

The following table describes the fields in this screen.

Table 13-7 Content Filter: Keyword Blocking

LABEL	DESCRIPTION
Enable URL Keyword Blocking	Select this check box to enable this feature.
Keyword Blocking	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed.

Table 13-7 Content Filter: Keyword Blocking

LABEL	DESCRIPTION
Add	Click **Add Keyword** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the Content Filter is blocking this request.
Delete	Highlight a keyword in the lower box and click **Delete Keyword** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear All	Click **Clear All** to remove all of the domain names from the list.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

Part VI:

VPN/IPSec

This part provides information on how to configure VPN/IPSec.

Chapter 14
Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

14.1 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

14.1.1 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

14.1.2 Security Association

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

14.1.3 Other Terminology

- **Encryption**

  Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms “ciphertext” to plaintext. Decryption also requires a key.

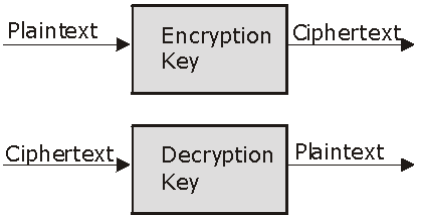


Figure 14-1 Encryption and Decryption

- **Data Confidentiality**

  The IPSec sender can encrypt packets before transmitting them across a network.

- **Data Integrity**

  The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

- **Data Origin Authentication**

  The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

14.1.4 VPN Applications

The ZyWALL supports the following VPN applications.

- **Linking Two or More Private Networks Together**

  Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- **Accessing Network Resources When NAT Is Enabled**

  When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

- **Unsupported IP Applications**

  A VPN tunnel may be created to add support for unsupported emerging IP applications.

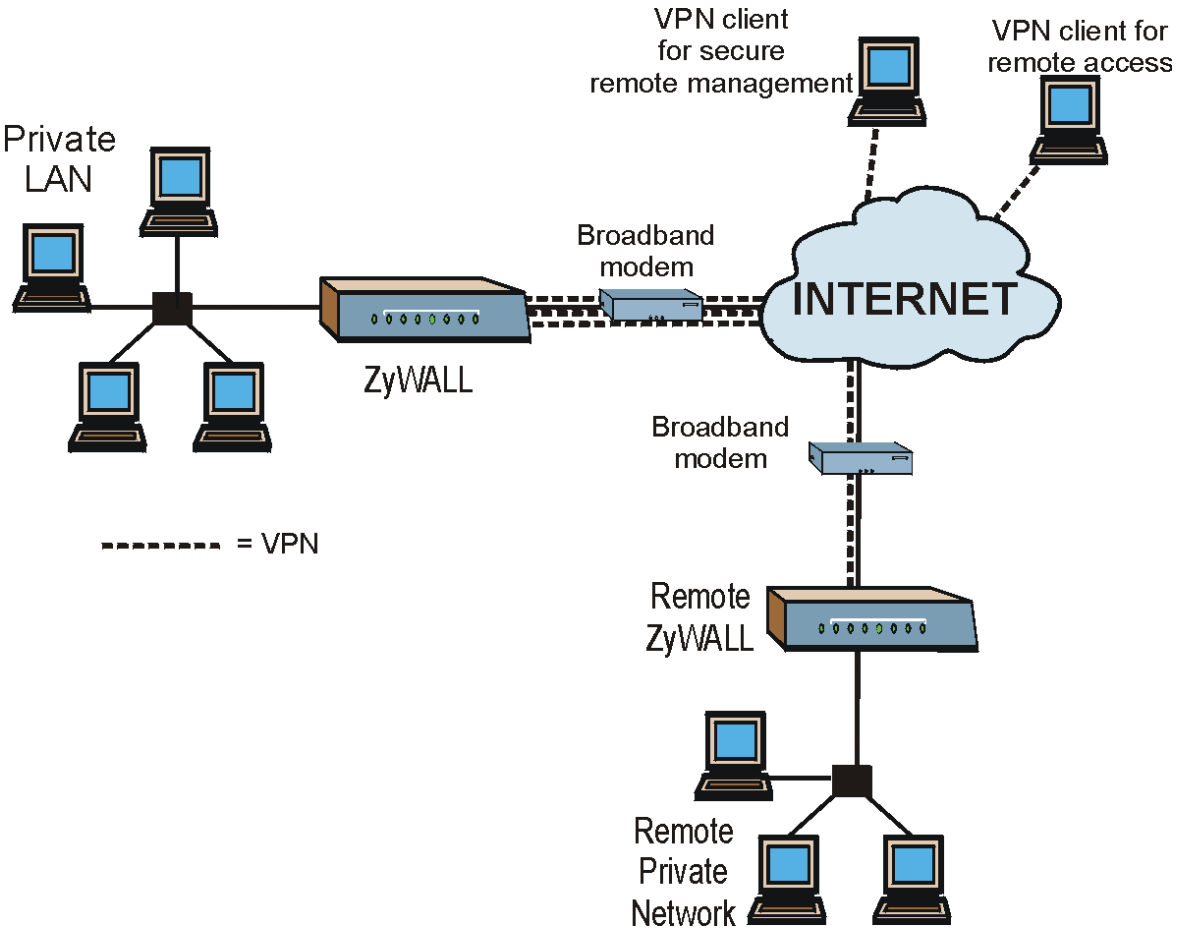


Figure 14-2 VPN Application

14.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

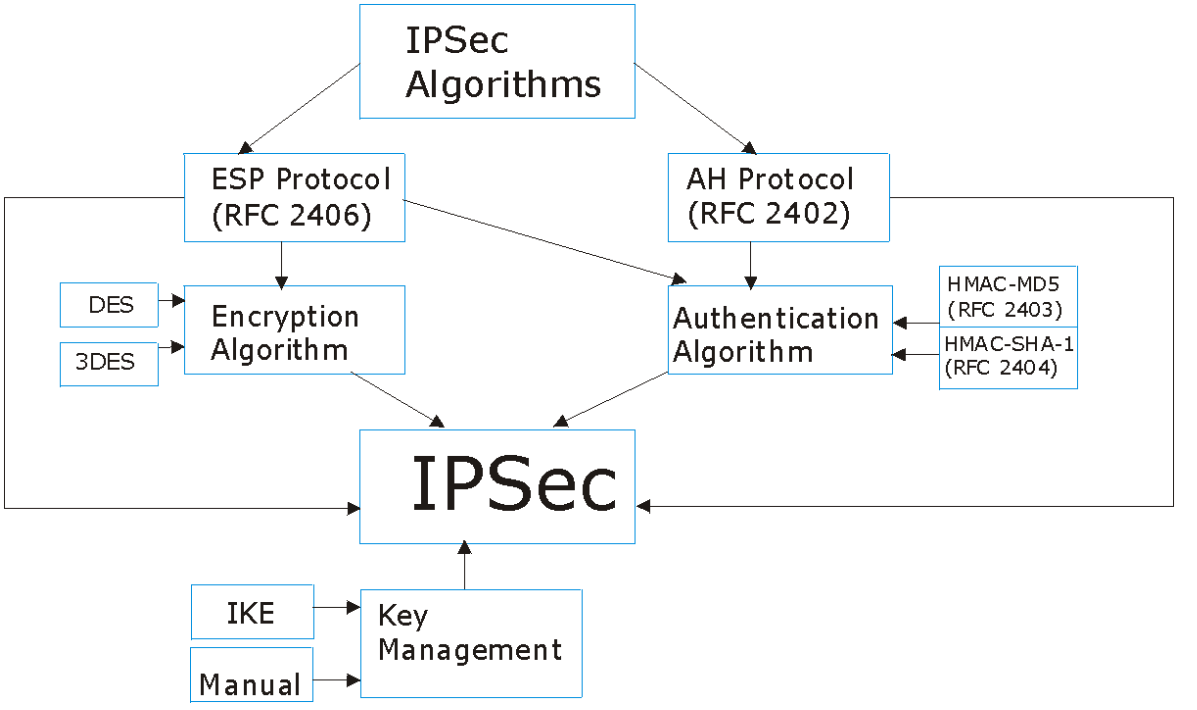


Figure 14-3 IPSec Architecture

14.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Please see *section 15.2* for more information.

14.2.2 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

14.3 Encapsulation

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

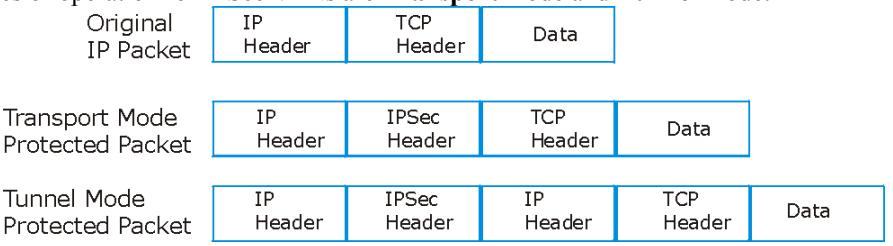


Figure 14-4 Transport and Tunnel Mode IPSec Encapsulation

14.3.1 Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP). With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

14.3.2 Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

14.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the ZyWALL.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (see *section 15.7* for details).

Table 14-1 VPN and NAT

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

Chapter 15
VPN Screens

This chapter introduces the VPN Web Configurator. See the Logs chapter for information on viewing logs and the Reference Guide for IPSec log descriptions.

15.1 VPN/IPSec Overview

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

15.2 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

15.2.1 AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.
In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

15.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.
An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 15-1 AH and ESP

ESP	AH
Select **DES** for minimal security and **3DES** for maximum. Select **NULL** to set up a tunnel without encryption.	Select **MD5** for minimal security and **SHA-1** for maximum security.
DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
Select **DES** for minimal security and **3DES** for maximum. Select **NULL** to set up a tunnel without encryption.	Select **MD5** for minimal security and **SHA-1** for maximum security.

15.3 My IP Address

My IP Address is the WAN IP address of the ZyWALL. If this field is configured as 0.0.0.0, then the ZyWALL will use the current ZyWALL WAN IP address (static or dynamic) to set up the VPN tunnel. The ZyWALL has to rebuild the VPN tunnel if the **My IP Address** changes after setup.

15.4 Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyWALL has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

15.4.1 Dynamic Secure Gateway Address

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful

for telecommuters initiating a VPN tunnel to the company network. See *section 15.17* for configuration examples.

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

15.5 Summary Screen

The following figure helps explain the main fields in the web configurator.

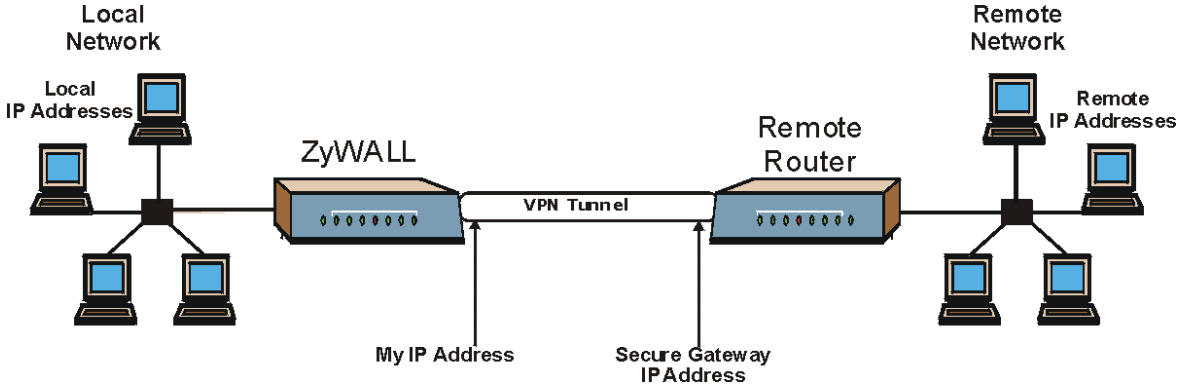


Figure 15-1 IPSec Summary Fields

Local and remote IP addresses must be static.

Click **VPN** to open the **Summary** screen. This is a read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then clicking **Edit** to configure the associated submenus.

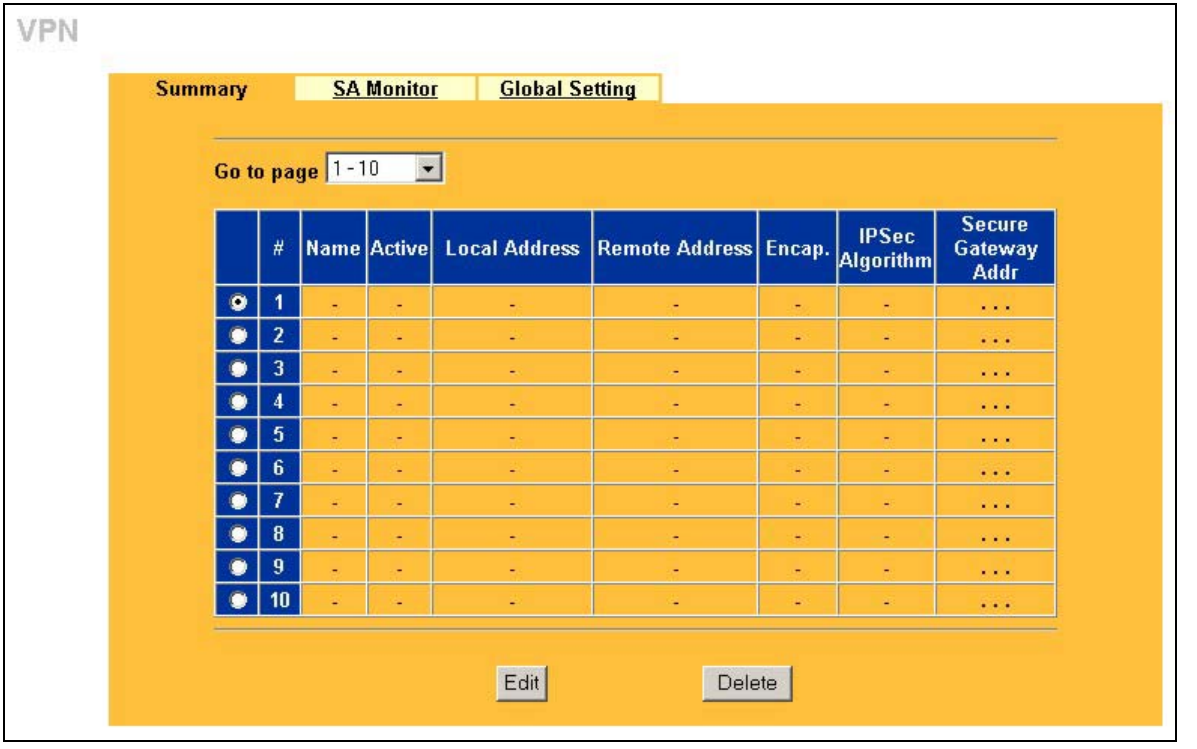


Figure 15-2 Summary

The following table describes the fields in this screen.

Table 15-2 Summary

LABEL	DESCRIPTION
#	The VPN policy index number
Name	This field displays the identification name for this VPN policy.
Active	This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active.

Table 15-2 Summary

LABEL	DESCRIPTION
Local Address	This is the IP address(es) of computer(s) on your local network behind your ZyWALL. The same (static) IP address is displayed twice when the **Local Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Single Address**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Range Address**. A (static) IP address and a subnet mask are displayed when the **Local Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Subnet Address**.
Remote Address	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router. This field displays **N/A** when the **Secure Gateway Addr** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. The same (static) IP address is displayed twice when the **Remote Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Single Address**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Range Address**. A (static) IP address and a subnet mask are displayed when the **Remote Address Type** field in the **Configure-IKE** (or **Manual**) screen is configured to **Subnet Address**.
Encap	This field displays **Tunnel** or **Transport** mode (Tunnel is the default selection).
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase ZyWALL processing requirements and communications latency (delay).
Secure Gateway Addr	This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway Addr** field in the **Configure-IKE** screen to **0.0.0.0.**
Select the radio button next to a VPN index number and then click **Edit** to edit a specific VPN policy. Click the radio button next to an empty VPN policy index number and then **Edit** to add a new VPN policy. Select the radio button next to a VPN policy number you want to delete and then click **Delete**. When a VPN policy is deleted, subsequent policies do not move up in the page list.	

15.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the ZyWALL automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see *section 15.11* for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an "always on" connection after you initiate it. Both IPSec routers must have a ZyWALL-compatible keep alive feature enabled in order for this feature to work.

If the ZyWALL has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the ZyWALL because the ZyWALL never drops the tunnels that are already connected. Check *Table 1-1 Model Specific Features* in chapter 1 to see how many simultaneous IPSec SAs your ZyWALL model can support.

When there is outbound traffic with no inbound traffic, the ZyWALL automatically drops the tunnel after two minutes.

15.7 NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.

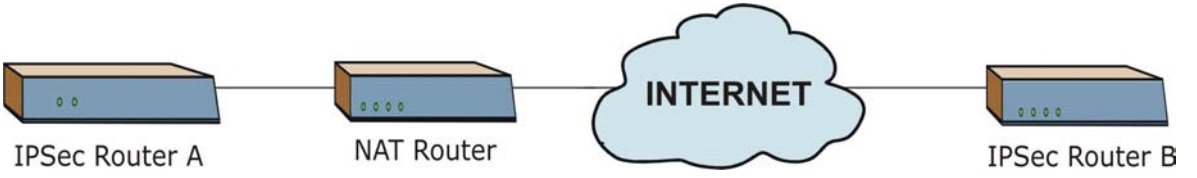


Figure 15-3 NAT Router Between IPSec Routers

Normally you cannot set up a VPN connection with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. In the previous figure, IPSec router A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the IPSec packet's header so it does not match the header for which IPSec router B is checking. Therefore, IPSec router B does not respond and the VPN connection cannot be built.

NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. IPSec router B checks the UDP port 500 header and responds. IPSec routers A and B build a VPN connection.

15.7.1 NAT Traversal Configuration

For NAT traversal to work you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.

- Enable NAT traversal on both IPSec endpoints.

In order for IPSec router A (see the figure) to receive an initiating IPSec packet from IPSec router B, set the NAT router to forward UDP port 500 to IPSec router A.

15.8 ID Type and Content

With aggressive negotiation mode (see *section 15.11.1*), the ZyWALL identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyWALL to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyWALL from IPSec routers with dynamic IP addresses (see *section 15.17.2* for a telecommuter configuration example).

With main mode (see *section 15.11.1*), the ID type and content are encrypted to provide identity protection. In this case the ZyWALL can only distinguish between up to eight different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyWALL can distinguish up to eight incoming SAs because you can select between two encryption algorithms (DES and 3DES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see *section 15.12*). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 15-3 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer or leave the field blank to have the ZyWALL automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyWALL.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyWALL.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

Table 15-4 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyWALL automatically use the address in the **Secure Gateway** field.

Table 15-4 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Addr** field below.	

15.8.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel. The two ZyWALLs in this example can complete negotiation and establish a VPN tunnel.

Table 15-5 Matching ID Type and Content Configuration Example

ZYWALL A	ZYWALL B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two ZyWALLs in this example cannot complete their negotiation because ZyWALL B's **Local ID type** is **IP**, but ZyWALL A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 15-6 Mismatching ID Type and Content Configuration Example

ZYWALL A	ZYWALL B
Local ID type: IP	**Local ID type: IP**
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

15.9 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see *section 15.11* for more on IKE phases). It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

15.10 Editing VPN Policies

Click **Edit** on the **Summary** screen to edit VPN policies.

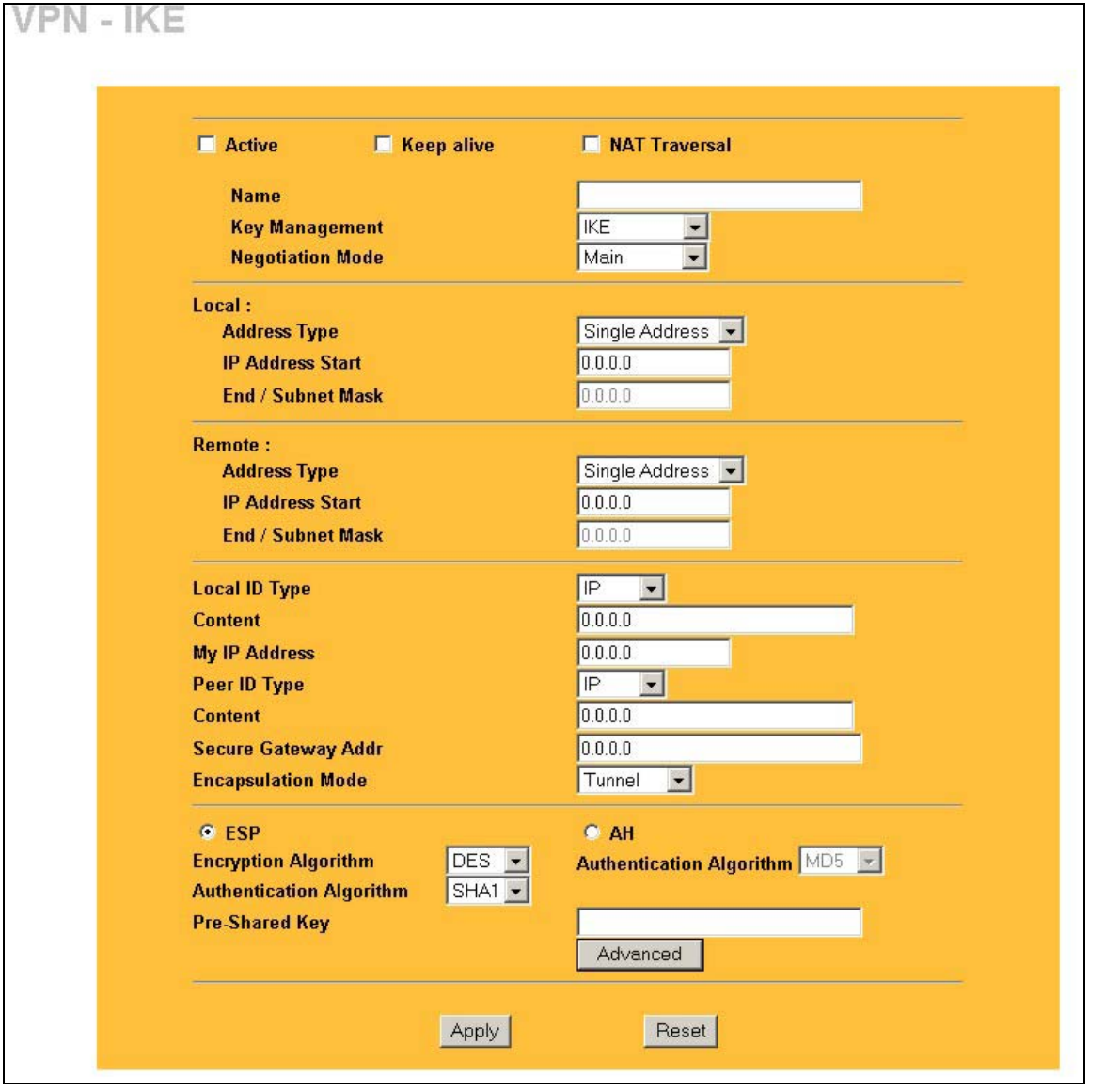


Figure 15-4 VPN IKE

The following table describes the fields in this screen.

Table 15-7 VPN IKE

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select either **Yes** or **No** from the drop-down list box. Select **Yes** to have the ZyWALL automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
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. The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Key Management	Select **IKE** or **Manual Key** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual Key** is a useful option for troubleshooting.
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Use the drop-down menu to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your ZyWALL.

Table 15-7 VPN IKE

LABEL	DESCRIPTION
End/ Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your ZyWALL.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway Addr** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Use the drop-down menu to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router.
End / Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router.
Local ID Type	Select **IP** to identify this ZyWALL by its IP address. Select **DNS** to identify this ZyWALL by a domain name. Select **E-mail** to identify this ZyWALL by an e-mail address.

Table 15-7 VPN IKE

LABEL	DESCRIPTION
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The ZyWALL automatically uses the IP address in the **My IP Address** field (refer to the My IP Address field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. ➢ When there is a NAT router between the two IPSec routers. ➢ When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyWALL in the local Content field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
My IP Address	Enter the WAN IP address of your ZyWALL. The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. The VPN tunnel has to be rebuilt if this IP address changes.
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.

Table 15-7 VPN IKE

LABEL	DESCRIPTION
Content	When you select **IP** in the **Peer ID Type** field, type the IP address of the computer with which you will make the VPN connection in the peer **Content** field. The ZyWALL automatically uses the address in the **Secure Gateway Addr** field (refer to the **Secure Gateway Addr** field description) if you configure the peer **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the peer **Content** field or use the **DNS** or **E-mail** ID type in the following situations. ➢ When there is a NAT router between the two IPSec routers. ➢ When you want the ZyWALL to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Peer ID Type** field, type a domain name or e-mail address by which to identify the remote IPSec router in the peer **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Secure Gateway Addr.	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**).
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
ESP	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select ESP here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. 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. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.

Table 15-7 VPN IKE

LABEL	DESCRIPTION
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **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 **SHA-1** for maximum security.
AH	Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described below).
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **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 **SHA-1** for maximum security.
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. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. 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.
Advanced	Click **Advanced** to configure more detailed settings of your IKE key management.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

15.11 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

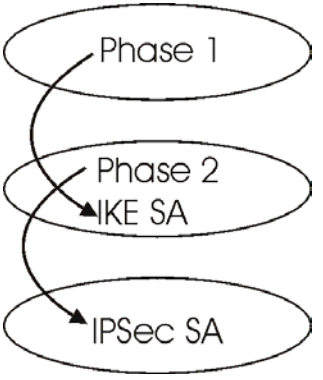


Figure 15-5 Two Phases to Set Up the IPSec SA

In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see *section 15.11.3*. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyWALL automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyWALL also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

15.11.1 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

15.11.2 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

15.11.3 Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.
This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the ZyWALL. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

15.12 Configuring Advanced IKE Settings

Select **Advanced** at the bottom of the **VPN IKE** screen. This is the **VPN IKE- Advanced** screen as shown next.

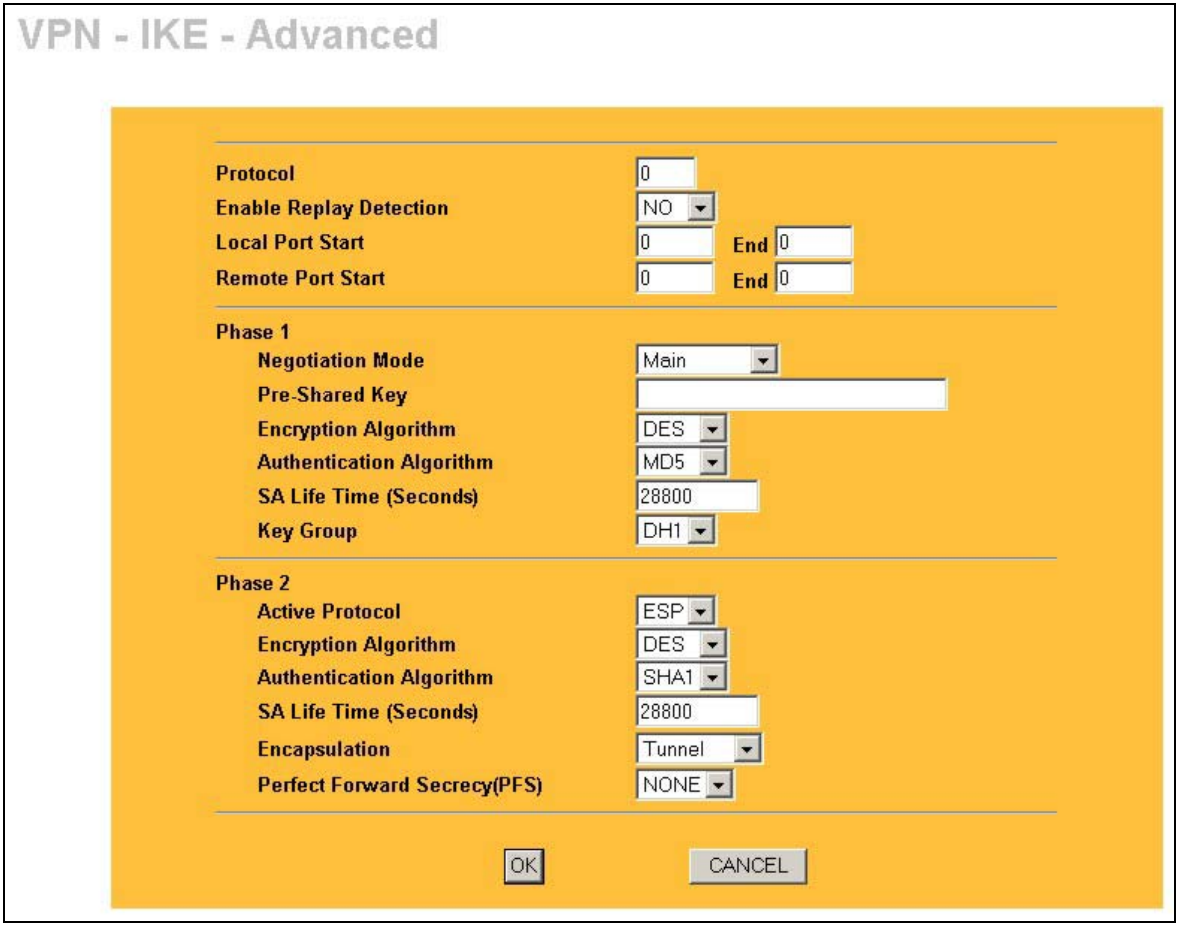


Figure 15-6 VPN IKE: Advanced

The following table describes the fields in this screen.

Table 15-8 VPN IKE: Advanced

LABEL	DESCRIPTION
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.

Table 15-8 VPN IKE: Advanced

LABEL	DESCRIPTION
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select **YES** from the drop-down menu to enable replay detection, or select **NO** to disable it.
Local Port Start	"0" is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Local Port End	Type a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Local Port Start** is left at 0, **Local Port End** will also remain at 0.
Remote Port Start	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Remote Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Remote Port Start is** left at 0, **Remote Port End** will also remain at 0.
Phase 1	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
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. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. 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.

Table 15-8 VPN IKE: Advanced

LABEL	DESCRIPTION
Encryption Algorithm	Select **DES** or **3DES** from the drop-down list box. 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.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **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 **SHA-1** for maximum security.
SA Life Time (seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). 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.
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.
Phase 2	
Active Protocol	Use the drop-down list box to choose from **ESP** or **AH**.
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. 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. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **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 **SHA-1** for maximum security.

Table 15-8 VPN IKE: Advanced

LABEL	DESCRIPTION
SA Life Time (seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). 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.
Encapsulation	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose **DH1** or **DH2** from the drop-down list box 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 (more secure, yet slower).
OK	Click **OK** to save your changes back to the ZyWALL and return to the **Configure-IKE** screen.
CANCEL	Click **CANCEL** to return to the **Configure-IKE** screen without saving your changes.

15.13 Manual Key Setup

Manual key management is useful if you have problems with **IKE** key management.

15.13.1 Security Parameter Index (SPI)

An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

15.14 Configuring Manual Key

You only configure **VPN Manual Key** when you select **Manual** in the **Key Management** field on the **VPN IKE** screen. This is the **VPN Manual Key** screen as shown next.

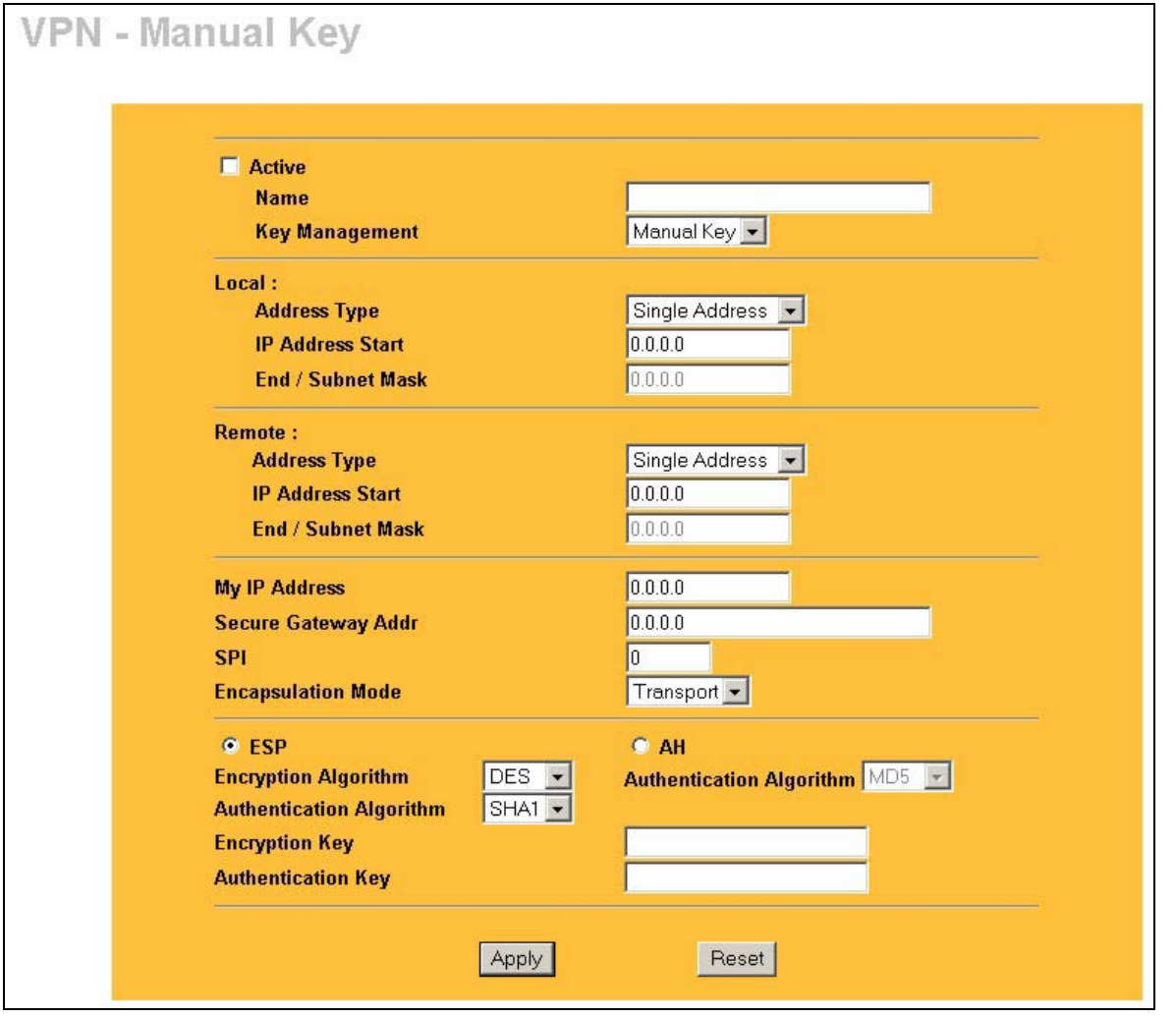


Figure 15-7 Manual Setup

The following table describes the fields in this screen.

Table 15-9 VPN Manual Setup

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN policy.

Table 15-9 VPN Manual Setup

LABEL	DESCRIPTION
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Key Management	Select **IKE** or **Manual Key** from the drop-down list box. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Local IP Address Start	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your ZyWALL.
Local End/Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your ZyWALL.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Remote IP	When the **Address Type** field is configured to **Single Address**, enter a (static) IP

Table 15-9 VPN Manual Setup

LABEL	DESCRIPTION
Address Start	address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router.
Remote End/ Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router.
My IP Address	Enter the WAN IP address of your ZyWALL. The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. The VPN tunnel has to be rebuilt if this IP address changes.
Secure Gateway Addr	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
SPI	Type a unique **SPI** from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9".
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
ESP	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select ESP here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next).
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. 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. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **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 **SHA-1** for maximum security.

Table 15-9 VPN Manual Setup

LABEL	DESCRIPTION
AH	Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described next).
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **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 **SHA-1** for maximum security.
Encryption Key (Only with ESP)	With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

15.15 Viewing SA Monitor

In the web configurator, click **VPN** and the **SA Monitor** tab. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See *section 15.6* on keep alive to have the ZyWALL renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

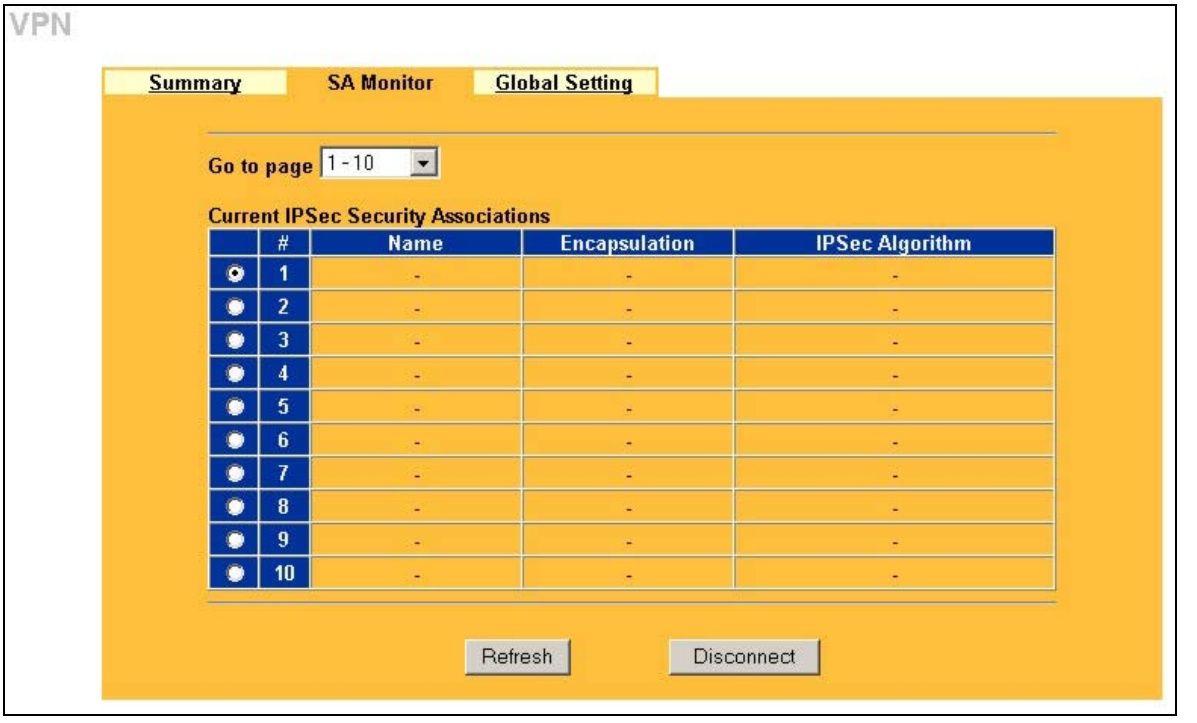


Figure 15-8 SA Monitor

The following table describes the fields in this screen.

Table 15-10 SA Monitor

LABEL	DESCRIPTION
Go to page	Choose the range of rules from the drop-down list box to display the summary page for the selected rules. Not all ZyWALL models have this **Go to page** feature.
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays Tunnel or Transport mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase ZyWALL processing requirements and communications latency (delay).

Table 15-10 SA Monitor

LABEL	DESCRIPTION
Previous Page (if applicable)	Click **Previous Page** to view more items in the summary (not all ZyWALL models have this feature).
Refresh	Click **Refresh** to display the current active VPN connection(s).
Disconnect	Select a security association index number that you want to disconnect and then click **Disconnect**.
Next Page	Click **Next Page** to view more items in the summary (not all ZyWALL models have this feature).

15.16 Configuring Global Setting

To change your ZyWALL's Global Settings, click **VPN**, then the **Global Setting** tab. The screen appears as shown.

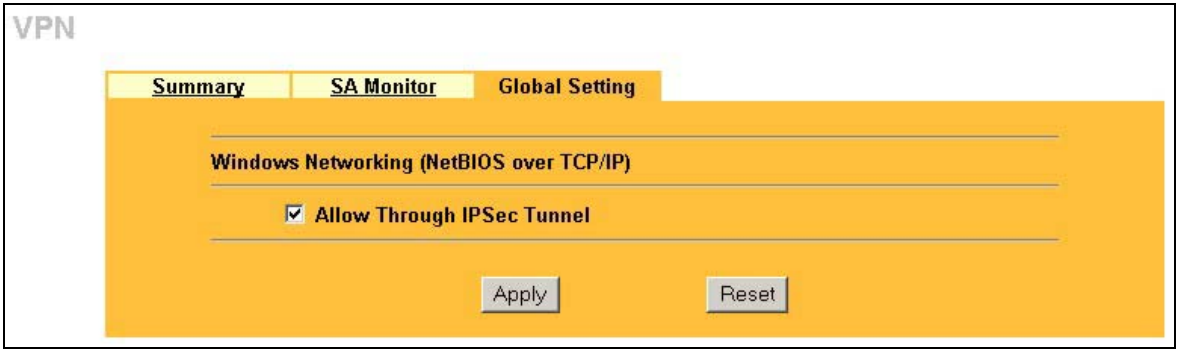


Figure 15-9 Global Setting

The following table describes the fields in this screen.

Table 15-11 SA Monitor

LABEL	DESCRIPTION
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.

Table 15-11 SA Monitor

LABEL	DESCRIPTION
Allow Through IP/Sec Tunnel	Select this check box to send NetBIOS packets through the VPN connection.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

15.17 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyWALL at headquarters from remote IPSec routers that use dynamic WAN IP addresses.

15.17.1 Telecommuters Sharing One VPN Rule Example

Multiple telecommuters can use one VPN rule to simultaneously access a ZyWALL at headquarters. They must all use the same IPSec parameters (including the pre-shared key) but the local IP addresses (or ranges of addresses) cannot overlap. See the following table and figure for an example.

Having everyone use the same pre-shared key may create a vulnerability. If the pre-shared key is compromised, all of the VPN connections using that VPN rule are at risk. A recommended alternative is to use a different VPN rule for each telecommuter and identify them by unique IDs (see *section 15.17.2* for an example)

Table 15-12 Telecommuter and Headquarters Configuration Example

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

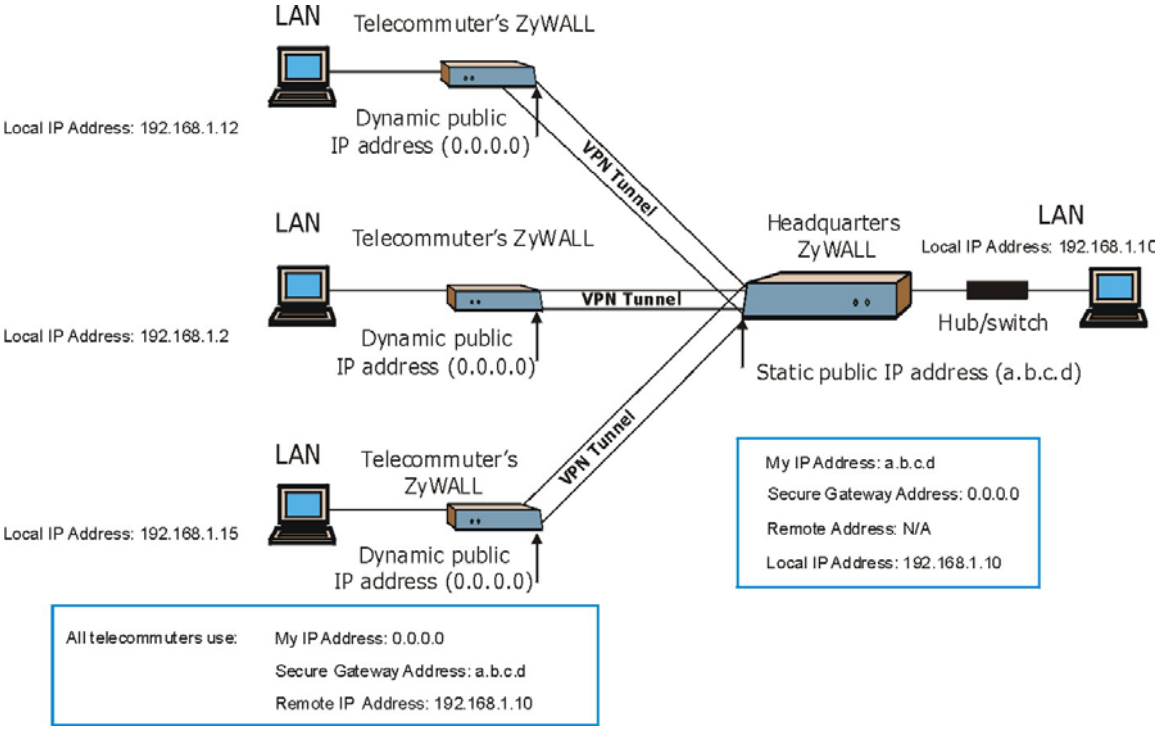


Figure 15-10 Telecommuters Sharing One VPN Rule Example

15.17.2 Telecommuters Using Unique VPN Rules Example

With aggressive negotiation mode (see *section 15.11.1*), the ZyWALL can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyWALL at headquarters. They can use different IPSec parameters (including the pre-shared key) and the local IP addresses (or ranges of addresses) can overlap.

See the following graphic for an example where three telecommuters each use a different VPN rule to initiate a VPN connection to a ZyWALL located at headquarters. The ZyWALL at headquarters identifies each by its ID type and contents and uses the appropriate VPN rule to establish the VPN connection.

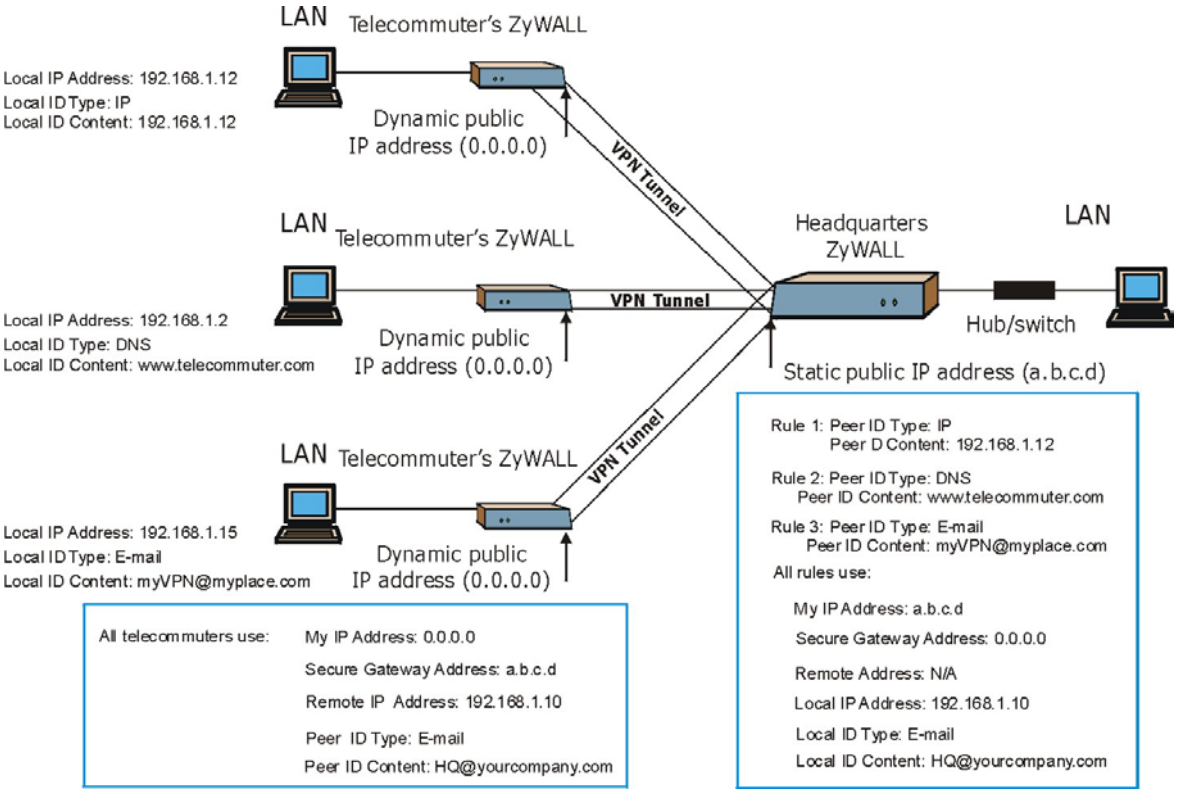


Figure 15-11 Telecommuters Using Unique VPN Rules Example

15.18 VPN and Remote Management

If a VPN tunnel uses a remote management service port (Telnet, FTP, WWW SNMP, DNS or ICMP) and terminates at the ZyWALL's LAN or WAN port, configure remote management (**REMOTE MGNT**) to allow access for that service.

If the VPN tunnel terminates at the ZyWALL's LAN IP address, configure remote management for **LAN** or **WAN** server access (or **LAN & WAN** or **LAN & WAN & DMZ** depending on your ZyWALL model).

If the VPN tunnel terminates at the ZyWALL's WAN IP address, configure remote management for **WAN** server access (or **LAN & WAN** or **LAN & WAN & DMZ** depending on your ZyWALL model).

Part VII:

Remote Management and UPnP

This part provides information and configuration instructions for remote management and Universal Plug and Play.

Chapter 16
Remote Management Screens

This chapter provides information on the Remote Management screens.

16.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyWALL interface (if any) from which computers.

When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

You may manage your ZyWALL from a remote location via:

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

When you Choose WAN only **or** ALL **(LAN & WAN), you still need to configure a firewall rule to allow access.**

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

16.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in one of the remote management screens.

3. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
6. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

16.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyWALL's WAN IP address when configuring from the WAN.
- Use the ZyWALL's LAN IP address when configuring from the LAN.

16.1.3 System Timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or telnet/web/FTP connections. Your ZyWALL automatically logs you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

16.2 Telnet

You can configure your ZyWALL for remote Telnet access as shown next.

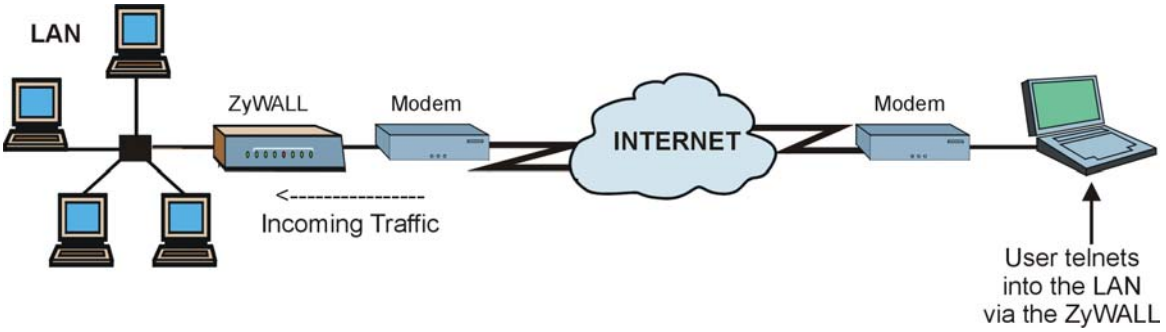


Figure 16-1 Telnet Configuration on a TCP/IP Network

16.3 Configuring TELNET

Click **REMOTE MANAGEMENT** to open the **TELNET** screen.

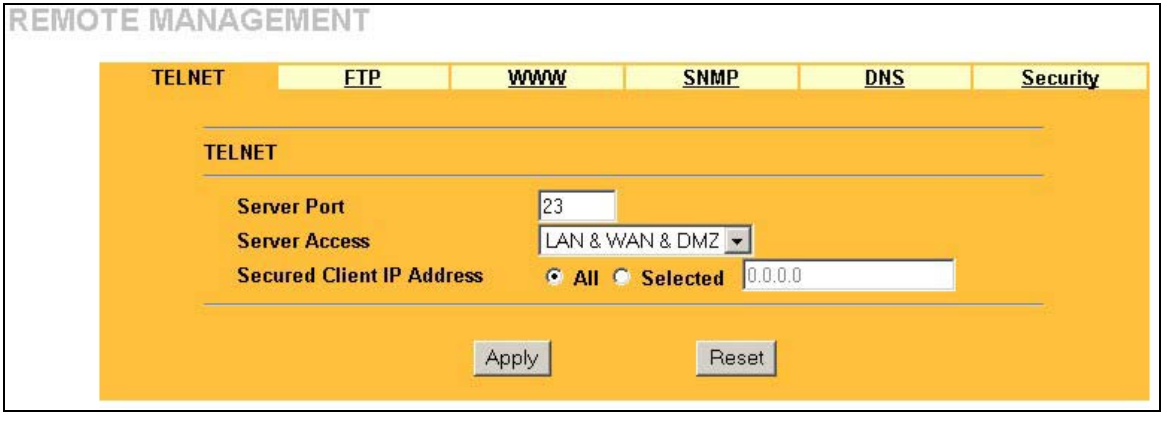


Figure 16-2 Telnet

The following table describes the fields in this screen.

Table 16-1 Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

16.4 Configuring FTP

You can upload and download the ZyWALL’s firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyWALL’s FTP settings, click **REMOTE MANAGEMENT**, then the **FTP** tab. The screen appears as shown.

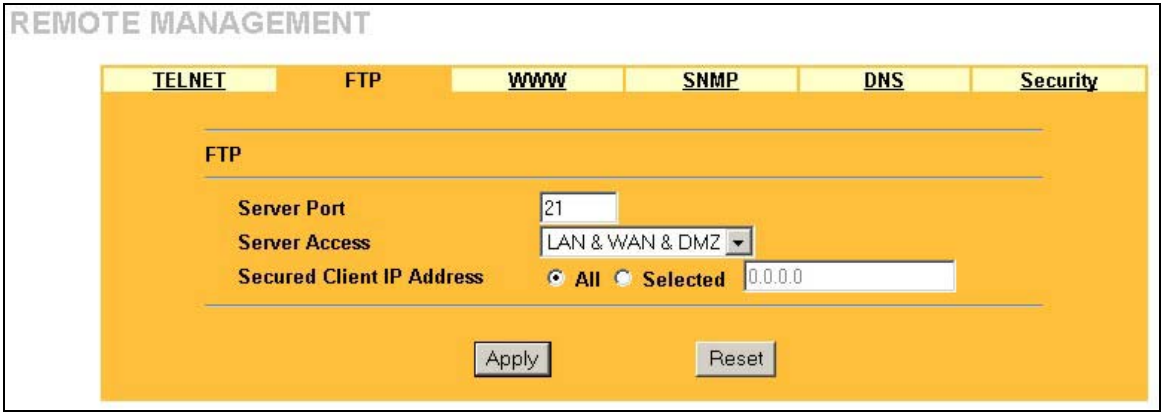


Figure 16-3 FTP

The following table describes the fields in this screen.

Table 16-2 FTP

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

16.5 Configuring WWW

To change your ZyWALL's World Wide Web settings, click **REMOTE MANAGEMENT**, then the **WWW** tab. The screen appears as shown.

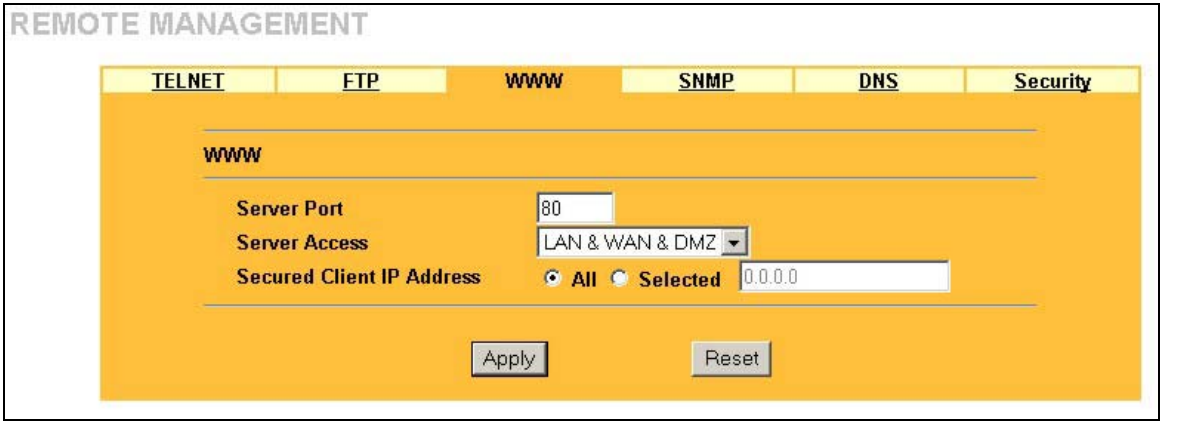


Figure 16-4 WWW

The following table describes the fields in this screen.

Table 16-3 WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

16.6 Configuring SNMP

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

SNMP is only available if TCP/IP is configured.

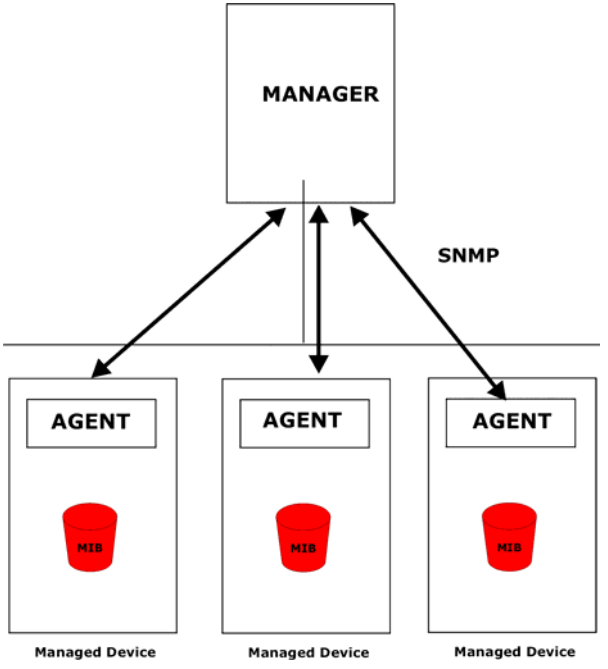


Figure 16-5 SNMP Management Model

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.

16.6.1 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.

16.6.2 SNMP Traps

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

Table 16-4 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).

Table 16-4 SNMP Traps

4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

16.6.3 REMOTE MANAGEMENT: SNMP

To change your ZyWALL's SNMP settings, click **REMOTE MANAGEMENT**, then the **SNMP** tab. The screen appears as shown.

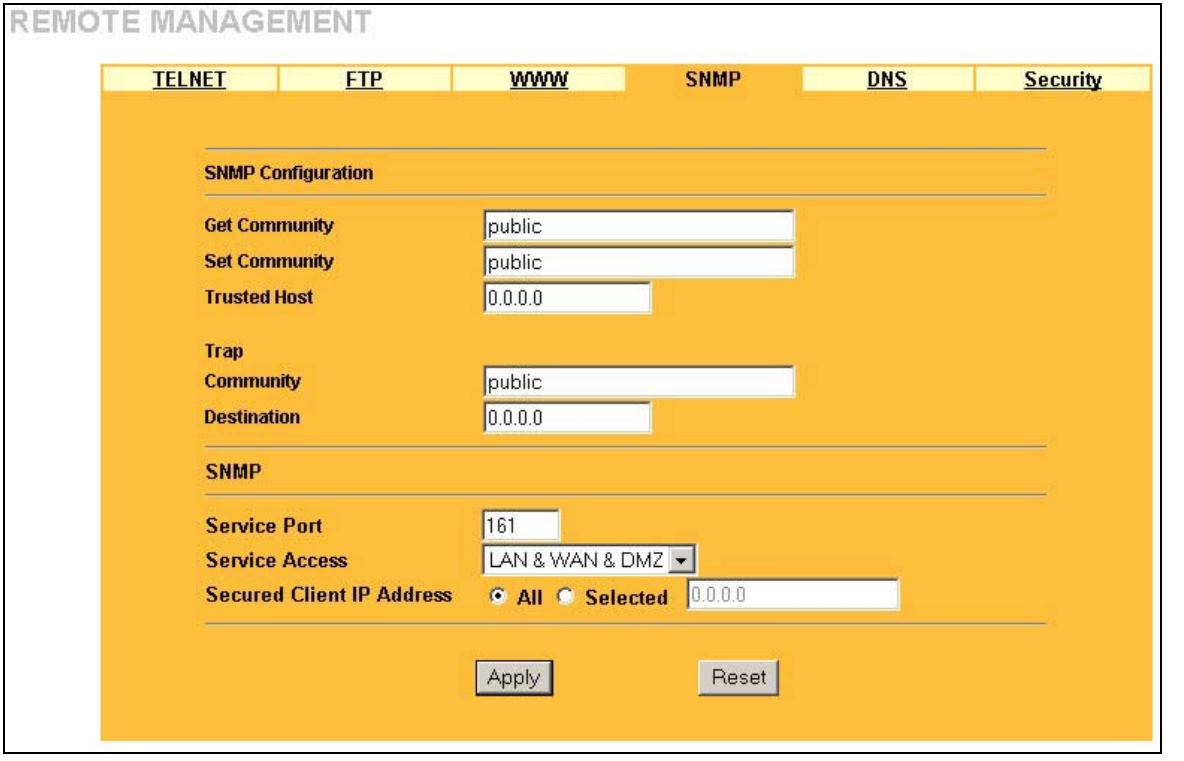


Figure 16-6 SNMP

The following table describes the fields in this screen.

Table 16-5 SNMP

LABEL	DESCRIPTION
SNMP Configuration	
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 public and allows all requests.

Table 16-5 SNMP

LABEL	DESCRIPTION
Trusted Host	If you enter a trusted host, your ZyWALL will only respond to SNMP messages from this address. 0.0.0.0 (default) means your ZyWALL will respond to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

16.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for example, the IP address of www.zyxel.com is 204.217.0.2. Refer to the *Internet Access* chapter for more information.

To change your ZyWALL’s DNS settings, click **REMOTE MANAGEMENT**, then the **DNS** tab. The screen appears as shown.

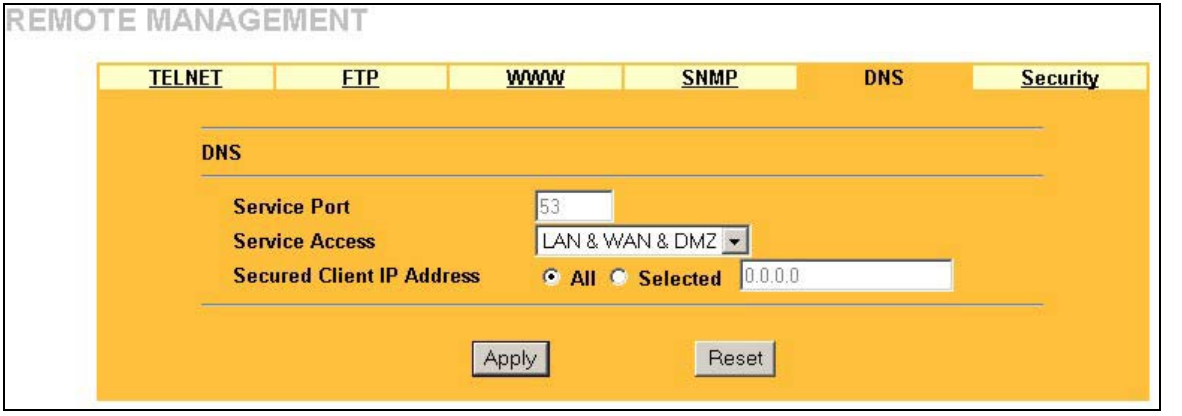


Figure 16-7 DNS

The following table describes the fields in this screen.

Table 16-6 DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the ZyWALL.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send DNS queries to the ZyWALL. Select **All** to allow any computer to send DNS queries to the ZyWALL. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the ZyWALL.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

16.8 Configuring Security

To change your ZyWALL’s Security settings, click **REMOTE MANAGEMENT**, then the **Security** tab. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your ZyWALL, an ICMP response packet is automatically returned. This allows the outside user to know the ZyWALL exists. The ZyWALL series support anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyWALL when unsupported ports are probed.

Figure 16-8 Security

The following table describes the fields in this screen.

Table 16-7 Security

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyWALL will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests**.** Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** (**& DMZ** if your ZyWALL has a DMZ port) to reply to both incoming LAN and WAN (and DMZ if present) Ping requests.

Table 16-7 Security

LABEL	DESCRIPTION
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the ZyWALL by probing for unused ports. If you select this option, the ZyWALL will not send ICMP response packets to port request(s) for unused ports, thus leaving the unused ports and the ZyWALL unseen. If the firewall blocks a packet from the WAN, the ZyWALL sends a TCP reset packet. Use the "sys firewall tcprst rst off" command in the command interpreter if you want to stop the ZyWALL from sending TCP reset packets.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 17
UPnP

This chapter introduces the Universal Plug and Play feature.

17.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

17.1.1 How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

17.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the *SUA/NAT* chapter for further information about NAT.

17.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

17.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

UPnP broadcasts are only allowed on the LAN.

Please see later in this *User's Guide* for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

17.3 Configuring UPnP

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

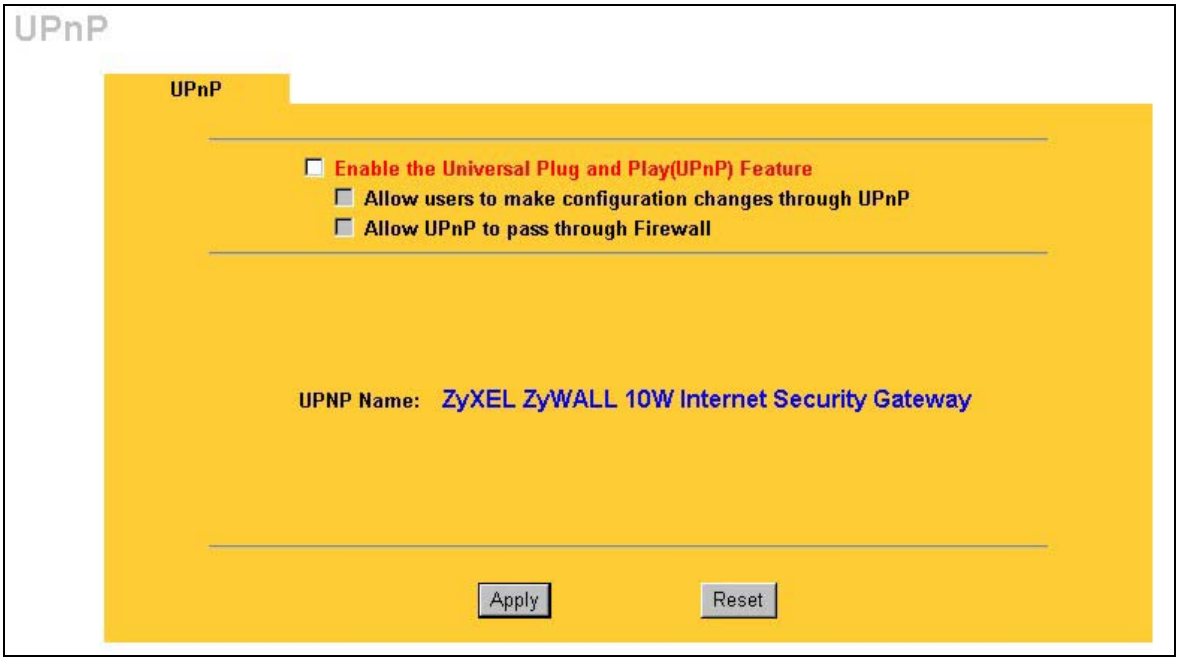


Figure 17-1 Configuring UPnP

The following table describes the fields in this screen.

Table 17-1 Configuring UPnP

FIELD	DESCRIPTION
Enable the Universal Plug and Play (UPnP) feature	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyWALL's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyWALL so that they can communicate through the ZyWALL, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Table 17-1 Configuring UPnP

FIELD	DESCRIPTION
Allow UPnP to pass through firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
UPNP Name	This identifies the ZyXEL device in UPnP applications.
Click **Apply** to save your changes back to the ZyWALL. Click **Reset** to begin configuring this screen afresh.	

17.4 Installing UPnP in Windows Example

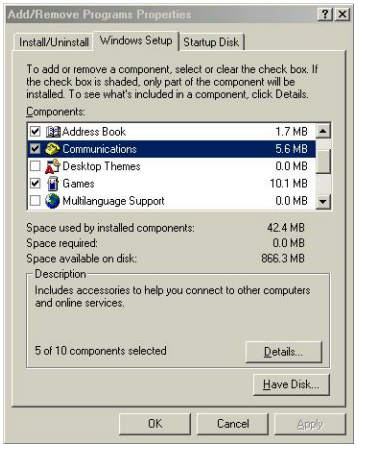
This section shows how to install UPnP in Windows Me and Windows XP.

17.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

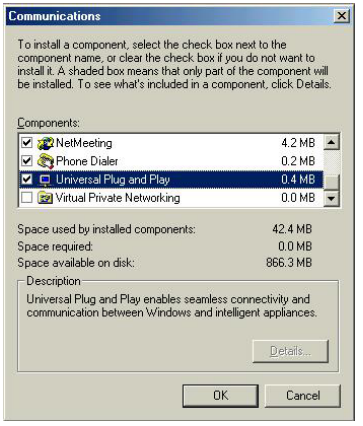
Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

Restart the computer when prompted.



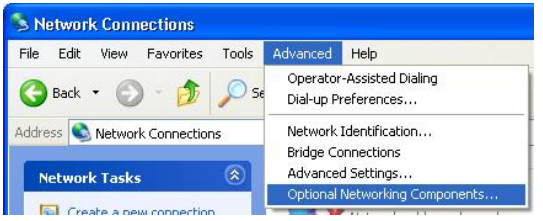
17.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

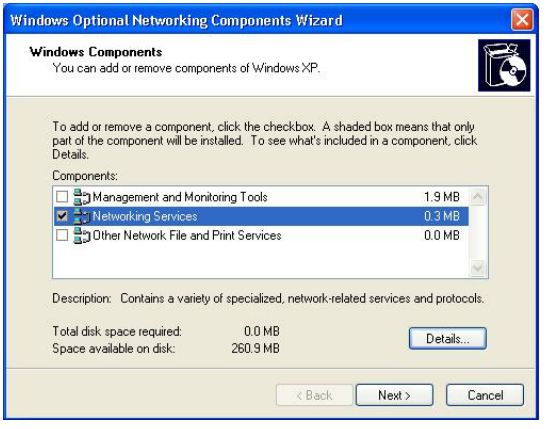
Step 1. Click **start** and **Control Panel**.

Double-click **Network Connections**.

In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**
The **Windows Optional Networking Components Wizard** window displays.

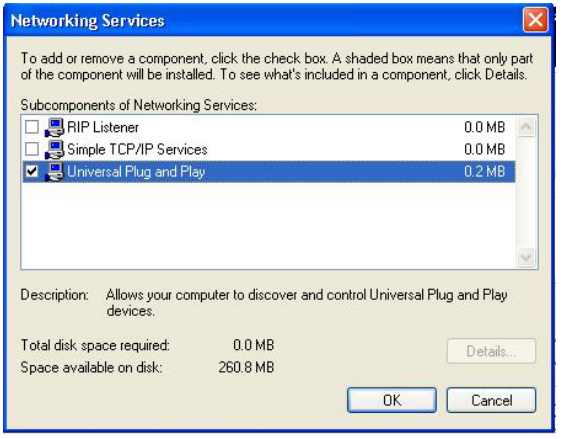


Select **Networking Service** in the **Components** selection box and click **Details**.



In the **Networking Services** window, select the **Universal Plug and Play** check box.

Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.



17.5 Using UPnP in Windows XP Example

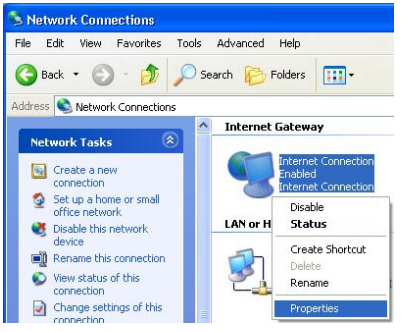
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

Make sure the computer is connected to a LAN port of the ZyXEL device. Turn on your computer and the ZyXEL device.

17.5.1 Auto-discover Your UPnP-enabled Network Device

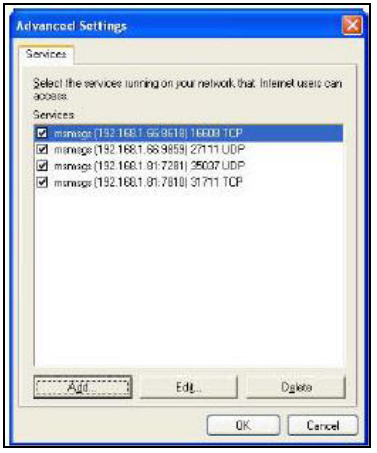
Step 1. Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

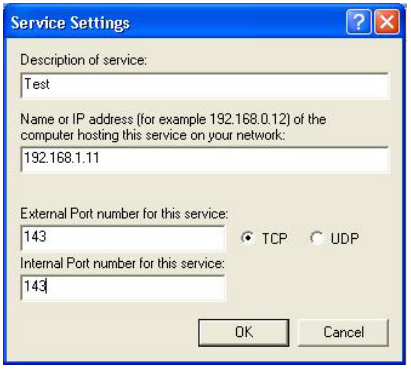
Step 2. Right-click the icon and select **Properties**.



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

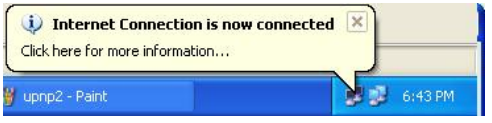
You may edit or delete the port mappings or click **Add** to manually add port mappings.



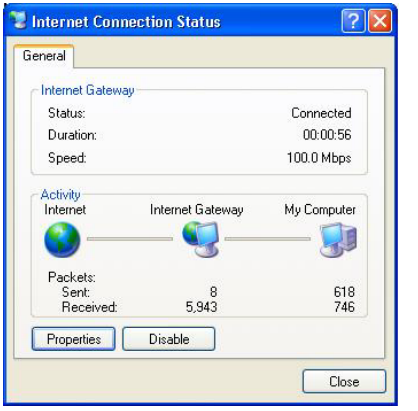


When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray



Double-click the icon to display your current Internet connection status.



17.5.2 Web Configurator Easy Access

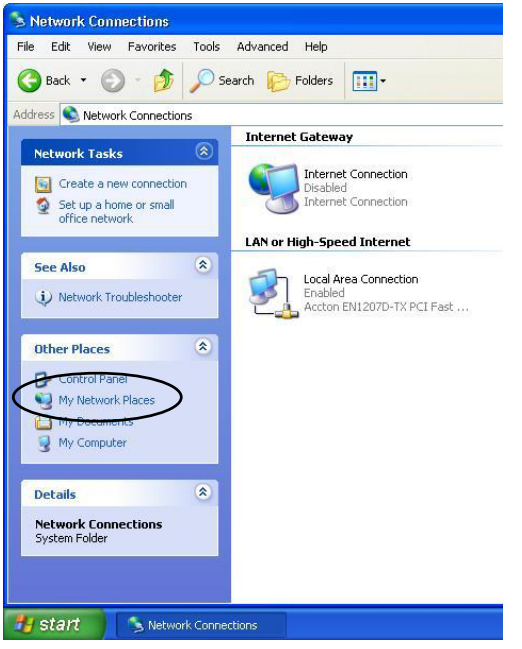
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

Step 1. Click **start** and then **Control Panel**.

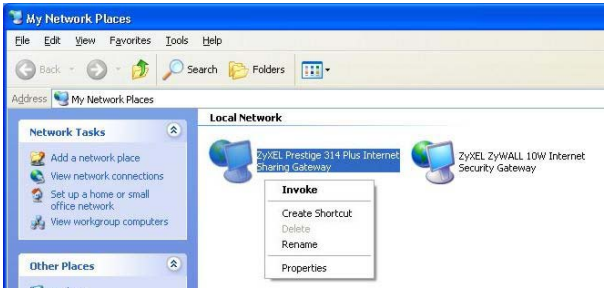
Double-click **Network Connections**.

Select **My Network Places** under **Other Places**.

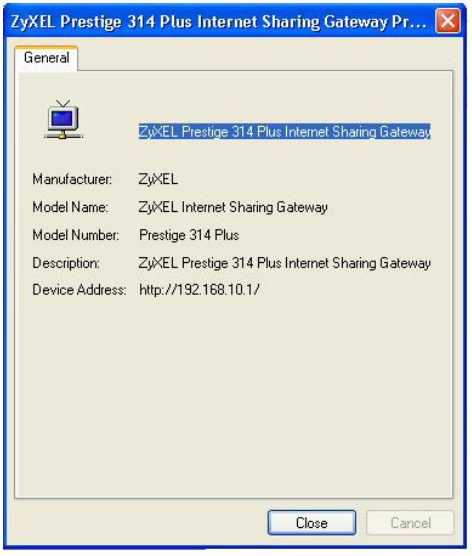


An icon with the description for each UPnP-enabled device displays under **Local Network**.

Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.



Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.



Part VIII:

Bandwidth Management

This part provides information on the functions and configuration of bandwidth management.

Chapter 18
Bandwidth Management Screens

This chapter describes the functions and configuration of bandwidth management. Bandwidth management applies to the ZyWALL 100.

18.1 Bandwidth Management Overview

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the ZyWALL forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- What priority level should you give to each type of traffic?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1000kbps if the broadband device connected to the WAN port has an upstream speed of 1000kbps. All configuration screens display measurements in kbps (kilobits per second), but this *User's Guide* also uses Mbps (megabits per second) for brevity's sake.

18.2 Bandwidth Classes and Filters

Use bandwidth classes and child-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or child-class) based on a specific

application and/or subnet. Use the **Class Configuration** tab (see *section 18.9.1*) to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter. You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended that you configure child-classes with filters for any classes that you configure without filters. The ZyWALL leaves the bandwidth budget allocated and unused for a class that does not have a filter itself or child-classes with filters. View your configured bandwidth classes and child-classes in the **Class Setup** tab (see *section 18.9* for details).

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

18.3 Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

18.4 Bandwidth Management Usage Examples

These examples show bandwidth management allotments on a WAN interface that is configured for 10Mbps.

18.4.1 Application-based Bandwidth Management Example

The bandwidth classes in the following example are based solely on application. Each bandwidth class (VoIP, Web, FTP, E-mail and Video) is allotted 2 Mbps.

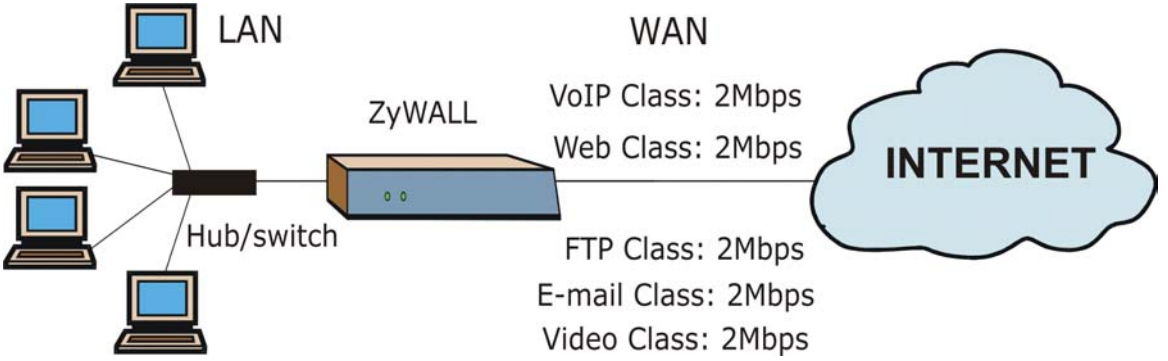


Figure 18-1 Application-based Bandwidth Management Example

18.4.2 Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based solely on LAN subnets. Each bandwidth class (Subnet A and Subnet B) is allotted 5 Mbps.

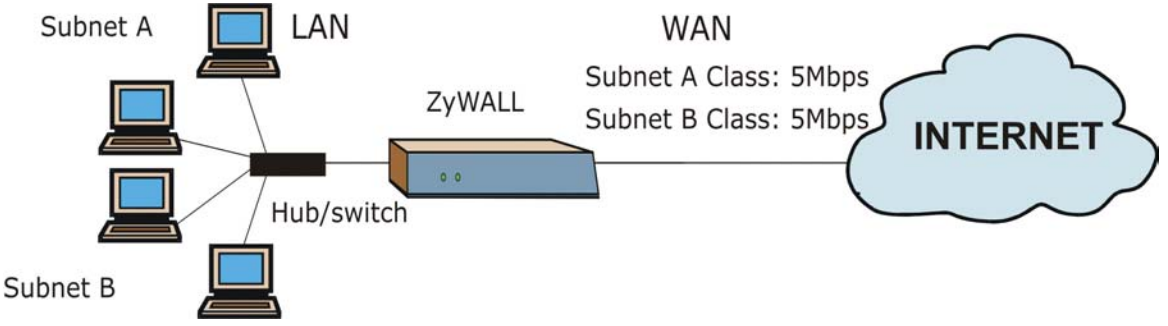


Figure 18-2 Subnet-based Bandwidth Management Example

18.4.3 Application and Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based on LAN subnets and applications (specific applications in each subnet are allotted bandwidth).

Table 18-1 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	1 Mbps	1 Mbps
Web	1 Mbps	1 Mbps
FTP	1 Mbps	1 Mbps
E-mail	1 Mbps	1 Mbps
Video	1 Mbps	1 Mbps

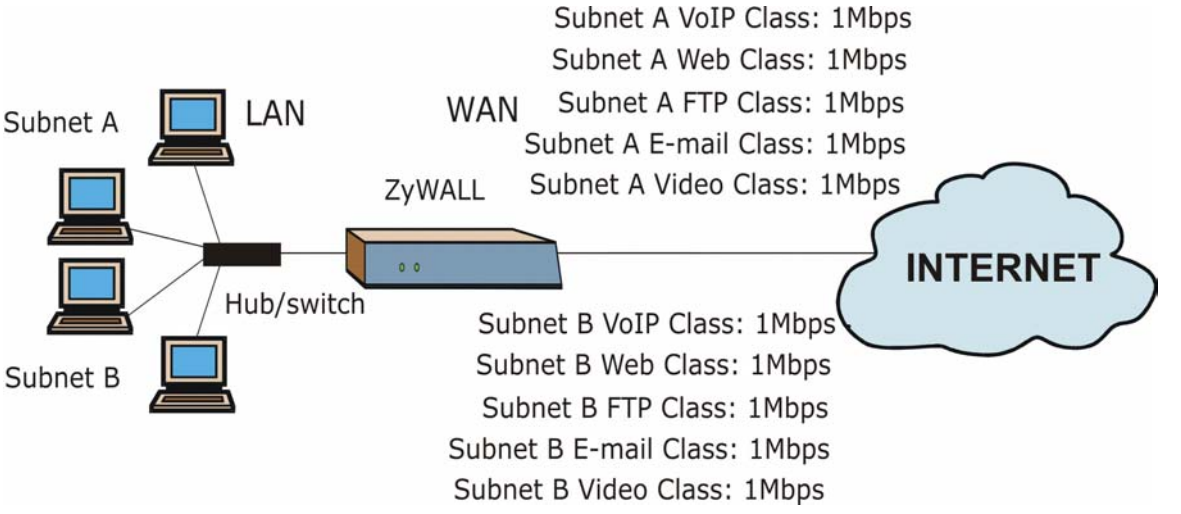


Figure 18-3 Application and Subnet-based Bandwidth Management Example

18.5 Scheduler

The scheduler divides up an interface's bandwidth among the bandwidth classes. The ZyWALL has two types of scheduler: fairness-based and priority-based.

18.5.1 Priority-based Scheduler

With the priority-based scheduler, the ZyWALL forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

18.5.2 Fairness-based Scheduler

The ZyWALL divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

18.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see *Figure 18-7*) allows the ZyWALL to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the ZyWALL first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the ZyWALL divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the ZyWALL gives extra bandwidth to that class.

When multiple classes require more bandwidth, the ZyWALL gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The ZyWALL distributes the available bandwidth equally among classes with the same priority level.

18.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

Do the following three steps to configure the ZyWALL to allow bandwidth for traffic that is not defined in a bandwidth filter.

Step 1. Leave some of the interface's bandwidth unbudgeted.

Step 2. Do not enable the interface's **Maximize Bandwidth Usage** option.

Step 3. Do not enable bandwidth borrowing on the child-classes that have the root class as their parent (see *section 18.7*).

18.6.2 Maximize Bandwidth Usage Example

Here is an example of a ZyWALL that has maximize bandwidth usage enabled on an interface. The first figure shows each bandwidth class's bandwidth budget and priority. The classes are set up based on subnets. The interface is set to 10 Mbps. Each subnet is allocated 2 Mbps. The unbudgeted 2 Mbps allows traffic not defined in one of the bandwidth filters to go out when you do not select the maximize bandwidth option.

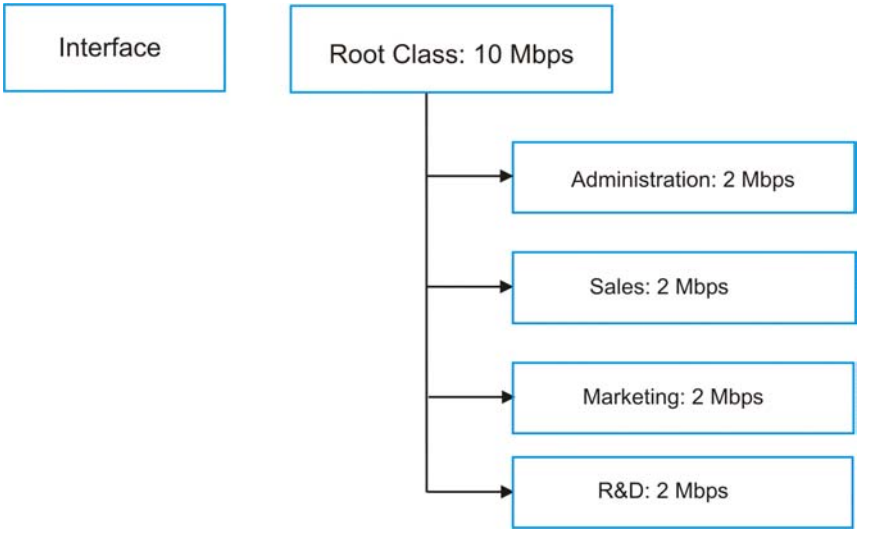


Figure 18-4 Bandwidth Allotment Example

The following figure shows the bandwidth usage with the maximize bandwidth usage option enabled. The ZyWALL divides up the unbudgeted 2 Mbps among the classes that require more bandwidth. If the administration department only uses 1 Mbps of the budgeted 2 Mbps, the ZyWALL also divides the remaining 1 Mbps among the classes that require more bandwidth. Therefore, the ZyWALL divides a total of 3 Mbps total of unbudgeted and unused bandwidth among the classes that require more bandwidth.

In this case, suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1 Mbps of its budgeted 2 Mbps.
- Sales and Marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1.5 Mbps or more of extra bandwidth, the ZyWALL divides the total 3 Mbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1.5 Mbps extra to each for a total of 3.5 Mbps for each) because they both have the highest priority level.
- R&D requires more bandwidth but only gets its budgeted 2 Mbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.
- The ZyWALL does not send any traffic that is not defined in the bandwidth filters because all of the unbudgeted bandwidth goes to the classes that need it.

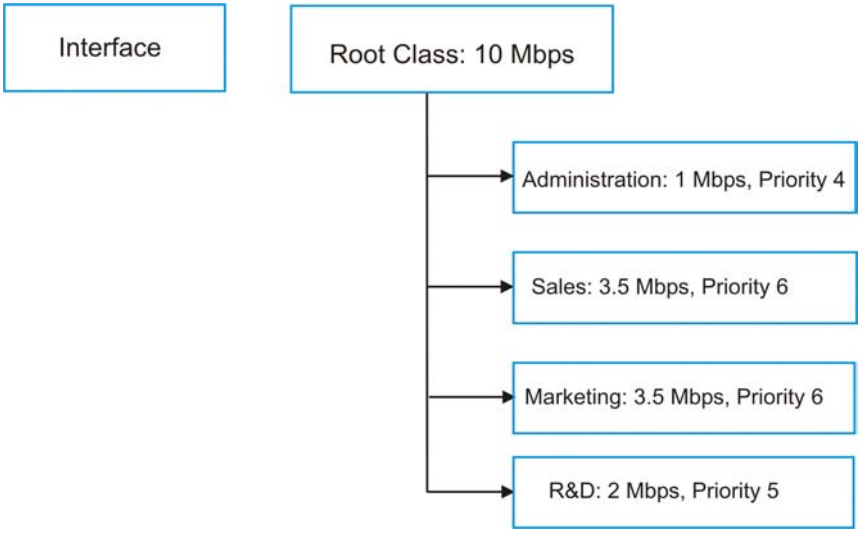


Figure 18-5 Maximize Bandwidth Usage Example

18.7 Bandwidth Borrowing

Bandwidth borrowing allows a child-class to borrow unused bandwidth from its parent class, whereas maximize bandwidth usage allows bandwidth classes to borrow any unused or unbudgeted bandwidth on the whole interface.

Enable bandwidth borrowing on a child-class to allow the child-class to use its parent class's unused bandwidth. A parent class's unused bandwidth is given to the highest priority child-class first. The child-class can also borrow bandwidth from a higher parent class (grandparent class) if the child-class's parent class is also configured to borrow bandwidth from its parent class. This can go on for as many levels as are configured to borrow bandwidth from their parent class (see *section 18.7.1*).

The total of the bandwidth allotments for child-classes cannot exceed the bandwidth allotment of their parent class. The ZyWALL uses the scheduler to divide a parent class's unused bandwidth among the child-classes.

18.7.1 Bandwidth Borrowing Example

Here is an example of bandwidth management with classes configured for bandwidth borrowing. The classes are set up based on departments and individuals within certain departments.

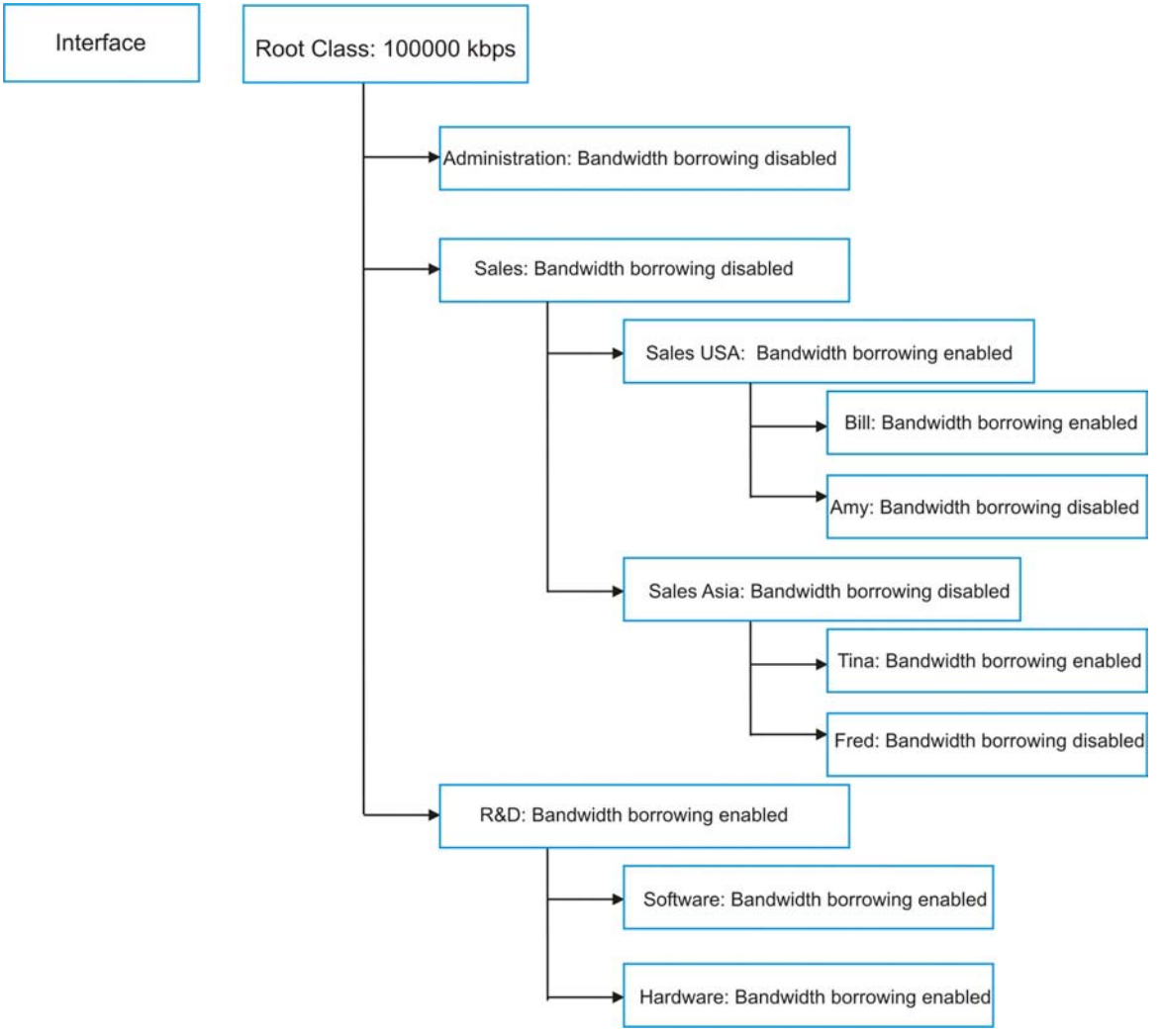


Figure 18-6 Bandwidth Borrowing Example

- The Bill class can borrow unused bandwidth from the Sales USA class because the Bill class has bandwidth borrowing enabled.
- The Bill class can also borrow unused bandwidth from the Sales class because the Sales USA class also has bandwidth borrowing enabled.

- The Bill class cannot borrow unused bandwidth from the Root class because the Sales class has bandwidth borrowing disabled.
- The Amy class cannot borrow unused bandwidth from the Sales USA class because the Amy class has bandwidth borrowing disabled.
- The R&D Software and Hardware classes can both borrow unused bandwidth from the R&D class because the R&D Software and Hardware classes both have bandwidth borrowing enabled.
- The R&D Software and Hardware classes can also borrow unused bandwidth from the Root class because the R&D class also has bandwidth borrowing enabled.

18.7.2 Maximize Bandwidth Usage With Bandwidth Borrowing

If you configure both maximize bandwidth usage (on the interface) and bandwidth borrowing (on individual child-classes), the ZyWALL functions as follows.

1. The ZyWALL sends traffic according to each bandwidth class's bandwidth budget.
2. The ZyWALL assigns a parent class's unused bandwidth to its child-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The ZyWALL gives priority to bandwidth child-classes of higher priority and treats bandwidth classes of the same priority equally.
3. The ZyWALL assigns any remaining unused or unbudgeted bandwidth on the interface to any bandwidth class that requires it. The ZyWALL gives priority to bandwidth classes of higher priority and treats bandwidth classes of the same level equally.
4. The ZyWALL assigns any remaining unbudgeted bandwidth to traffic that does not match any of the bandwidth classes.

18.8 Configuring Summary

Click **BW MANAGER** to open the **Summary** screen.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

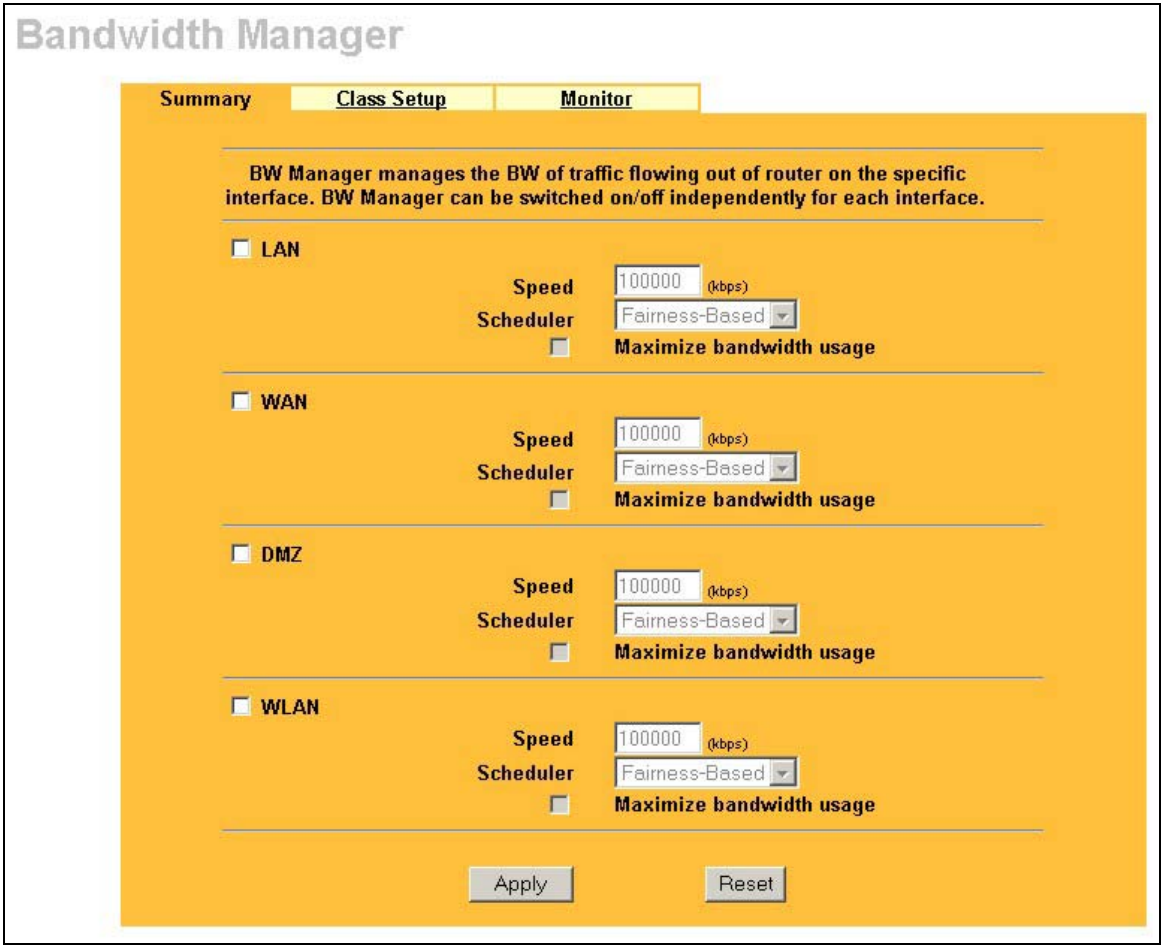


Figure 18-7 Bandwidth Manager: Summary

The following table describes the fields in this screen.

Table 18-2 Bandwidth Manager: Summary

LABEL	DESCRIPTION
LAN WAN DMZ WLAN	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Not all interfaces are available on every ZyWALL.
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class (see *section 18.9*). The recommendation is to set this speed to match what the device connected to the port can handle. For example, set the WAN interface speed to 1000 kbps if the broadband device connected to the WAN port has an upstream speed of 1000 kbps.
Scheduler	Select either **Priority-Based** or **Fairness-Based** from the drop-down menu to control the traffic flow. Select **Priority-Based** to give preference to bandwidth classes with higher priorities. Select **Fairness-Based** to treat all bandwidth classes equally. See *section 18.5*.
Maximize Bandwidth Usage	Select this check box to have the ZyWALL divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class (see *section 18.6.1*) or you want to limit the speed of this interface (see the **Speed** field description).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

18.9 Configuring Class Setup

The class setup screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click "+" to expand the class tree or click "-" to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see *section 18.8* to configure the speed of the interface). Configure child-class layers for the root class.

To add or delete child classes on an interface, click **BW MANAGER**, then the **Class Setup** tab. The screen appears as shown (with example classes).

The example reserves 15 Mbps of unbudgeted bandwidth for traffic that is not defined in the bandwidth filters (see *section 18.6.1*). The Administration, Sales USA and Sales Asia bandwidth classes each have bigger bandwidth budgets than the total of the budgets of their child-classes. The child-classes can borrow the extra bandwidth as long as they have bandwidth borrowing enabled (see *section 18.7*).

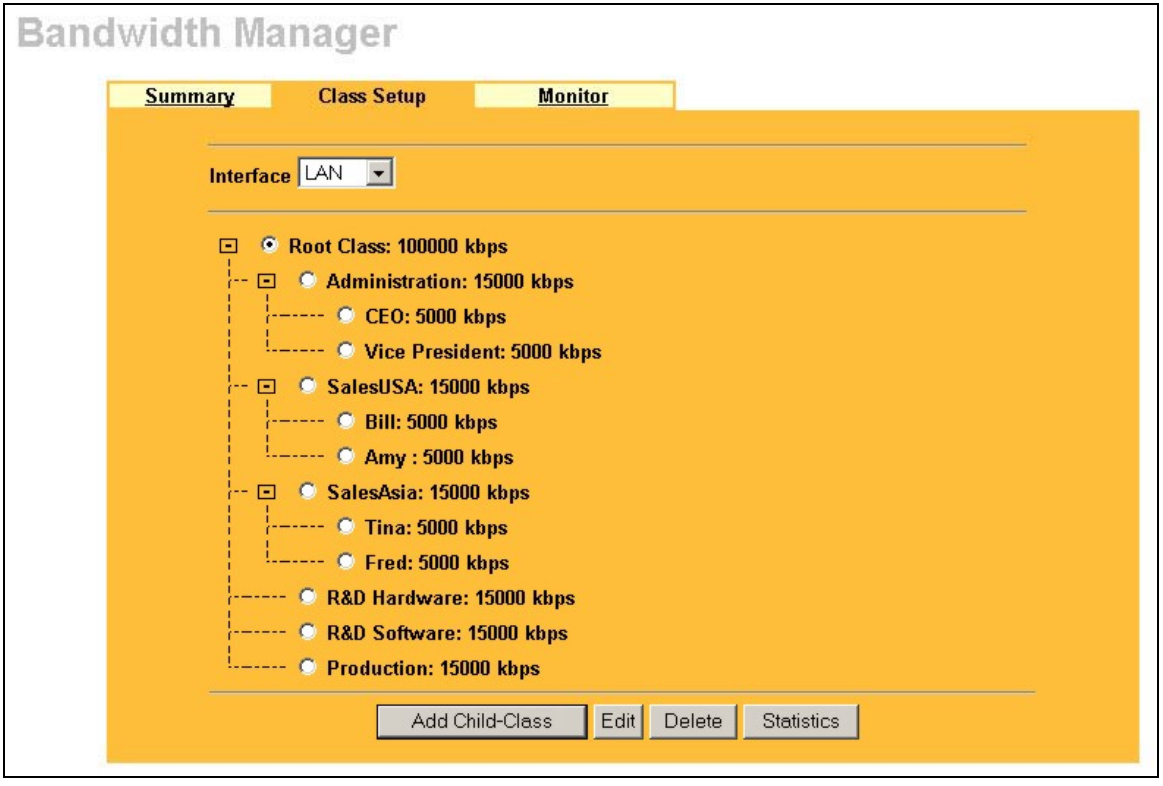


Figure 18-8 Bandwidth Manager: Class Setup

The following table describes the fields in this screen.

Table 18-3 Bandwidth Manager: Class Setup

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box for which you wish to set up classes.
Add Child-Class	Click **Add Child-class** to add a sub-class.

Table 18-3 Bandwidth Manager: Class Setup

LABEL	DESCRIPTION
Edit	Click **Edit** to configure the selected class. You cannot edit the root class.
Delete	Click **Delete** to delete the class and all its child-classes. You cannot delete the root class.
Statistics	Click **Statistics** to display the status of the selected class.

18.9.1 Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Configuration** screen. You must use the **Bandwidth Manager Summary** screen to enable bandwidth management on an interface before you can configure classes for that interface.

To add a child class, click **BW MANAGER**, then the **Class Setup** tab. Click the **Add Child-Class** button to open the following screen.

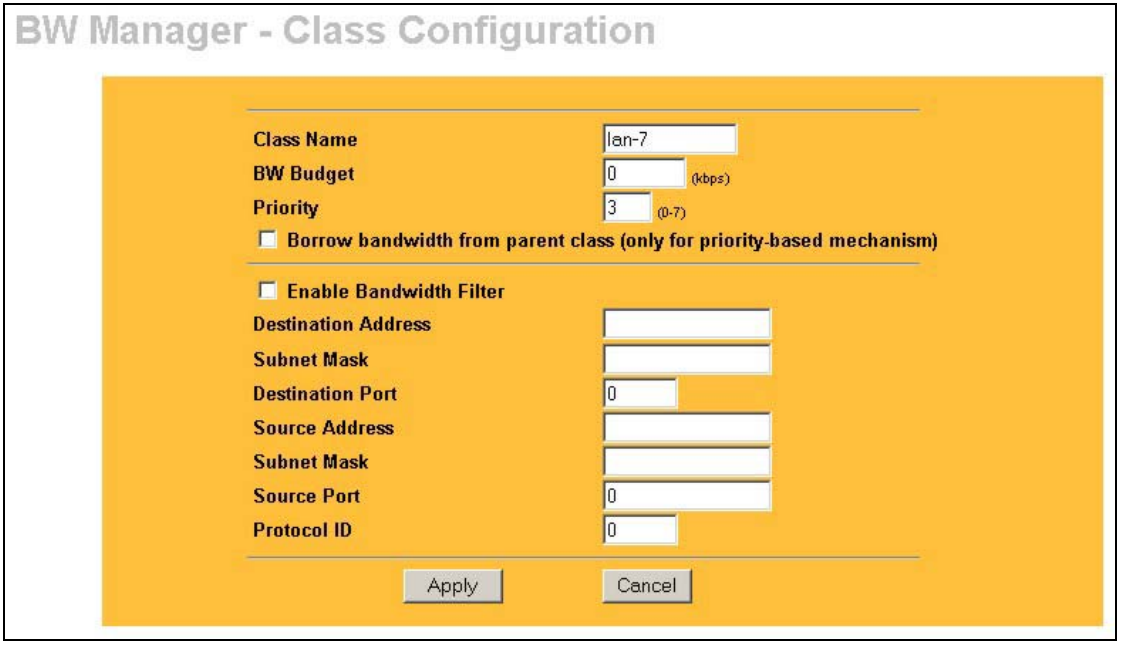


Figure 18-9 Bandwidth Manager: Class Configuration

The following table describes the fields in this screen.

Table 18-4 Bandwidth Manager: Class Configuration

LABEL	DESCRIPTION
Class Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
BW Budget (kbps)	Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class.
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Borrow bandwidth from parent class	Select this option to allow a child-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget. Bandwidth borrowing is governed by the priority of the child-classes. That is, a child-class with the highest priority (7) is the first to borrow bandwidth from its parent class. Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types (see *18.6.1*) or you want to set the interface's speed to match what the next device in network can handle (see the **Speed** field description in *Table 18-2*).
Enable Bandwidth Filter	Select **Enable Bandwidth Filter** to have the ZyWALL use this bandwidth filter when it performs bandwidth management. You must enter a value in at least one of the following fields (other than the **Subnet Mask** fields which are only available when you enter the destination or source IP address).
Destination Address	Enter the destination IP address in dotted decimal notation.
Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a **Destination Address**. Refer to the *Reference Guide* for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See the chapter on creating custom firewall rules for a table of services and port numbers.
Source Address	Enter the source IP address.
Subnet Mask	Enter the source subnet mask. This field is N/A if you do not specify a **Source Address**. Refer to the *Reference Guide* for more information on IP subnetting.
Source Port	Enter the port number of the source. See the following table for some common services and port numbers.

Table 18-4 Bandwidth Manager: Class Configuration

LABEL	DESCRIPTION
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

Table 18-5Services and Port Numbers

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

18.9.2 Bandwidth Management Statistics

Use the **Bandwidth Management Statistics** screen to view network performance information. Click the **Statistics** button in the **Class Setup** screen to open the **Statistics** screen.

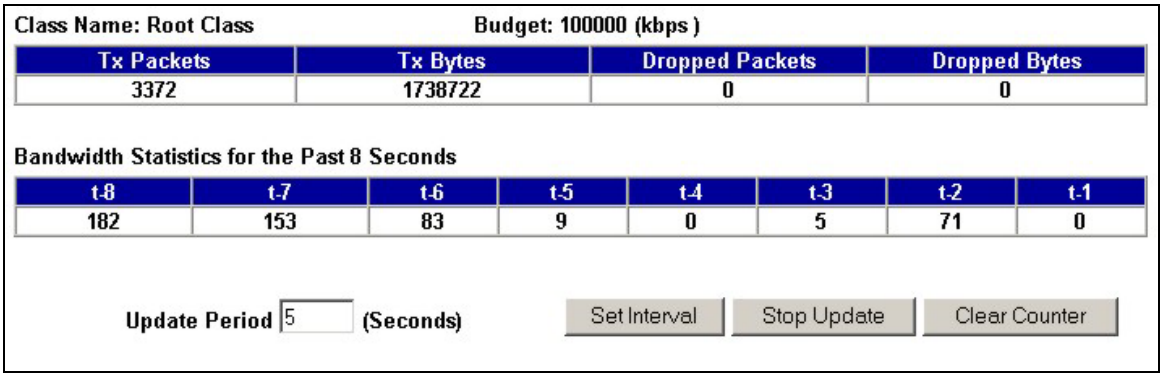


Figure 18-10 Bandwidth Management Statistics

The following table describes the fields in this screen.

Table 18-6 Bandwidth Management Statistics

LABEL	DESCRIPTION
Class Name	This field displays the name of the class the statistics page is showing.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Tx Packets	This field displays the total number of packets transmitted.
TX Bytes	This field displays the total number of bytes transmitted.
Dropped Packets	This field displays the total number of packets dropped.
Dropped Bytes	This field displays the total number of bytes dropped.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago.	
Update Period (seconds)	Enter the time interval in seconds to define how often the information should be refreshed.
Set Interval	Click **Set Interval** to apply the new update period you entered in the **Update Period** field above.
Stop Update	Click **Stop Update** to stop the browser from refreshing bandwidth management statistics.

Table 18-6 Bandwidth Management Statistics

LABEL	DESCRIPTION
Clear Counter	Click **Clear Counter** to clear all of the bandwidth management statistics.

18.10 Configuring Monitor

To view the device's bandwidth usage and allotments, click **BW MANAGER**, then the **Monitor** tab. The screen appears as shown.

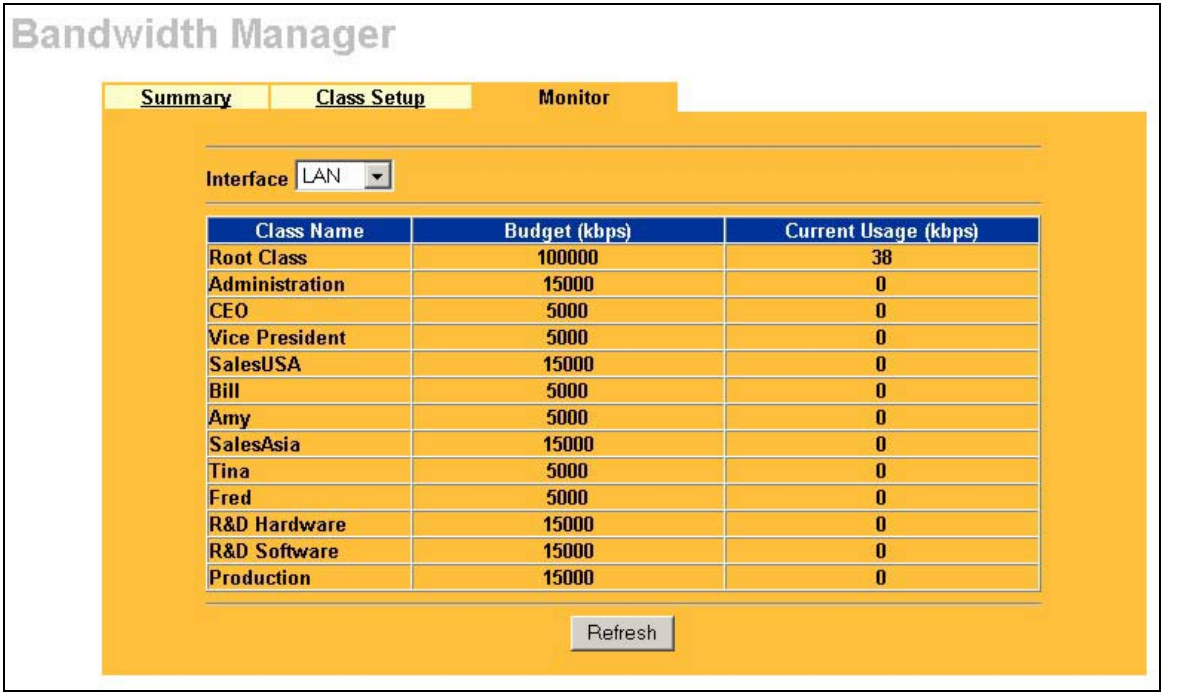


Figure 18-11 Bandwidth Manager Monitor

The following table describes the fields in this screen.

Table 18-7 Bandwidth Manager Monitor

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes.
Class Name	This field displays the name of the class.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Current Usage (kbps)	This field displays the amount of bandwidth that each class is using.
Refresh	Click **Refresh** to update the page.

Part IX:

Logs

This part provides information and instructions for the logs and reports.

Chapter 19
Logs Screens

This chapter contains information about configuring general log settings and viewing the ZyWALL's logs. Refer to the Reference Guide for example log message explanations.

19.1 Configuring View Log

The web configurator allows you to look at all of the ZyWALL's logs in one location.

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see *section 19.2*). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

#	Time	Message	Source	Destination	Notes
1	01/10/2003 01:55:52	Firewall default policy: UDP (W to W/ZW)	172.21.4.47:138	172.21.255.255:138	ACCESS BLOCK
2	01/10/2003 01:55:51	Firewall default policy: UDP (W to W/ZW)	172.21.1.230:137	172.21.255.255:137	ACCESS BLOCK
3	01/10/2003 01:55:51	Firewall default policy: UDP (W to W/ZW)	172.21.3.97:137	172.21.255.255:137	ACCESS BLOCK
4	01/10/2003 01:55:50	Firewall default policy: UDP (W to W/ZW)	172.21.3.97:137	172.21.255.255:137	ACCESS BLOCK
5	01/10/2003 01:55:49	Firewall default policy: UDP (W to W/ZW)	172.21.3.97:137	172.21.255.255:137	ACCESS BLOCK
6	01/10/2003 01:55:47	Firewall default policy: UDP (W to W/ZW)	172.21.4.141:138	172.21.255.255:138	ACCESS BLOCK
7	01/10/2003 01:55:47	Firewall default policy: UDP (W to W/ZW)	172.21.4.141:138	172.21.255.255:138	ACCESS BLOCK
8	01/10/2003 01:55:46	Firewall default policy: UDP (W to W/ZW)	172.21.3.97:137	172.21.255.255:137	ACCESS BLOCK
9	01/10/2003 01:55:46	Firewall default policy: UDP (W to W/ZW)	172.21.3.10:138	172.21.255.255:138	ACCESS BLOCK
10	01/10/2003 01:55:46	Firewall default policy: UDP (W to W/ZW)	172.21.3.97:137	172.21.255.255:137	ACCESS BLOCK
11	01/10/2003 01:55:45	Firewall default policy: UDP (W to W/ZW)	172.21.3.97:137	172.21.255.255:137	ACCESS BLOCK
12	01/10/2003 01:55:45	Firewall default policy: UDP (W to W/ZW)	172.21.4.23:137	172.21.255.255:137	ACCESS BLOCK
13	01/10/2003 01:55:44	Firewall default policy: UDP (W to W/ZW)	172.21.4.23:137	172.21.255.255:137	ACCESS BLOCK
14	01/10/2003 01:55:43	Firewall default policy: UDP (W to W/ZW)	172.21.4.23:137	172.21.255.255:137	ACCESS BLOCK

Figure 19-1 View Log

The following table describes the fields in this screen.

Table 19-1 View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see *section 19.2*) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the ZyWALL's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**, see *section 19.2*).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

19.2 Configuring Log Settings

To change your ZyWALL's log settings, click **Logs**, then the **Log Settings** tab. The screen appears as shown.

Use the **Log Settings** screen to configure to where the ZyWALL is to send logs; the schedule for when the ZyWALL is to send the logs and which logs and/or immediate alerts the ZyWALL is to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

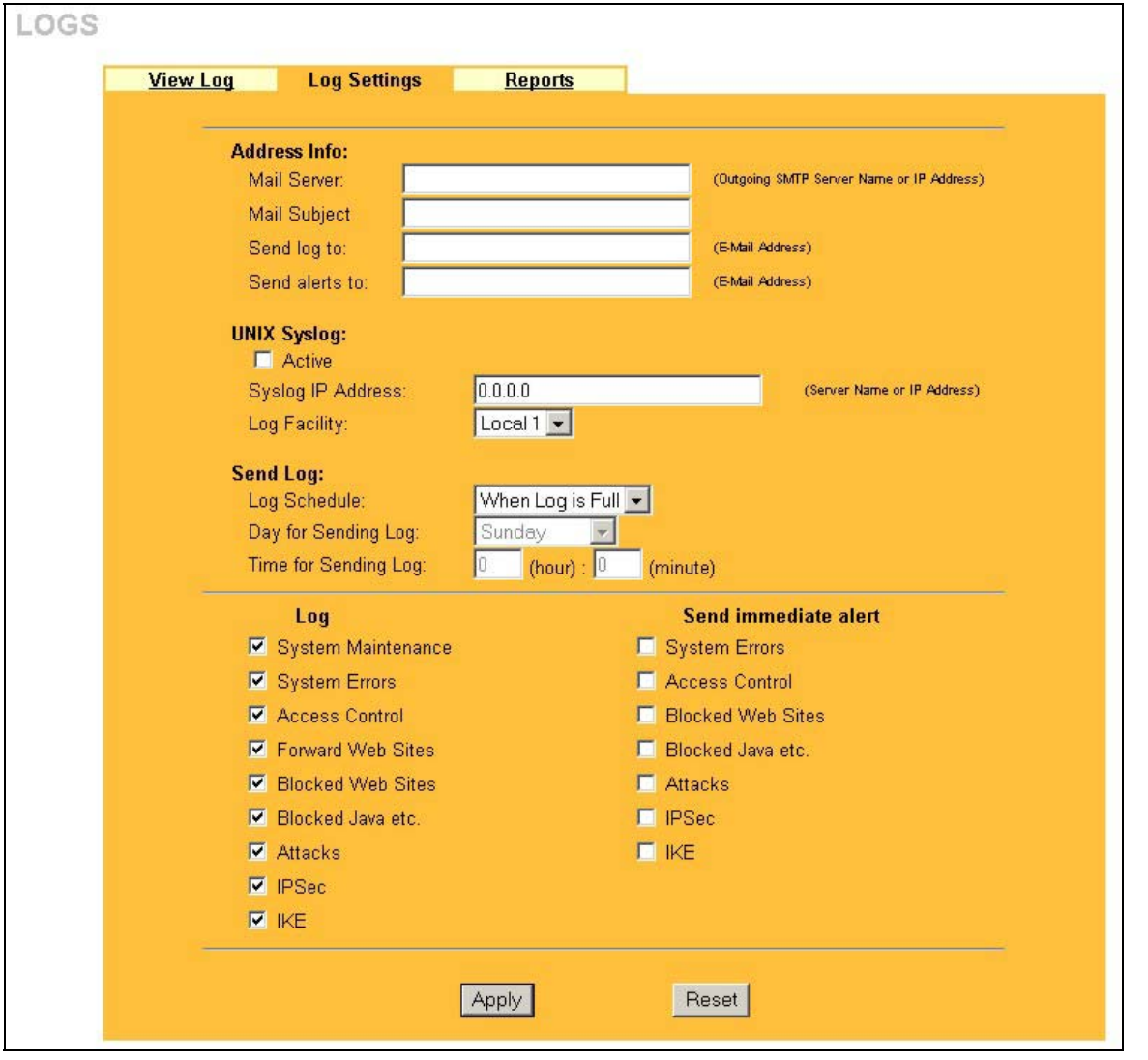


Figure 19-2 Log Settings (ZyWALL 10W)

The following table describes the fields in this screen.

Table 19-2 Log Settings Screen (ZyWALL 10W)

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyWALL sends.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
UNIX Syslog	UNIX syslog sends a log to an external UNIX server used to store logs.
Active	Click **Active** to enable UNIX syslog.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to your UNIX manual for more information.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • **Daily** • **Weekly** • **Hourly** • **When the Log is Full** • **None.** If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Log	Select the categories of logs that you want to record. Logs include alerts.

Table 19-2 Log Settings Screen (ZyWALL 10W)

LABEL	DESCRIPTION
Send Immediate Alert	Select the categories of alerts for which you want the ZyWALL to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

19.3 Configuring Reports

To change your ZyWALL's log reports, click **Logs**, then the **Reports** tab. The screen appears as shown.

The **Reports** page displays which computers on the LAN send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. Use the **Reports** screen to have the ZyWALL record and display the following network usage details:

- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN IP addresses to and/or from which the most traffic has been sent
- How much traffic has been sent to and from the LAN IP addresses to and/or from which the most traffic has been sent

The web site hit count may not be 100% accurate because sometimes when an individual web page loads, it may contain references to other web sites that also get counted as hits.

The ZyWALL records web site hits by counting the HTTP GET packets. Many web sites include HTTP GET references to other web sites and the ZyWALL may count these as hits, thus the web hit count is not (yet) 100% accurate.

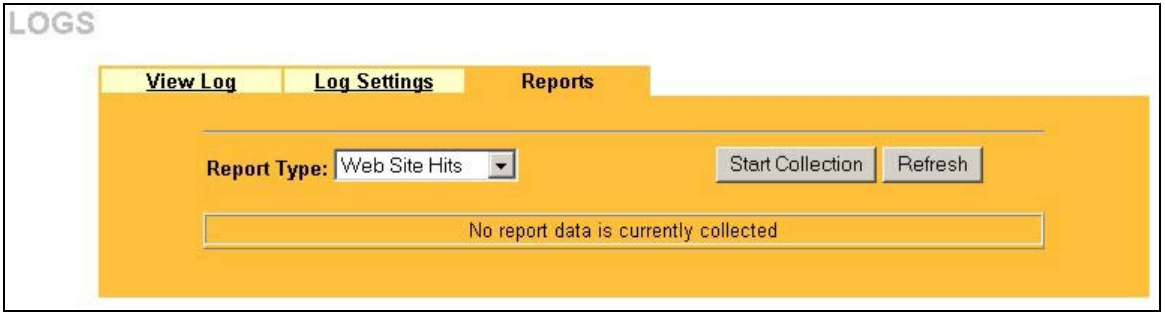


Figure 19-3 Reports

Enabling the ZyWALL's reporting function decreases the overall throughput by about 1 Mbps.

The following table describes the fields in this screen.

Table 19-3 Reports

LABEL	DESCRIPTION
Report Type	Use the drop-down list box to select the type of reports to display. **Web Site Hits** displays the web sites that have been visited the most often from the LAN and how many times they have been visited. **Protocol/Port** displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports. **LAN IP Address** displays the LAN IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses.
Start Collection/ Stop Collection	The button text shows **Start Collection** when the ZyWALL is not recording report data and **Stop Collection** when the ZyWALL is recording report data. Click **Start Collection** to have the ZyWALL record report data. Click **Stop Collection** to halt the ZyWALL from recording more data.
Refresh	Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen.

All of the recorded reports data is erased when you turn off the ZyWALL.

19.3.1 Viewing Web Site Hits

In the **Reports** screen, select **Web Site Hits** from the **Report Type** drop-down list box to have the ZyWALL record and display which web sites have been visited the most often and how many times they have been visited.

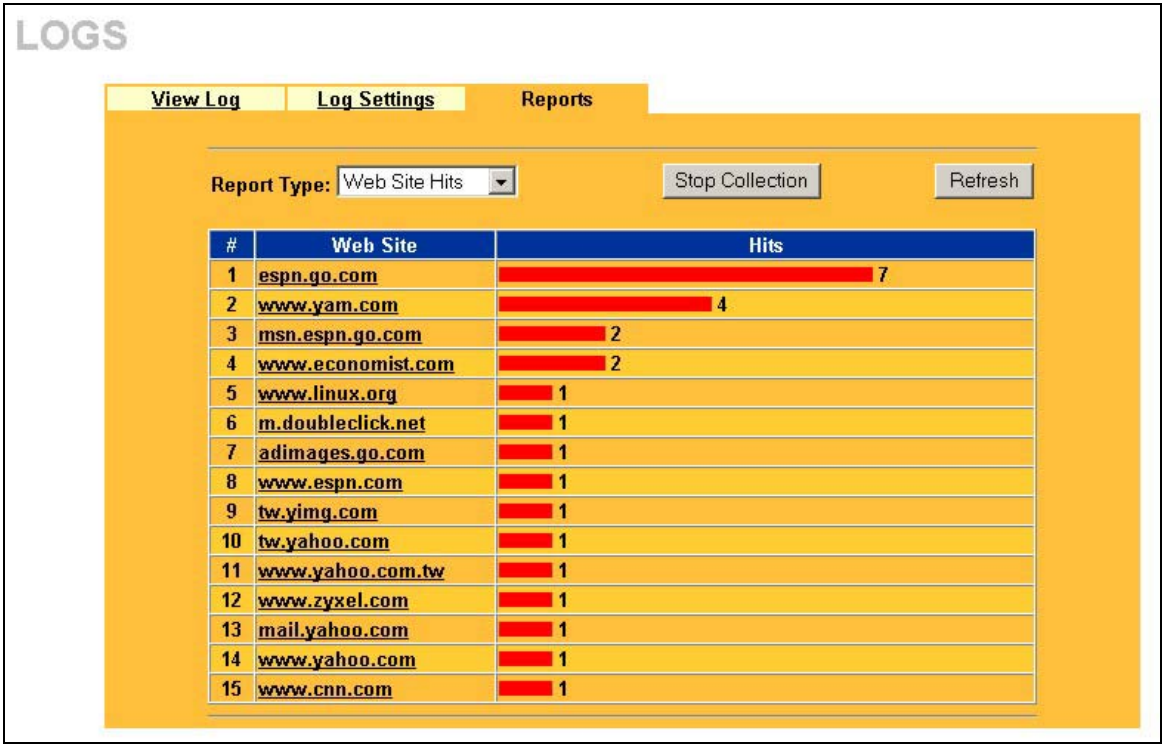


Figure 19-4 Web Site Hits Report Example

The following table describes the fields in this screen.

Table 19-4 Web Site Hits Report

LABEL	DESCRIPTION
Web Site	This column lists the domain names of the web sites visited most often from computers on the LAN. The names are ranked by the number of visits to each web site and listed in descending order with the most visited web site listed first. The ZyWALL counts each page viewed in a web site as another hit on the web site.
Hits	This column lists how many times each web site has been visited. The count starts over at 0 if a web site passes the hit count limit (see *Table 19-7 Report Specifications*).

19.3.2 Viewing Protocol/Port

In the **Reports** screen, select **Protocol/Port** from the **Report Type** drop-down list box to have the ZyWALL record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.

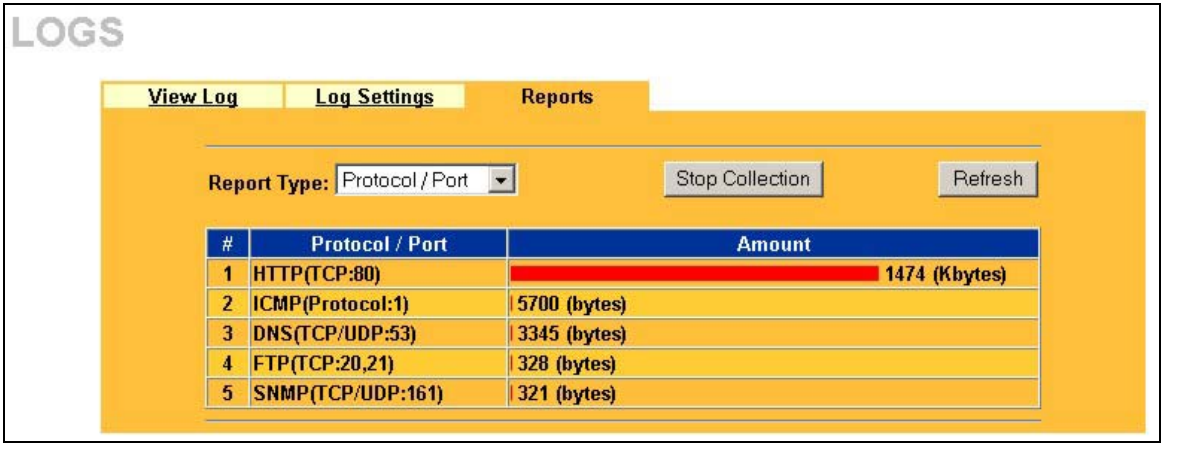


Figure 19-5 Protocol/Port Report Example

The following table describes the fields in this screen.

Table 19-5 Protocol/ Port Report

LABEL	DESCRIPTION
Protocol/Port	This column lists the protocols or service ports for which the most traffic has gone through the ZyWALL. The protocols or service ports are listed in descending order with the most used protocol or service port listed first.
Amount	This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see *Table 19-7 Report Specifications*).

19.3.3 Viewing LAN IP Address

In the **Reports** screen, select **LAN IP Address** from the **Report Type** drop-down list box to have the ZyWALL record and display the LAN IP addresses that the most traffic has been sent to and/or from and how much traffic has been sent to and/or from those IP addresses.

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

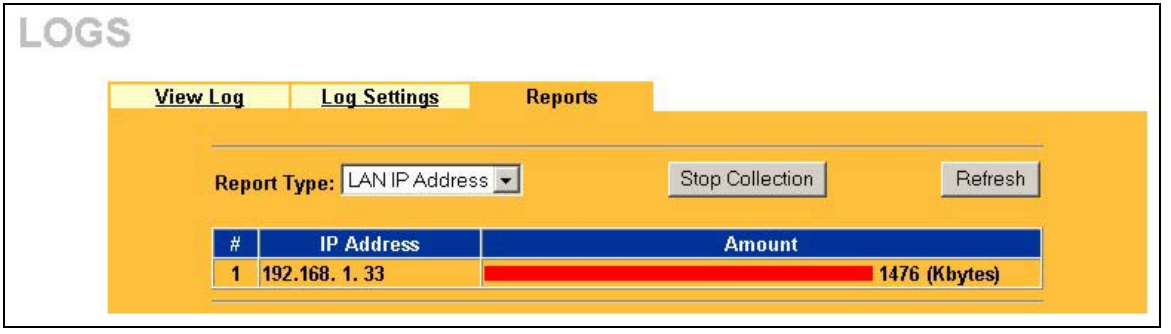


Figure 19-6 LAN IP Address Report Example

The following table describes the fields in this screen.

Table 19-6 LAN IP Address Report

LABEL	DESCRIPTION
IP Address	This column lists the LAN IP addresses to and/or from which the most traffic has been sent. The LAN IP addresses are listed in descending order with the LAN IP address to and/or from which the most traffic was sent listed first.
Amount	This column displays how much traffic has gone to and from the listed LAN IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN IP passes the bytes count limit (see *Table 19-7 Report Specifications*).

19.3.4 Reports Specifications

The following table lists detailed specifications on the reports feature.

Table 19-7 Report Specifications

LABEL	DESCRIPTION
Number of web sites/protocols or ports/IP addresses listed:	20
Hit count limit:	Up to 2^{32} hits can be counted per web site. The count starts over at 0 if it passes four billion.
Bytes count limit:	Up to 2^{64} bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes 2^{64} bytes.

Part X:

Maintenance

This part covers the maintenance screens.

Chapter 20
Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

20.1 Maintenance Overview

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

20.2 Status Screen

Click **MAINTENANCE** to open the **Status** screen, where you can use to monitor your ZyWALL. Note that these fields are READ-ONLY and are meant to be used for diagnostic purposes.

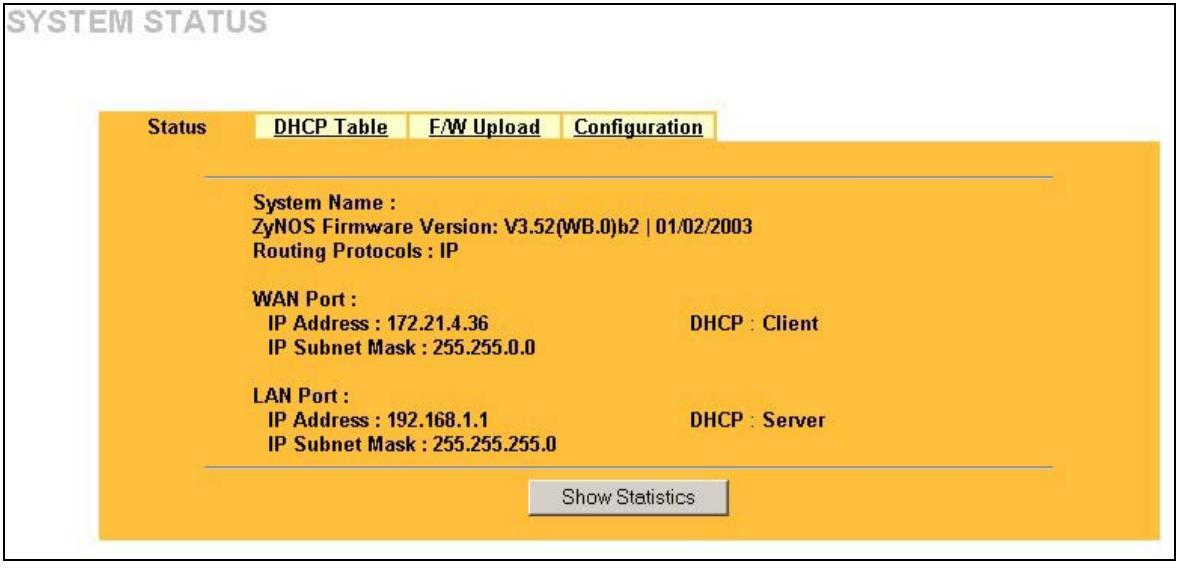


Figure 20-1 System Status

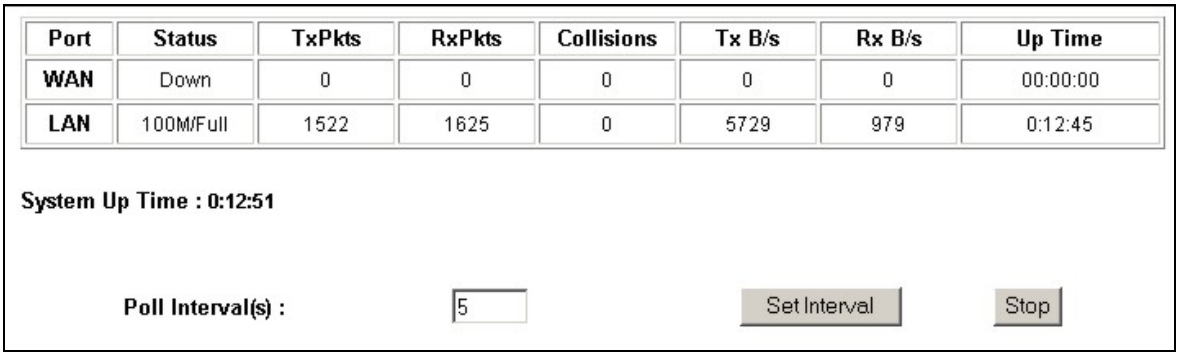
The following table describes the fields in this screen.

Table 20-1 System Status

LABEL	DESCRIPTION
System Name	This is the **System Name** you chose in the first Internet Access Wizard screen. It is for identification purposes
ZyNOS Firmware Version:	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Routing Protocols	This shows the routing protocol - **IP** for which the ZyWALL is configured. This field is not configurable in all ZyWALL router models.
WAN Port	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role - **Client** or **None**.
LAN Port	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role - **Server**, **Relay** (not all ZyWALL models) or **None**.
DMZ Port (not available on all ZyWALL models)	
IP Address	This is the DMZ port IP address.
IP Subnet Mask	This is the DMZ port subnet mask.
DHCP	This is the DMZ port DHCP role - **Server**, **Relay** (not all ZyWALL models) or **None**.
Show Statistics	Click **Show Statistics** to see router performance statistics such as number of packets sent and number of packets received for each port.

20.2.1 System Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.



Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	1522	1625	0	5729	979	0:12:45

System Up Time : 0:12:51

Poll Interval(s) : 5 Set Interval Stop

Figure 20-2 System Status: Show Statistics

The following table describes the fields in this screen.

Table 20-2 System Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the WAN, LAN, DMZ or Wireless LAN port.
Status	This displays the port speed and duplex setting if you're using Ethernet encapsulation and **down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the ZyWALL has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.

Table 20-2 System Status: Show Statistics

LABEL	DESCRIPTION
Stop	Click **Stop** to stop refreshing statistics, click **Stop**.

20.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyWALL as a DHCP server or disable it. When configured as a server, the ZyWALL provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

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

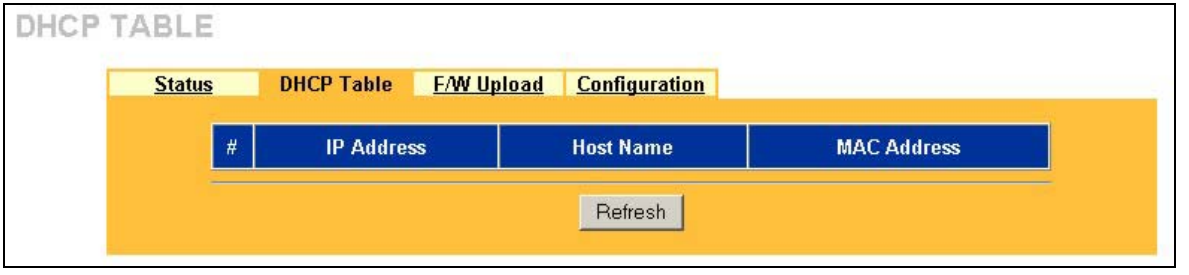


Figure 20-3 DHCP Table

The following table describes the fields in this screen.

Table 20-3 DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.

Table 20-3 DHCP Table

LABEL	DESCRIPTION
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click **Refresh** to renew the screen.

20.4 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "zywall.bin". The upload process uses FTP (File Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the *Firmware and Configuration File Maintenance* chapter in the *SMT User's Guide* for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **F/W UPLOAD** tab. Follow the instructions in this screen to upload firmware to your ZyWALL.

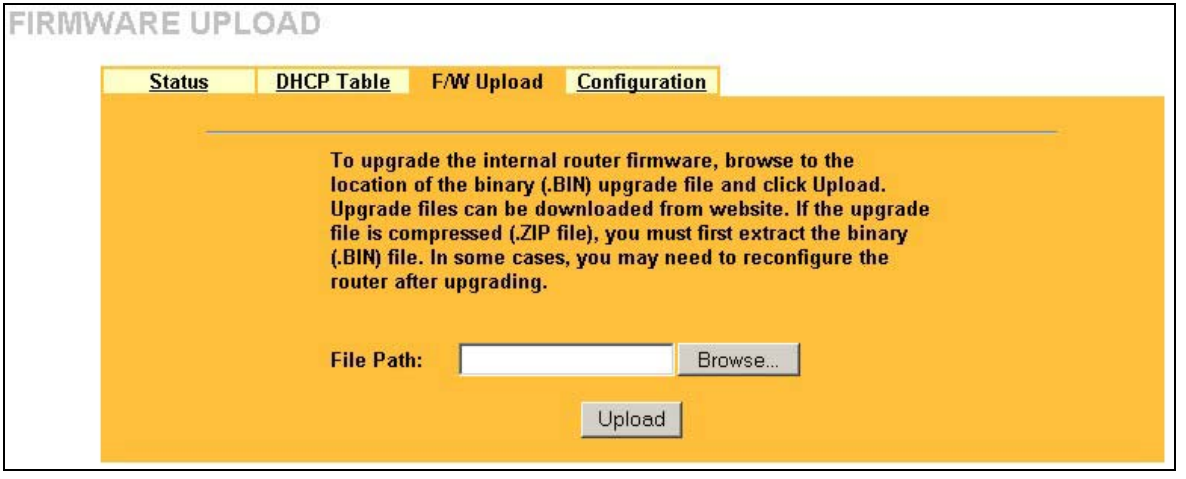


Figure 20-4 Firmware Upgrade

The following table describes the fields in this screen.

Figure 20-5 Firmware Upgrade

LABEL	DESCRIPTION
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.

Do not turn off the device while firmware upload is in progress!

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

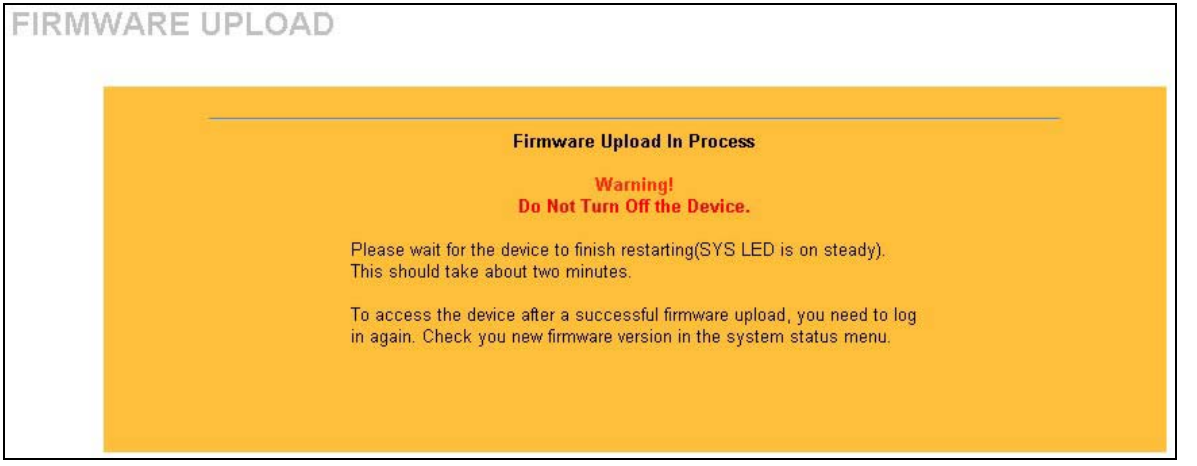


Figure 20-6 Firmware Upload In Process

The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

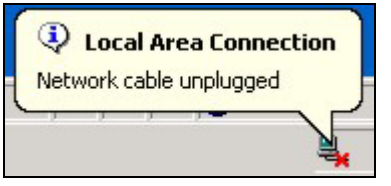


Figure 20-7 Network Temporarily Disconnected

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

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 20-8 Firmware Upload Error

20.5 Configuration Screen

The web configurator uses TFTP to transfer files. See the *Firmware and Configuration File Maintenance* chapter in the *SMT User's Guide* for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

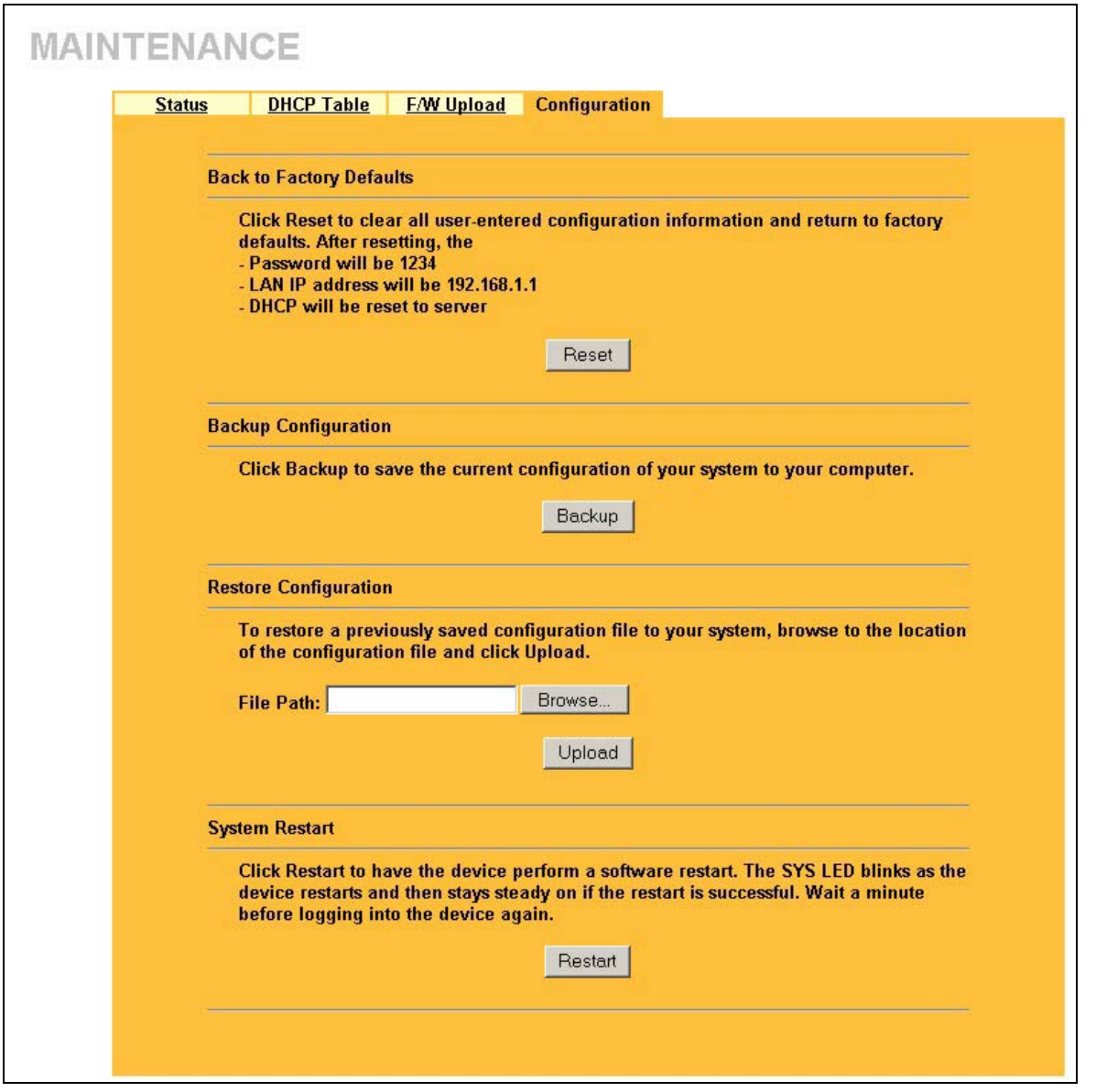


Figure 20-9 Configuration

20.5.1 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyWALL to its factory defaults as shown on the screen. The following warning screen will appear.

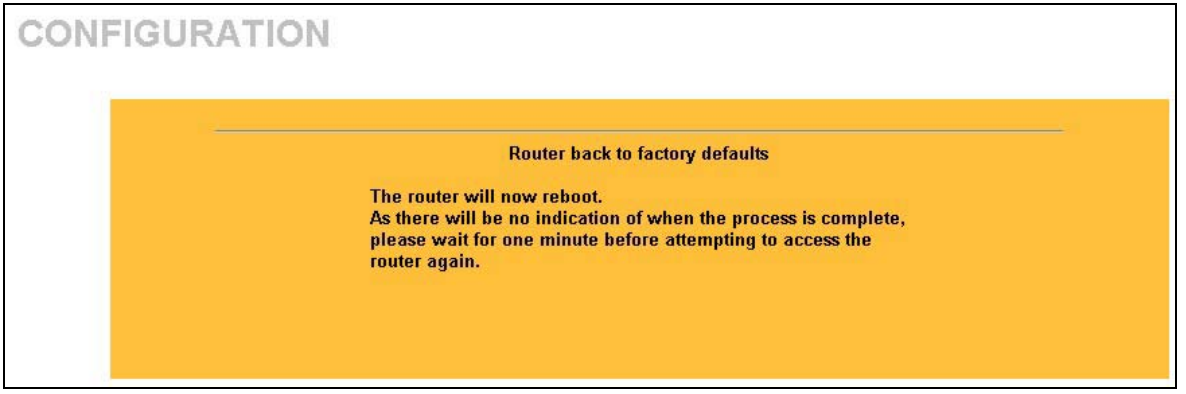


Figure 20-10 Reset Warning Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyWALL. Refer to the *Hardware Installation* chapter for more information on the **RESET** button.

20.5.2 Backup Configuration

Backup Configuration allows you to backup (save) the current system (ZyWALL) configuration to your computer. Backup is highly recommended once your ZyWALL is functioning properly.

Click **Backup** to save your current ZyWALL configuration to your computer.

20.5.3 Restore Configuration

Restore Configuration allows you to restore a previously saved configuration file from your computer to your ZyWALL.

Table 20-4 Restore Configuration

LABEL	DESCRIPTION
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 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.

Do not turn off the device while configuration file upload is in progress.

After you see a "configuration upload successful" screen, you must then wait one minute before logging into the device again.

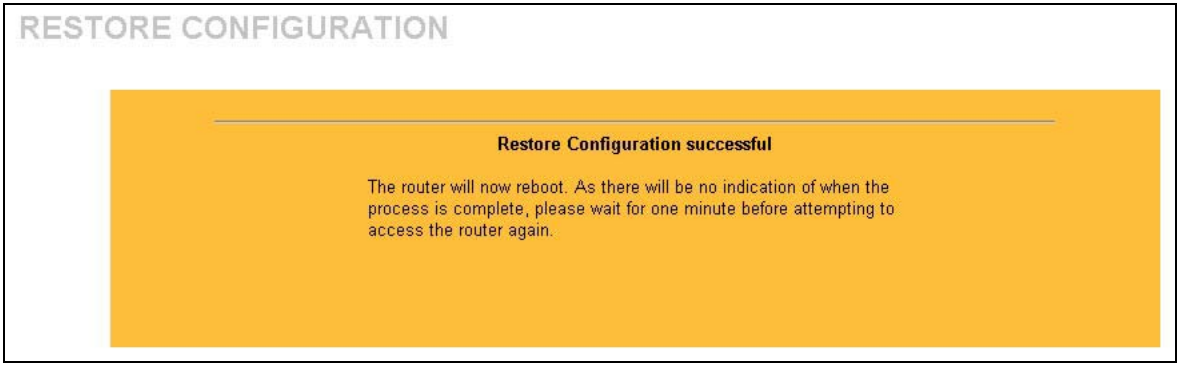


Figure 20-11 Configuration Upload Successful

The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 20-12 Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See your *Quick Start Guide* for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

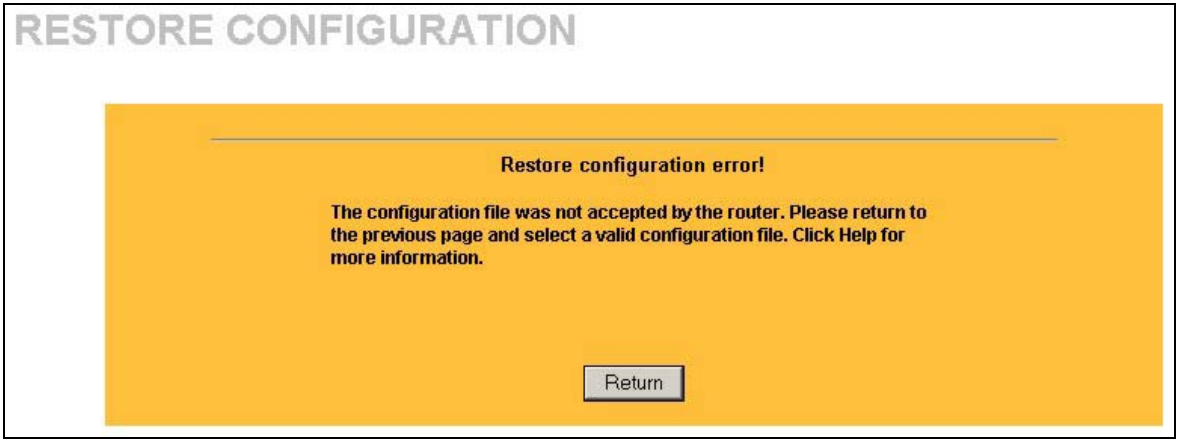


Figure 20-13 Configuration Upload Error

20.5.4 System Restart

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

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

Part XI:

SMT General Configuration

This part introduces the System Management Terminal and covers the General setup menu, WAN and dial backup setup, LAN and wireless LAN setup, DMZ setup, and Internet access.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 21
Introducing the SMT

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

21.1 Introduction to the SMT

The ZyWALL's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

21.2 Accessing the Console Port via the Console Port

Make sure you have the physical connection properly set up as described in the hardware installation chapter.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

21.2.1 Initial Screen

When you turn on your ZyWALL, it performs several internal tests as well as line initialization. After the tests, the ZyWALL asks you to press [ENTER] to continue, as shown next.

```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:41:51:61
initialize ch =1, ethernet address: 00:a0:c5:41:51:62
Press ENTER to continue...
```

Figure 21-1 Initial Screen

21.2.2 Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below.

For your first login, enter the default password "1234". As you type the password, the screen displays an "X" for each character you type.
Please note that if there is no activity for longer than five minutes after you log in, your ZyWALL will automatically log you out and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

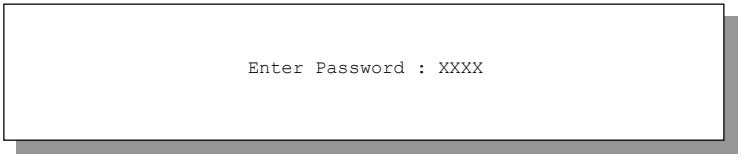


Figure 21-2 Password Screen

21.3 Navigating the SMT Interface

The SMT is an interface that you use to configure your ZyWALL.
Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 21-1 Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press the [ESC] key to move back to the previous menu.
Move to a "hidden" menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] to change **No** to **Yes**, and then press [ENTER] to go to a "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Fill in, or press [SPACE BAR], then press [ENTER] to select from choices.	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? >	All fields with the symbol <?> must be filled in order be able to save the new configuration.

Table 21-1 Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

21.3.1 Main Menu

After you enter the password, the SMT displays the **ZyWALL Main Menu**, as shown next. Not all models have all the features shown.

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

                      ZyWALL 100 Main Menu

       Getting Started              Advanced Management
         1. General Setup             21. Filter and Firewall Setup
         2. WAN Setup                 22. SNMP Configuration
         3. LAN Setup                 23. System Password
         4. Internet Access Setup     24. System Maintenance
         5. DMZ Setup                 25. IP Routing Policy
                                      26. Schedule Setup
       Advanced Applications          27. VPN/IPSec Setup
         11. Remote Node Setup
         12. Static Routing Setup
         15. NAT Setup
                                      99. Exit

                           Enter Menu Selection Number:
```

Figure 21-3 Main Menu (ZyWALL 100)

The following table describes the fields in this screen.

Table 21-2 Main Menu Summary

NO.	Menu Title	FUNCTION
1	General Setup	Use this menu to set up dynamic DNS and administrative information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN and configure the backup WAN dial-up connection.

Table 21-2 Main Menu Summary

NO.	Menu Title	FUNCTION
3	LAN Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings and configure the wireless LAN port (not available on all models).
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
5	DMZ Setup (This feature is not available on all models.)	Use this menu to configure your public servers connected to the DMZ port.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure IP static routes in this menu.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter and Firewall Setup	Configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Password	Change your password in this menu (recommended).
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
25	IP Routing Policy Setup	Use this menu to configure policies for use in IP policy routing.
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN /IPSec Setup	Use this menu to configure VPN connections.
99	Exit	Use this menu to exit (necessary for remote configuration).

21.3.2 SMT Menus at a Glance

The available SMT screens vary by ZyWALL model. The following SMT overview applies to the ZyWALL 100.

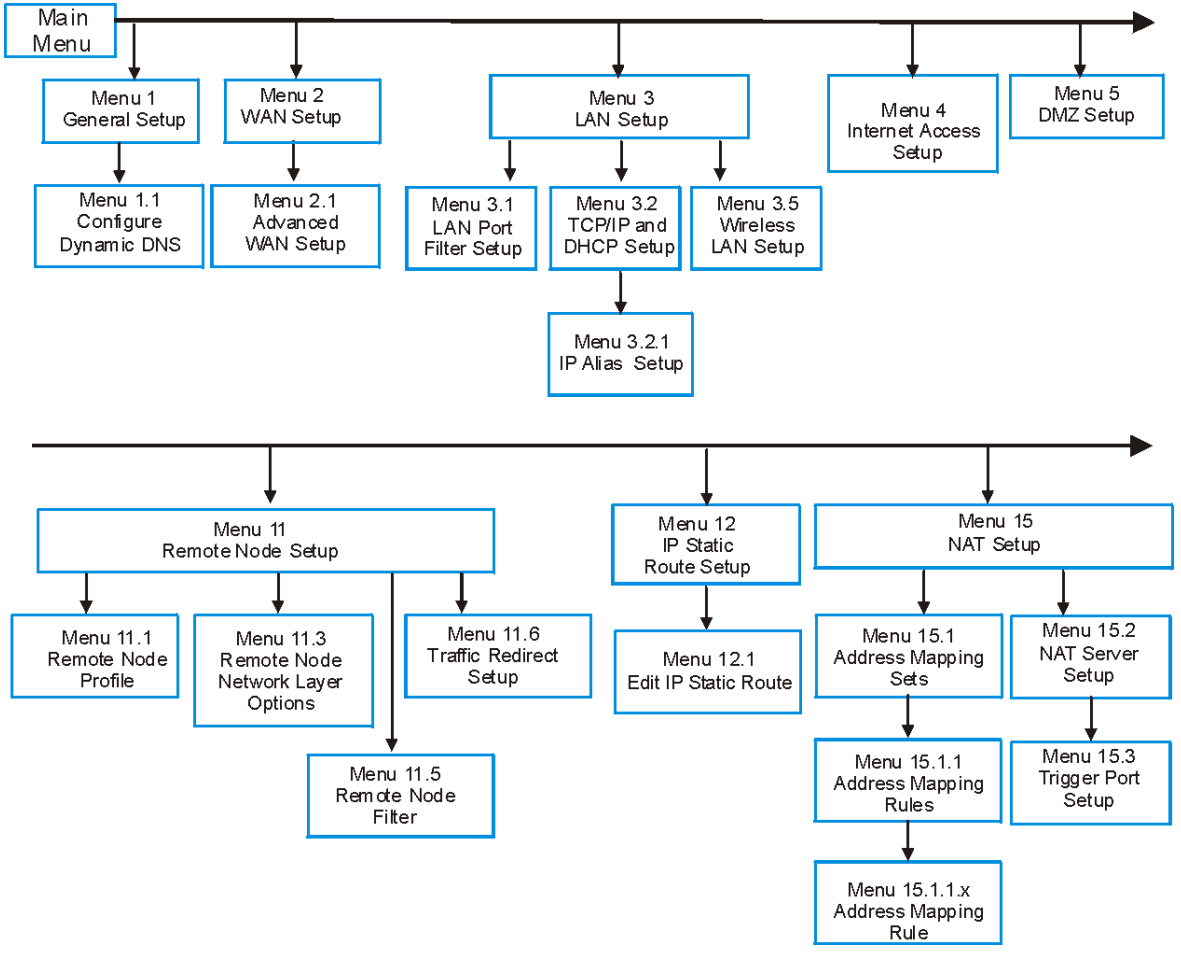


Figure 21-4 Getting Started and Advanced Applications SMT Menus

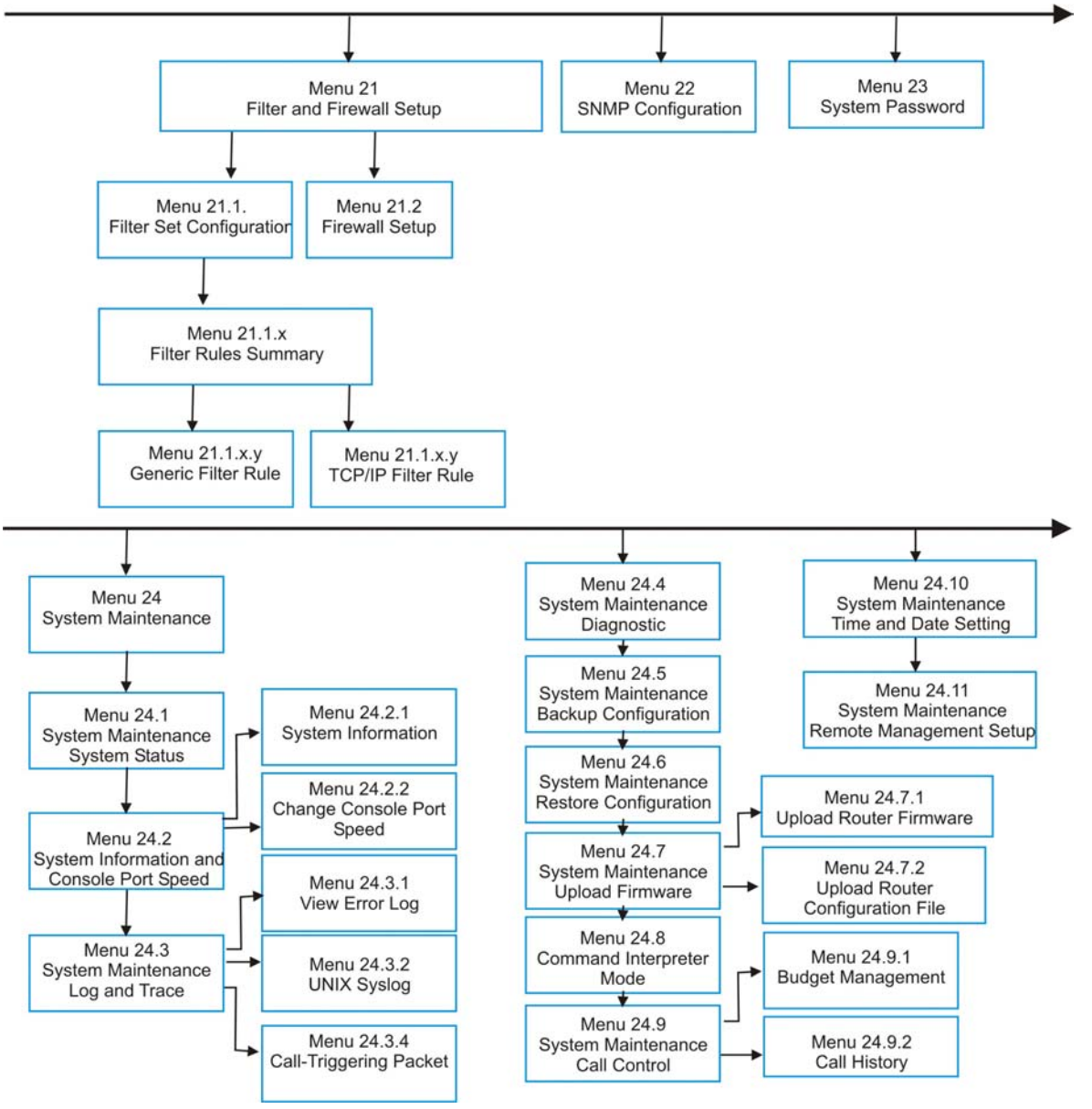


Figure 21-5 Advanced Management SMT Menus

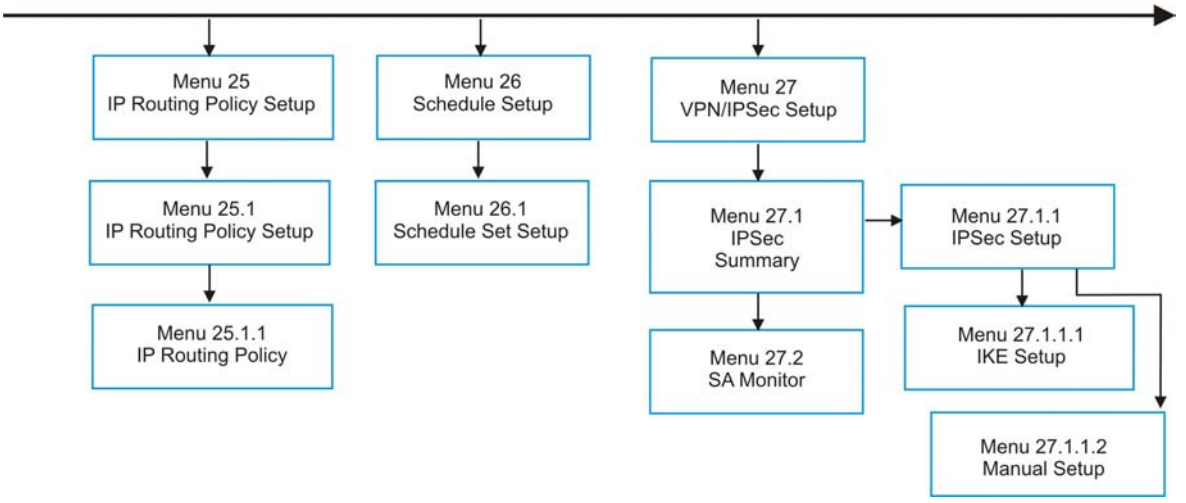


Figure 21-6 Schedule Setup and IPSec VPN Configuration SMT Menus

21.4 Changing the System Password

Change the system password by following the steps shown next.

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

```
                Menu 23 - System Password


        Old Password= ?
        New Password= ?
        Retype to confirm= ?




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

Figure 21-7 Menu 23: System Password

Step 2. Type your existing password and press [ENTER].

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

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

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

21.5 Resetting the ZyWALL

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

21.5.1 Uploading a Configuration File Via Console Port

Step 1. Download the default configuration file from the ZyXEL FTP site, unzip it and save it in a folder.

Step 2. Turn off the ZyWALL, begin a terminal emulation software session and turn on the ZyWALL again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.

Step 3. Enter "atlc" after "Enter Debug Mode" message.

Step 4. Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.

Step 5. Click **Transfer**, then **Send File** to display the following screen.

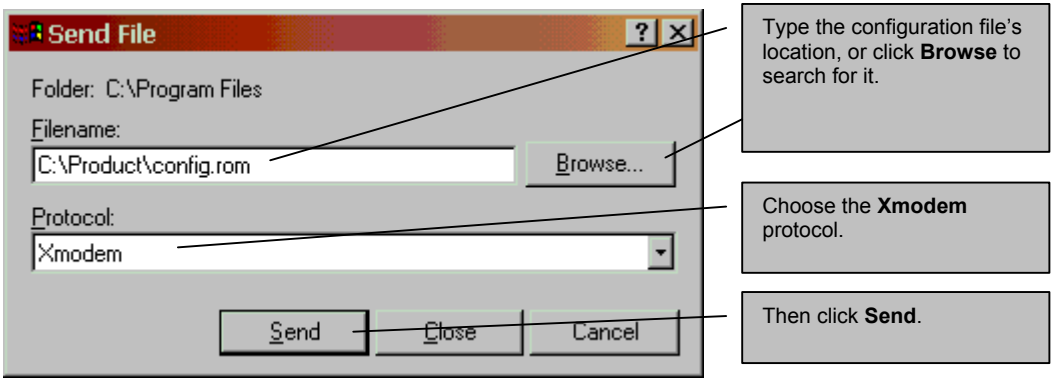


Figure 21-8 Example Xmodem Upload

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

21.5.2 Procedure To Use The Reset Button

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

Step 1. Press the **RESET** button for ten seconds, and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the ZyWALL restarts. Otherwise, go to step 2.

Step 2. Turn the ZyWALL off.

Step 3. While pressing the **RESET** button, turn the ZyWALL on.

Step 4. Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 10 or 15 seconds. This indicates that the defaults have been restored and the ZyWALL is now restarting.

Step 5. Release the **RESET** button and wait for the ZyWALL to finish restarting.

Chapter 22
SMT Menu 1 - General Setup

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

22.1 Introduction to General Setup

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

22.2 Configuring General Setup

Step 1. Enter 1 in the main menu to open **Menu 1: General Setup**.

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

```
                        Menu 1 - General Setup

                System Name= ZyWALL
                Domain Name=zyxel.com.tw
                Edit Dynamic DNS= No




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

Figure 22-1 Menu 1: General Setup

The following table describes the fields in this screen.

Table 22-1 General Setup Menu Field

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	ZyWALL

Table 22-1 General Setup Menu Field

FIELD	DESCRIPTION	EXAMPLE
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router. The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].	zyxel.com.tw
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1: Configure Dynamic DNS** discussed next.	**No** (default)
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

22.2.1 Configuring Dynamic DNS

To configure Dynamic DNS, go to **Menu 1: General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** (shown next). Not all models have every field shown.

```
                    Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= Yes
DDNSType= DynamicDNS
Host1=
Host2=
Host3=
EMAIL=
USER=
Password= ********
Enable Wildcard= No
Offline= N/A
Edit Update IP Address:
  Use Server Detected IP= Yes
  User Specified IP Address=No
  IP Address=N/A

               Press ENTER to confirm or ESC to cancel:
```

Figure 22-2 Configure Dynamic DNS

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

Table 22-2 Configure Dynamic DNS Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	**Yes**
DDNS Type	Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have a dynamic IP address(es). Select **StaticDNS** if you have a static IP address(s). Select **CustomDNS** to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.	**DynamicDNS** (default)
Host1-3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your ZyWALL supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider.	**No**
Offline	This field is only available when **CustomDNS** is selected in the **DDNS Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes**. When **Yes** is selected, http://www.dyndns.org/traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).	**Yes**
Edit Update IP Address: You can select **Yes** in either the **Use Server Detected IP** field (recommended) or the **User Specified IP Addr** field, but not both. With the **Use Server Detected IP** and **User Specified IP Addr** fields both set to **No**, the DDNS server automatically updates the IP address of the host name(s) with the ZyWALL's WAN IP address. DDNS does not work with a private IP address. When both fields are set to **No**, the ZyWALL must have a public WAN IP address in order for DDNS to work.		

Table 22-2 Configure Dynamic DNS Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Use Server Detected IP	Press [SPACE BAR] to select **Yes** and then press [ENTER] to have the DDNS server automatically update the IP address of the host name(s) with the public IP address that the ZyWALL uses or is behind. You can set this field to **Yes** whether the IP address is public or private, static or dynamic.	**Yes**
User Specified IP Address	Press [SPACE BAR] to select **Yes** and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below. Only select **Yes** if the ZyWALL uses or is behind a static public IP address.	**No**
IP Address	Enter the static public IP address if you select **Yes** in the **User Specified IP Addr** field.	**N/A**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

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

Chapter 23
WAN and Dial Backup Setup

This chapter describes how to configure the WAN using menu 2 and dial-backup using menus 2.1 and 11.1. Dial-backup applies to the ZyWALL 100 and 10W (see Table 1-1 Model Specific Features in the Web Configuration User's Guide).

23.1 Introduction to WAN and Dial Backup Setup

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

23.2 WAN Setup

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

```
                    Menu 2 - WAN Setup

MAC Address:
  Assigned By= Factory default
  IP Address= N/A

Dial-Backup:
  Active= No
  Phone Number=
  Port Speed= 115200
  AT Command String:
    Init= at&fs0=0
  Edit Advanced Setup= No
```

Figure 23-1 MAC Address Cloning in WAN Setup

The following table describes the fields in this screen.

Table 23-1 MAC Address Cloning in WAN Setup

FIELD	DESCRIPTION	EXAMPLE
MAC Address		
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose **Factory Default** to select the factory assigned default MAC Address. Choose **IP address attached on LAN** to use the MAC Address of that workstation whose IP you give in the following field.	**IP address attached on LAN**
IP Address	This field is applicable only if you choose the **IP address attached on LAN** method in the **Assigned By** field. Enter the IP address of the computer on the LAN whose MAC you are cloning.	192.168.1.35
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

23.3 Dial Backup

The Dial Backup port or CON/AUX port can be used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. This feature is not available on all models. To set up the auxiliary port (Dial Backup or CON/AUX) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the Hardware Installation chapter), then configure

1. Menu 2 - WAN Setup,
2. Menu 2.1 - Advanced WAN Setup and
3. Menu 11.1 - Remote Node Profile (Backup ISP) as shown next

Refer also to the traffic redirect section for information on an alternate backup WAN connection.

23.4 Configuring Dial Backup in Menu 2

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

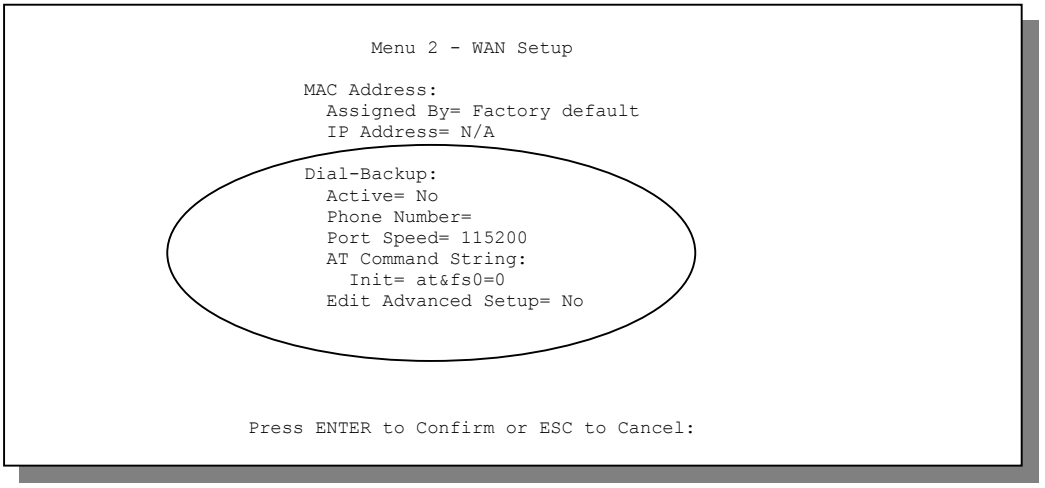


Figure 23-2 Menu 2: Dial Backup Setup

The following table describes the fields in this screen.

Table 23-2 Menu 2: Dial Backup Setup

FIELD	DESCRIPTION	EXAMPLE
Dial-Backup:		
Active	Use this field to turn the dial-backup feature on (**Yes**) or off (**No**).	**No**
Phone Number	Enter the telephone number assigned to your line by your telephone company. This field only accepts digits; do not include dashes and spaces.	1234567
Port Speed	Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.	**115200**
AT Command String:		
Init	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.	at&fs0=0
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 2.1: Advanced Setup**.	**Yes**

Table 23-2 Menu 2: Dial Backup Setup

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

23.5 Advanced WAN Setup

Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.

To edit the advanced setup for the Dial Backup port, move the cursor to the **Edit Advanced Setup** field in **Menu 2 - WAN Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].

```
                    Menu 2.1 - Advanced WAN Setup

AT Command Strings:                  Call Control:
  Dial= atdt                           Dial Timeout(sec)= 60
  Drop= ~~+++~~ath                     Retry Count= 0
  Answer= ata                          Retry Interval(sec)= N/A
                                       Drop Timeout(sec)= 20
Drop DTR When Hang Up= Yes             Call Back Delay(sec)= 15

AT Response Strings:
  CLID= NMBR =
  Called Id=
  Speed= CONNECT
```

Figure 23-3 Menu 2.1 Advanced WAN Setup

The following table describes fields in this menu.

Table 23-3 Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION	DEFAULT
AT Command Strings:		
Dial	Enter the AT Command string to make a call.	atdt

Table 23-3 Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION	DEFAULT
Drop	Enter the AT Command string to drop a call. "~" represents a one second wait, e.g., "~~~+++~~ath" can be used if your modem has a slow response time.	+++ath
Answer	Enter the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Press the [SPACE BAR] to choose either **Yes** or **No**. When **Yes** is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the "AT Command String: Drop" is sent out.	**Yes**
AT Response String:		
CLID (Calling Line Identification)	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyWALL capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR =
Called Id	Enter the keyword preceding the dialed number.	TO
Speed	Enter the keyword preceding the connection speed.	CONNECT

Table 23-4 Advanced WAN Port Setup: Call Control Parameters

FIELD	DESCRIPTION	DEFAULT
Call Control		
Dial Timeout (sec)	Enter a number of seconds for the ZyWALL to keep trying to set up an outgoing call before timing out (stopping). The ZyWALL times out and stops if it cannot set up an outgoing call within the timeout value.	60 seconds
Retry Count	Enter a number of times for the ZyWALL to retry a busy or no-answer phone number before blacklisting the number.	0 to disable the blacklist control
Retry Interval (sec)	Enter a number of seconds for the ZyWALL to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	

Table 23-4 Advanced WAN Port Setup: Call Control Parameters

FIELD	DESCRIPTION	DEFAULT
Drop Timeout (sec)	Enter a number of seconds for the ZyWALL to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20 seconds
Call Back Delay (sec)	Enter a number of seconds for the ZyWALL to wait between dropping a callback request call and dialing the co-responding callback call.	15 seconds

23.6 Remote Node Profile (Backup ISP)

Enter **2** in **Menu 11 Remote Node Setup** to open **Menu 11.1 Remote Node Profile (Backup ISP)** (shown below) and configure the setup for your Dial Backup port connection. This feature is not available on all models.

```
                Menu 11.1 - Remote Node Profile (Backup ISP)

Rem Node Name= ?                    Edit PPP Options= No
Active= Yes                         Rem IP Addr= 0.0.0.0
                                    Edit IP= No
Outgoing:                           Edit Script Options= No
  My Login=
  My Password= ********             Telco Option:
  Authen= CHAP/PAP                    Allocated Budget(min)= 0
  Pri Phone #= ?                        Period(hr)= 0
  Sec Phone #=                        Nailed-Up Connection= No

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



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

Figure 23-4 Menu 11.1 Remote Node Profile (Backup ISP)

The following table describes the fields in this screen.

Table 23-5 Fields in Menu 11.1 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice

Table 23-5 Fields in Menu 11.1 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node.	**Yes**
Outgoing		
My Login	Enter the login name assigned by your ISP for this remote node.	jim
My Password	Enter the password assigned by your ISP for this remote node.	*****
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.	**CHAP/PAP**
Pri Phone # Sec Phone #	Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.	
Edit PPP Options	Move the cursor to this field and use the space bar to select [Yes] and press [Enter] to edit the PPP options for this remote node. This brings you to Menu 11.2 - Remote Node PPP Options (see *section 23.7*).	**No** (default)
Rem IP Addr	Leave the field set to 0.0.0.0 (default) if the remote gateway has a dynamic IP address. Enter the remote gateway's IP address here if it is static.	0.0.0.0 (default)
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to M**enu 11.3 - Remote Node Network Layer Options**. See *section 23.8* for more information.	**No** (default)
Edit Script Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.4 - Remote Node Script**). See *section 23.9* for more information.	**No** (default)
Telco Option		

Table 23-5 Fields in Menu 11.1 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Allocated Budget	Enter the maximum number of minutes that this remote node may be called within the time period configured in the **Period** field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node.	0 (default)
Period(hr)	Enter the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).	0 (default)
Nailed-Up Connection	Press [SPACE BAR] to select **Yes** to set this connection to always be on, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection.	**No** (default)
Session Options		
Edit Filter sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See *section 23.10* for more details.	**No** (default)
Idle Timeout	Enter the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) that can elapse before the ZyWALL automatically disconnects the PPP connection. This option only applies when the ZyWALL initiates the call.	100 seconds (default)
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

23.7 Editing PPP Options

The ZyWALL's dial back-up feature uses PPP. To edit the remote node PPP Options, move the cursor to the **[Edit PPP Options]** field in Menu 11.1 - Remote Node Profile, and use the space bar to select **[Yes].** Press [Enter] to open Menu 11.2 as shown next.

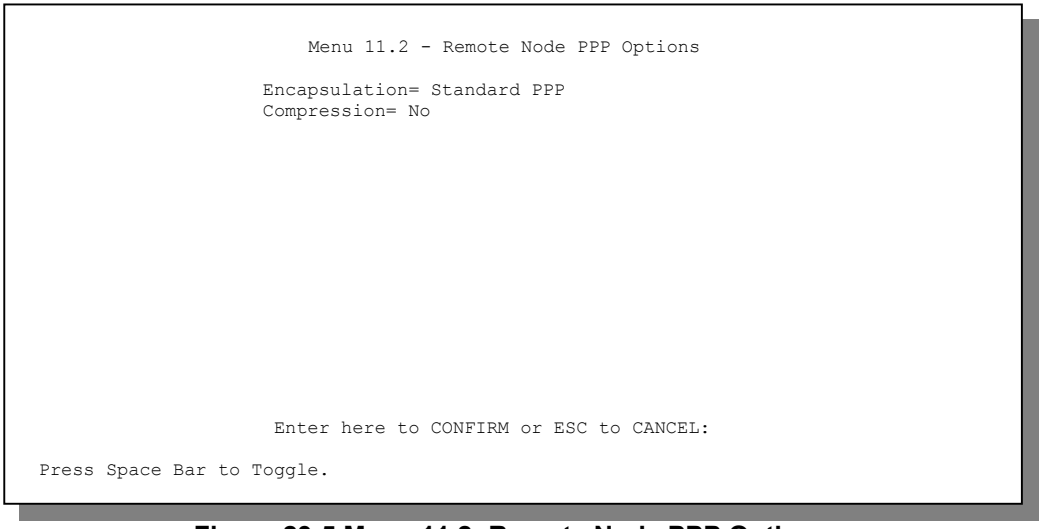


Figure 23-5 Menu 11.2: Remote Node PPP Options

This table describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

Figure 23-6 Remote Node PPP Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then [ENTER] to select **CISCO PPP** if your Dial Backup WAN device uses Cisco PPP encapsulation, otherwise select **Standard PPP**.	**Standard PPP** (default)
Compression	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable or **No** to disable Stac compression.	**No** (default)

23.8 Editing TCP/IP Options

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

```
Menu 11.3 - Remote Node Network Layer Options

          Rem IP Addr= 0.0.0.0
          Rem Subnet Mask= 0.0.0.0
          My WAN Addr= 0.0.0.0

          Network Address Translation= None
          Metric= 15
          Private= No
          RIP Direction= Both
            Version= RIP-2B
          Multicast= None




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

Figure 23-7 Menu 11.3: Remote Node Network Layer Options

The following table describes the fields in this screen.

Table 23-6 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Rem IP Address	Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Enter the remote gateway's IP address here if you know it (static).	0.0.0.0 (default)
Rem IP Subnet Mask	Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Enter the remote gateway's subnet mask here if you know it (static).	0.0.0.0 (default)
My WAN Addr	Leave the field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Enter your WAN IP address here if you know it (static). This is the address assigned to your local ZyWALL, not the remote router.	0.0.0.0 (default)

Table 23-6 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Press [SPACE BAR] and then [ENTER] to select either **Full Feature, None** or **SUA Only.** Choose **None** to disable NAT**.** Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set! See the Network Address Translation (NAT) chapter for a full discussion on this feature.	**None** (default)
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes. The smaller the number, the higher priority the route has.	15 (default)
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**No** (default)
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the **RIP direction** from **Both/ None/In Only**/**Out Only** and **None**.	**Both** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-1**
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See the LAN Setup chapter for more information on this feature.	**None** (default)

Table 23-6 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

23.9 Editing Login Script

For some remote gateways, text login is required before PPP negotiation is started. The ZyWALL provides a script facility for this purpose. The script has six programmable sets; each set is composed of an 'Expect' string and a 'Send' string. After matching a message from the server to the 'Expect' field, the ZyWALL returns the set's 'Send' string to the server.

For instance, a typical login sequence starts with the server printing a banner, a login prompt for you to enter the user name and a password prompt to enter the password:

```
Welcome to Acme, Inc.
Login: myLogin
Password:
```

To handle the first prompt, you specify "`ogin: `" as the 'Expect' string and "`myLogin`" as the 'Send' string in set 1. The reason for leaving out the leading "`L`" is to avoid having to know exactly whether it is upper or lower case. Similarly, you specify "`word: `" as the 'Expect' string and your password as the 'Send' string for the second prompt in set 2.

You can use two variables, `$USERNAME` and `$PASSWORD` (all UPPER case), to represent the actual user name and password in the script, so they will not show in the clear. They are replaced with the outgoing login name and password in the remote node when the ZyWALL sees them in a 'Send' string. Please note that both variables must been entered exactly as shown. No other characters may appear before or after, either, i.e., they must be used alone in response to login and password prompts.

Please note that the ordering of the sets is significant, i.e., starting from set 1, the ZyWALL will wait until the 'Expect' string is matched before it proceeds to set 2, and so on for the rest of the script. When both the 'Expect' and the 'Send' fields of the current set are empty, the ZyWALL will terminate the script processing and start PPP negotiation. This implies two things: first, the sets must be contiguous; the sets after an empty one are ignored. Second, the last set should match the final message sent by the server. For instance, if the server prints:

```
login successful.
Starting PPP...
```

after you enter the password, then you should create a third set to match the final "`PPP...`" but without a "Send" string. Otherwise, the ZyWALL will start PPP prematurely right after sending your password to the server.

If there are errors in the script and it gets stuck at a set for longer than the "Dial Timeout" in menu 2 (default 60 seconds), the ZyWALL will timeout and drop the line. To debug a script, go to Menu 24.4 to initiate a

manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.

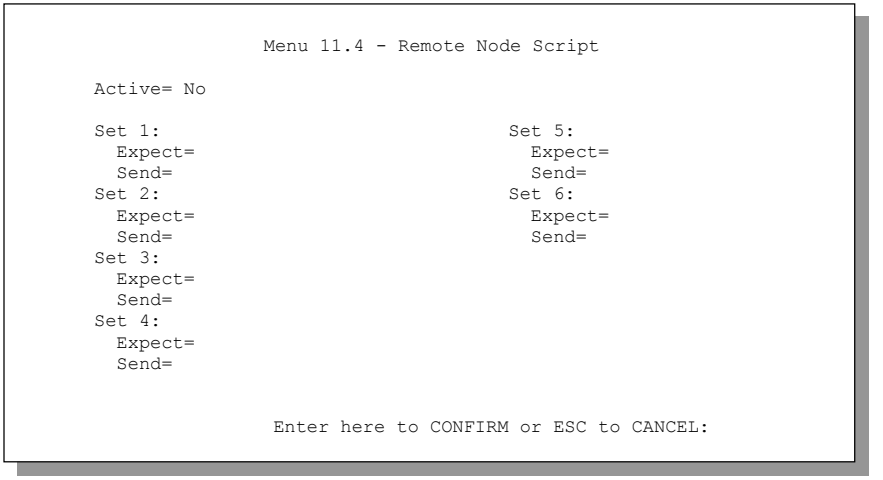


Figure 23-8 Menu 11.4 – Remote Node Setup Script

The following table describes the fields in this screen.

Table 23-7 Remote Node Script Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] and then [ENTER] to select either **Yes** to enable the AT strings or **No** to disable them.	**No** (default)
Set 1-6: Expect	Enter an Expect string to match. After matching the Expect string, the ZyWALL returns the string in the **Send** field.	
Set 1-6: Send	Enter a string to send out after the Expect string is matched.	0.0.0.0

23.10 Remote Node Filter

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

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to four filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. Please refer to the *Filters* chapter for more information on defining the filters.

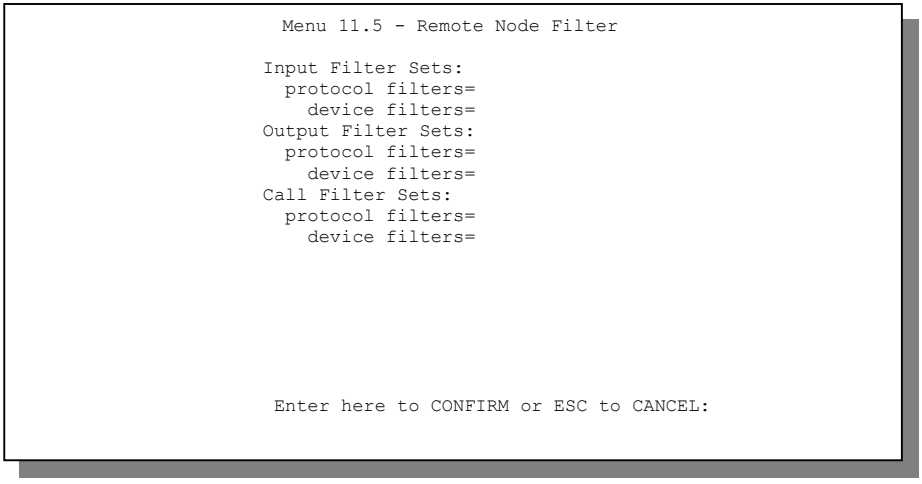


Figure 23-9 Menu 11.5: Dial Backup Remote Node Filter

Chapter 24
LAN Setup

*This chapter describes how to configure the LAN using **Menu 3: LAN Setup**. Wireless LAN is available on the ZyWALL 10W, 30W and 100 models.*

24.1 Introduction to LAN Setup

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

24.2 Accessing the LAN Menus

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

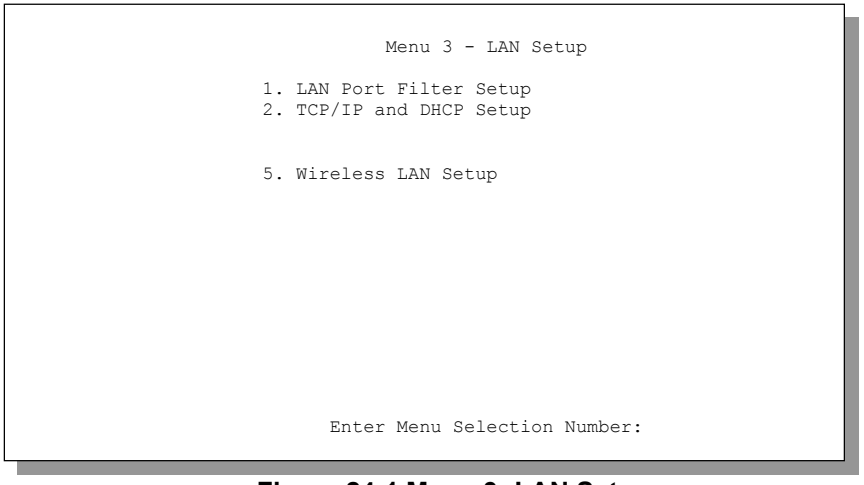


Figure 24-1 Menu 3: LAN Setup

24.3 LAN Port Filter Setup

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

```
                Menu 3.1 - LAN Port Filter Setup

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


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

Figure 24-2 Menu 3.1: LAN Port Filter Setup

24.4 TCP/IP and DHCP Ethernet Setup Menu

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

```
                        Menu 3 - LAN Setup

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


                  5. Wireless LAN Setup

                        Enter Menu Selection Number:
```

Figure 24-3 Menu 3: TCP/IP and DHCP Setup

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

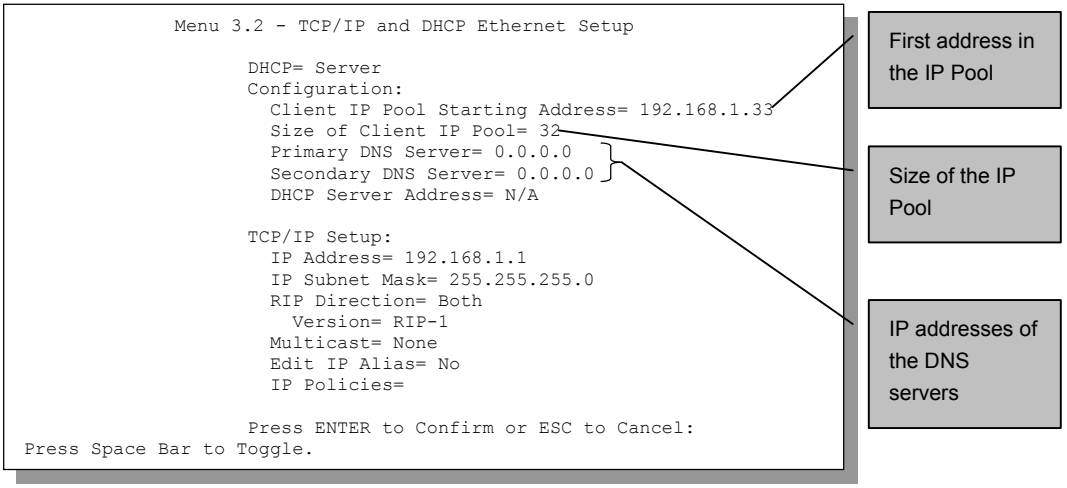


Figure 24-4 Menu 3.2: TCP/IP and DHCP Ethernet Setup

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

Table 24-1 DHCP Ethernet Setup Menu Fields

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

Table 24-1 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP Server Address	If **Relay** is selected in the **DHCP** field above, then type the IP address of the actual, remote DHCP server here.	

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

LAN and DMZ IP addresses must be on separate subnets.

Table 24-2 LAN TCP/IP Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup:		
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select **None** (default) to disable it.	**None**
Edit IP Alias	The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.2.1	**Yes**
IP Policies	You can apply up to four IP Policy sets (from twelve) by typing their numbers separated by commas.	2,7,9,11
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

24.4.1 IP Alias Setup

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

```
                Menu 3.2.1 - IP Alias Setup

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

                    Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

Figure 24-5 Menu 3.2.1: IP Alias Setup

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

Table 24-3 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Alias	Choose **Yes** to configure the LAN network for the ZyWALL.	**Yes**
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.	192.168.2.1
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only, Out Only** or **None**.	**None**
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**

Table 24-3 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyWALL.	1
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyWALL.	2
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

24.5 Wireless LAN Setup

Use menu 3.5 to set up your ZyWALL as the wireless access point.
See the *Web Configurator User's Guide* for instructions on WEP and configuring the MAC address filter.

If you are configuring the ZyWALL from a computer connected to the wireless LAN and you change the ZyWALL's ESSID or WEP settings, you will lose your wireless connection when you press [ENTER] to confirm. You must then change the wireless settings of your computer to match the ZyWALL's new settings.

From the main menu, enter 3 to open **Menu 3 – LAN Setup** to configure the Wireless LAN setup. To edit the wireless LAN configuration, enter 5 to open **Menu 3.5 – Wireless LAN Setup** as shown next.

```
Menu 3.5 - Wireless LAN Setup

    Enable Wireless LAN= No
    ESSID= Wireless
    Hide ESSID= No
    Channel ID= CH01 2412MHz
    RTS Threshold= 2432
    Frag. Threshold= 2432
    WEP= Disable
      Default Key= N/A
      Key1= N/A
      Key2= N/A
      Key3= N/A
      Key4= N/A
    Edit MAC Address Filter= No
```

Figure 24-6 Menu 3.5 – Wireless LAN Setup

The settings of all client stations on the wireless LAN must match those of the ZyWALL.

Follow the instructions in the next table on how to configure the wireless LAN parameters.

Table 24-4 Wireless LAN Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Enable Wireless LAN	Press [SPACE BAR] to select **Yes** to turn on the wireless LAN. The wireless LAN is off by default. Configure wireless LAN security features such as Mac filters and 802.1X before you turn on the wireless LAN.	**No** (default)
ESSID	(Extended Service Set IDentification) The ESSID identifies the Service Set the station is to connect to. Wireless clients associating to the Access Point must have the same ESSID. Enter a descriptive name (up to 32 characters) for the wireless LAN.	Wireless
Hide ESSID	Press [SPACE BAR] to select **Yes** to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.	**No** (default)
Channel ID	This allows you to set the operating frequency/channel depending on your particular region. Use the [SPACE BAR] to select a channel. • CH01 2412 MHz / CH02 2417 MHz ~ CH11 2462 MHz (North America/FCC) • CH01 2412 MHz / CH02 2417 MHz ~ CH13 2472 MHz (Europe CE/ ETSI) • CH01 2412 MHz / CH02 2417 MHz ~ Ch14 2484 MHz (Japan) • CH10 2457 MHz / CH11 2462 MHz (Spain) • CH10 2457 MHz / CH11 2462 MHz ~ CH13 2472 MHz (France)	**CH01 2412 MHz**
RTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **0** and **2432**.	2432 (default)
Frag. Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **256** and **2432**.	2432 (default)
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

The ZyWALL LAN Ethernet and wireless ports can transparently communicate with each other (transparent bridge).

Chapter 25
DMZ Setup

*This chapter describes how to configure the ZyWALL 100's DMZ using **Menu 5: DMZ Setup**.*

25.1 Configuring DMZ Setup

From the main menu, enter 5 to open **Menu 5 – DMZ Setup**.

```
                    Menu 5 - DMZ Setup


                1. DMZ Port Filter Setup
                2. TCP/IP Setup




                   Enter Menu Selection Number:
```

Figure 25-1 Menu 5: DMZ Setup

25.2 DMZ Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to your public server(s) traffic. This feature is not available on all models.

```
                Menu 5.1 - DMZ Port Filter Setup

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


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

Figure 25-2 Menu 5.1: DMZ Port Filter Setup

25.3 TCP/IP Setup

For more detailed information about RIP setup, IP Multicast and IP alias, please refer to the LAN chapter.

25.3.1 IP Address

From the main menu, enter 5 to open **Menu 5 - DMZ Setup** to configure TCP/IP (RFC 1155).

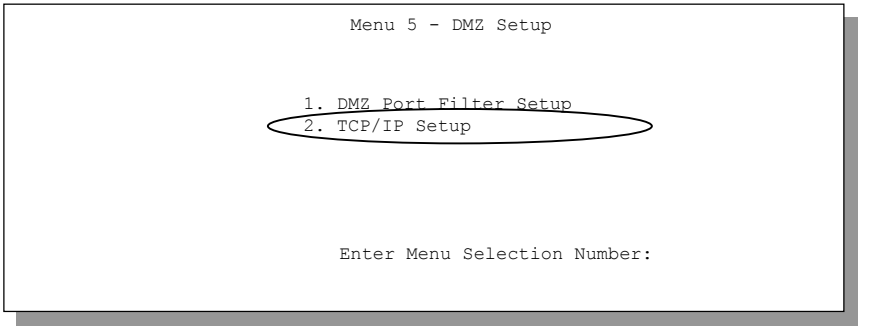


Figure 25-3 Menu 5: TCP/IP Setup

From menu 5, select the submenu option **2. TCP/IP Setup** and press [ENTER]. The screen now displays **Menu 5.2: TCP/IP Setup**, as shown next.

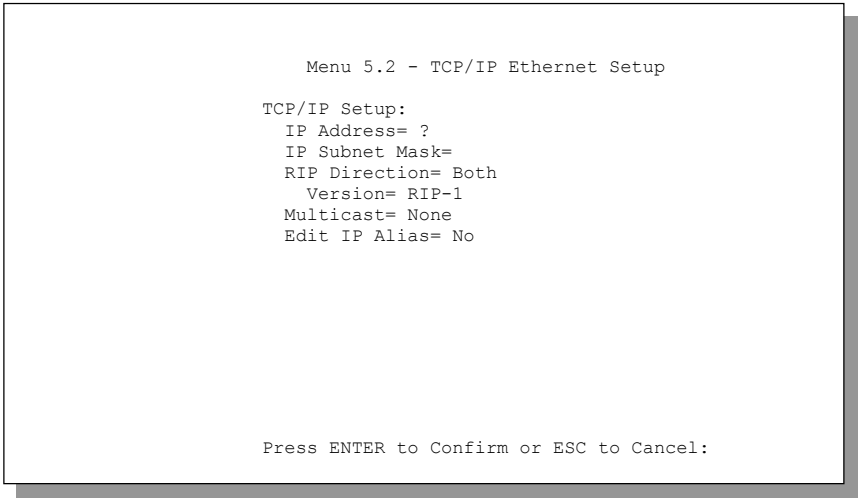


Figure 25-4 Menu 5.2: TCP/IP Setup

The TCP/IP setup fields are the same as the ones in **Menu 3.2 TCP/IP Ethernet Setup**. Each public server will need a unique IP address. Refer to section *24.4* for information on how to configure these fields.

DMZ and LAN IP addresses must be on separate subnets.
You must also configure NAT for the DMZ port (see the *NAT* chapter) in menus 15.1 and 15.2.

25.3.2 IP Alias Setup

You must use menu 5.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network. Pressing [ENTER] opens **Menu 5.2.1 - IP Alias Setup**, as shown next.

```
                          Menu 5.2.1 - IP Alias Setup

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

                         Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

Figure 25-5 Menu 5.2.1: IP Alias Setup

Refer to *Table 24-3* for instructions on configuring IP Alias parameters.

Chapter 26
Internet Access

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

26.1 Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your ZyWALL to access the Internet. There are three different menu 4 screens depending on whether you chose **Ethernet, PPTP** or **PPPoE Encapsulation**. Contact your ISP to determine what encapsulation type you should use.

26.2 Ethernet Encapsulation

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

```
            Menu 4 - Internet Access Setup

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

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



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

Figure 26-1 Menu 4: Internet Access Setup (Ethernet)

The following table describes the fields in this screen.

Table 26-1 Menu 4: Internet Access Setup Menu Fields

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.

Table 26-1 Menu 4: Internet Access Setup Menu Fields

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **Ethernet**. The encapsulation method influences your choices for the **IP Address** field.
Service Type	Press [SPACE BAR] and then [ENTER] to select **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method) or **RR-Telstra**. Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
Note: DSL users must choose the **Standard** option only. The **My Login**, **My Password** and **Login Server** fields are not applicable in this case.	
My Login	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
Login Server	The ZyWALL will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address Assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.

Table 26-1 Menu 4: Internet Access Setup Menu Fields

FIELD	DESCRIPTION
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT**.** Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set! Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

26.3 Configuring the PPTP Client

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

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

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

```
                Menu 4 - Internet Access Setup

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

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


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

Figure 26-2 Internet Access Setup (PPTP)

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

Table 26-2 New Fields in Menu 4 (PPTP) Screen

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

26.4 Configuring the PPPoE Client

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

```
                Menu 4 - Internet Access Setup

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

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


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

Figure 26-3 Internet Access Setup (PPPoE)

The following table describes the fields in this screen.

Table 26-3 New Fields in Menu 4 (PPPoE) screen

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

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

26.5 Basic Setup Complete

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

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

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

Part XII:

SMT Advanced Applications

This part covers setting up remote nodes, IP static routes and Network Address Translation. It also covers the SMT firewall menu, filters and SNMP.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 27
Remote Node Setup

This chapter shows you how to configure a remote node.

27.1 Introduction to Remote Node Setup

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

27.2 Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 Remote Node Setup** (shown below). Then enter **1** to open **Menu 11.1 Remote Node Profile** and configure the setup for your regular ISP. Enter **2** to open **Menu 11.1 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection (see the *WAN and Dial Backup Setup* chapter).

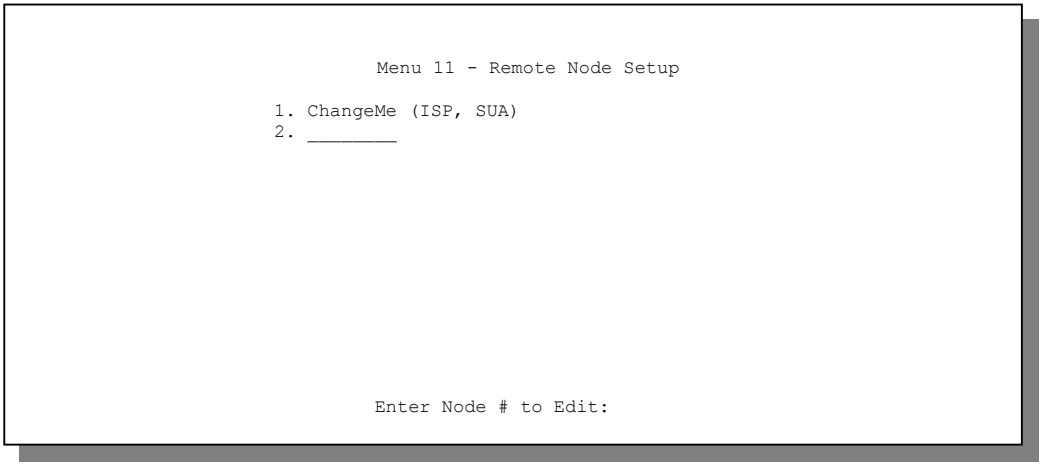


Figure 27-1 Menu 11 Remote Node Setup

27.3 Remote Node Profile Setup

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

27.3.1 Ethernet Encapsulation

There are two variations of menu 11.1 depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation.** You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

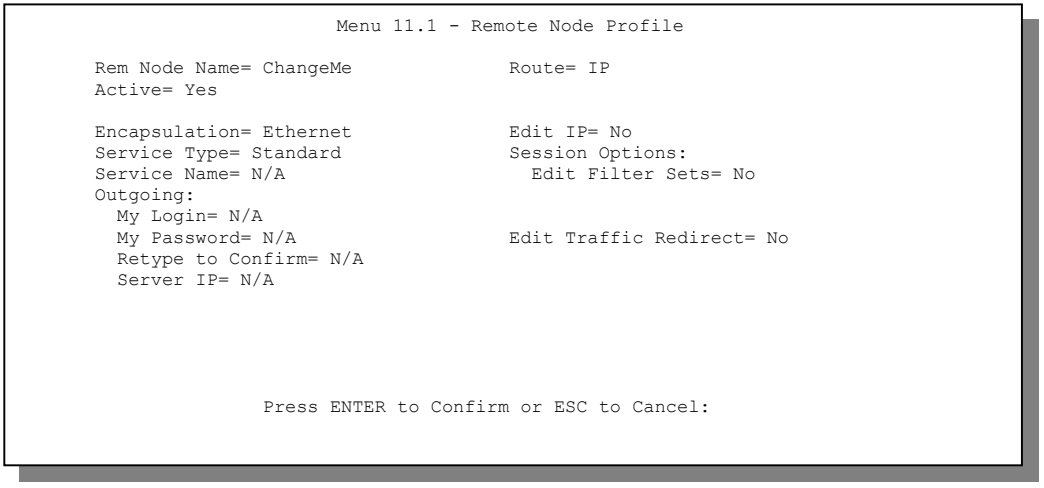


Figure 27-2 Menu 11.1: Remote Node Profile for Ethernet Encapsulation

The following table describes the fields in this screen.

Table 27-1 Fields in Menu 11.1

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node).	**Yes**
Encapsulation	**Ethernet** is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to **PPPoE** or **PPTP** encapsulation.	**Ethernet**
Service Type	Press [SPACE BAR] and then [ENTER] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method) or **RR-Manager** (RoadRunner Manager authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.	**Standard**
Service Name	If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here. Only valid with **PPPoE** encapsulation.	poellc
Outgoing My Login	This field is applicable for **PPPoE** encapsulation only. Enter the login name assigned by your ISP when the ZyWALL calls this remote node. Some ISPs append this field to the **Service Name** field above (e.g., jim@poellc) to access the PPPoE server.	jim

Table 27-1 Fields in Menu 11.1

FIELD	DESCRIPTION	EXAMPLE
My Password	Enter the password assigned by your ISP when the ZyWALL calls this remote node. Valid for **PPPoE** encapsulation only.	*****
Retype to Confirm	Type your password again to make sure that you have entered it correctly.	*****
Server IP	This field is valid only when **RoadRunner** is selected in the **Service Type** field. The ZyWALL will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.	
Route	This field refers to the protocol that will be routed by your ZyWALL – IP is the only option for the ZyWALL 100.	**IP**
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to M**enu 11.3 - Remote Node Network Layer Options**.	**No** (default)
Session Options Edit Filter sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details.	**No** (default)
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

27.3.2 PPPoE Encapsulation

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

```
                        Menu 11.1 - Remote Node Profile

        Rem Node Name= ChangeMe             Route= IP
        Active= Yes

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

                                            Edit Traffic Redirect= No

                     Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle.
```

Figure 27-3 Menu 11.1: Remote Node Profile for PPPoE Encapsulation

Outgoing Authentication Protocol

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

Nailed-Up Connection

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

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

The following table describes the fields not already described in *Table 27-1*.

Metric

See the *Metric* section in the *WAN and Dial Backup Setup* chapter for details on the **Metric** field.

Table 27-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific)

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

27.3.3 PPTP Encapsulation

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

```
                        Menu 11.1 - Remote Node Profile

      Rem Node Name= ChangeMe              Route= IP
      Active= Yes

      Encapsulation= PPTP                  Edit IP= No
      Service Type= Standard               Telco Option:
      Service Name=N/A                       Allocated Budget(min)= 0
      Outgoing=                              Period(hr)= 0
        My Login=                            Schedules=
        My Password= ********                Nailed-up Connections=
        Retype to Confirm= ********
        Authen= CHAP/PAP
       PPTP :                              Session Options:
        My IP Addr=                          Edit Filter Sets= No
        My IP Mask=                          Idle Timeout(sec)= 100
        Server IP Addr=
        Connection ID/Name=                Edit Traffic Redirect= No


                     Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Figure 27-4 Menu 11.1: Remote Node Profile for PPTP Encapsulation

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

Table 27-3 Fields in Menu 11.1 (PPTP Encapsulation)

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then [ENTER] to select **PPTP**. You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.	**PPTP**
My IP Addr	Enter the IP address of the WAN Ethernet port.	10.0.0.140
My IP Mask	Enter the subnet mask of the WAN Ethernet port.	255.255.255.0
My Server IP Addr	Enter the IP address of the ANT modem.	10.0.0.138
Connection ID/Name	Enter the connection ID or connection name in the ANT. It must follow the “c:id” and “n:name” format. This field is optional and depends on the requirements of your DSL modem.	N:My ISP
Schedules	You can apply up to four schedule sets here. For more details refer to the *Call Schedule Setup* chapter.	

Table 27-3 Fields in Menu 11.1 (PPTP Encapsulation)

FIELD	DESCRIPTION	EXAMPLE
Nailed-Up Connections	Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to make the connection to this remote node a nailed-up connection.	**No**

27.4 Edit IP

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

```
                Menu 11.3 - Remote Node Network Layer Options

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

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




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

Figure 27-5 Menu 11.3: Remote Node Network Layer Options for Ethernet Encapsulation

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this screen.

Table 27-4 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.	**Dynamic** (default)
(Rem) IP Address	If you have a Static IP Assignment, enter the IP address assigned to you by your ISP.	

Table 27-4 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
(Rem) IP Subnet Mask	If you have a Static IP Assignment, enter the subnet mask assigned to you.	
Gateway IP Addr	This field is applicable to **Ethernet** encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.	
My WAN Addr	This field is applicable to **PPPoE** and **PPTP** encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your ZyWALL. Note that this is the address assigned to your local ZyWALL, not the remote router.	
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT**.** Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set! See the *NAT chapter* for a full discussion on this feature.	**SUA Only** (default)
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see the *Metric* section in the *WAN and Dial Backup Setup* chapter) The smaller the number, the higher priority the route has.	1
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**No**

Table 27-4 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from **Both**/ **None**/**In Only**/**Out Only**. See the *LAN Setup* chapter for more information on RIP. The default for RIP on the WAN side is **None**. It is recommended that you do not change this setting.	**None** (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**/**RIP-2B**/**RIP-2M** or **None**.	N/A
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2)**. Press [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See the *LAN Setup* chapter for more information on this feature.	**None** (default)
Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

27.5 Remote Node Filter

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

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

```
                    Menu 11.5 - Remote Node Filter

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

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

Figure 27-6 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)

```
                  Menu 11.5 - Remote Node Filter

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




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

Figure 27-7 Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)

To configure the parameters for traffic redirect, enter 11 from the main menu to display **Menu 11.1—Remote Node Profile** as shown next.

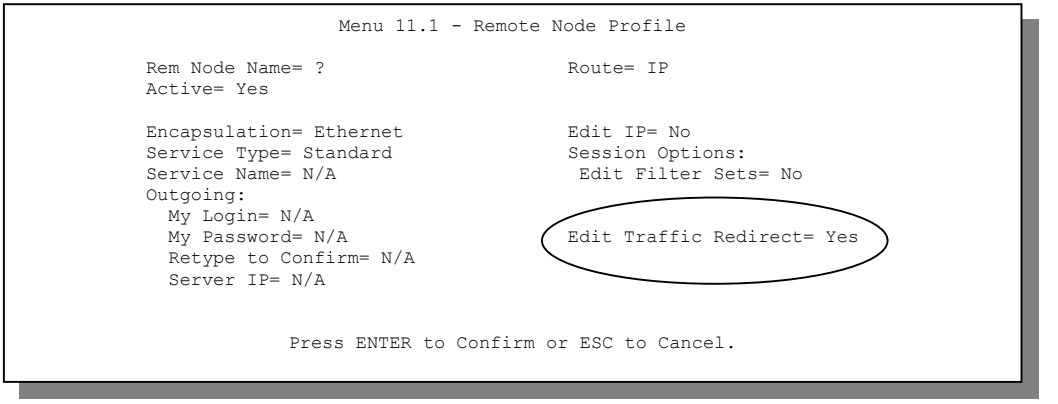


Figure 27-8 Menu 11.1: Remote Node Profile

To configure traffic redirect properties, press [SPACE BAR] to select **Yes** in the **Edit Traffic Redirect** field and then press [ENTER].

Table 27-5 Menu 11.1: Remote Node Profile (Traffic Redirect Field)

FIELD	DESCRIPTION	EXAMPLE
Edit Traffic Redirect	Press [SPACE BAR] to select **Yes** or **No**. Select **No** (default) if you do not want to configure this feature. Select **Yes** and press [ENTER] to configure **Menu 11.6 — Traffic Redirect Setup**.	**Yes**
Press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

27.5.1 Traffic Redirect Setup

Configure parameters that determine when the ZyWALL will forward WAN traffic to the backup gateway using **Menu 11.6 — Traffic Redirect Setup**.

```
                Menu 11.6 - Traffic Redirect Setup


Active= Yes
Configuration:
  Backup Gateway IP Address= 0.0.0.0
  Metric= 15
  Check WAN IP Address= 0.0.0.0
    Fail Tolerance= 2
    Period (sec)= 5
    Timeout (sec)= 3

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

Figure 27-9 Menu 11.6: Traffic Redirect Setup

The following table describes the fields in this screen.

Table 27-6 Traffic Redirect Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup. The default is **No**. When the **Active** field is **Yes**, you must configure every field in this screen unless you are using PPPoE or PPTP encapsulation (except **Check WAN IP Address** and **Timeout**). If you don't configure these fields and are using PPTP or PPPoE encapsulation, then the ZyWALL checks the PPPoE channel or PPTP tunnel to determine if the WAN connection is down.	**Yes**
Configuration:		

Table 27-6 Traffic Redirect Setup

FIELD	DESCRIPTION	EXAMPLE
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates.	0.0.0.0
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see the *Metric* section in the *WAN and Dial Backup Setup* chapter) The smaller the number, the higher priority the route has.	15 (default)
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your ZyWALL's WAN accessibility. The ZyWALL uses the default gateway IP address if you do not enter an IP address here. If you are using PPTP or PPPoE Encapsulation, enter "0.0.0.0" to configure the ZyWALL to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.	0.0.0.0
Fail Tolerance	Enter the number of times your ZyWALL may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number.	2
Period (sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.	5
Timeout (sec)	Enter the number of seconds the ZyWALL waits for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The number in this field should be less than the number in the **Period** field. Three to 50 is usually a good number. The WAN connection is considered "down" after the ZyWALL times out the number of times specified in the **Fail Tolerance** field.	3
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

Chapter 28
IP Static Route Setup

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

28.1 IP Static Route Setup

Enter 12 from the main menu. Select one of the IP static routes as shown next to configure IP static routes in menu 12. 1.

```
                Menu 12 - IP Static Route Setup

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



                Enter selection number:
```

Figure 28-1 Menu 12: IP Static Route Setup (ZyWALL 10W)

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

```
                Menu 12.1 - Edit IP Static Route


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


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

Figure 28-2 Menu 12. 1: Edit IP Static Route

`The following table describes the IP Static Route Menu fields.

Table 28-1 IP Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyWALL; over the WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see the *Metric* section in the *WAN and Dial Backup Setup* chapter). The smaller the number, the higher priority the route has.

Table 28-1 IP Static Route Menu Fields

FIELD	DESCRIPTION
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
Once you have completed filling in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.	

Chapter 29
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

29.1 Using NAT

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyWALL.

29.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See *section 29.2.1* for a detailed description of the NAT set for SUA. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in the *Web Configurator User's Guide.*

1. **Choose** SUA Only **if you have just one public WAN IP address for your ZyWALL.**
2. **Choose** Full Feature **if you have multiple public WAN IP addresses for your ZyWALL.**

29.1.2 Applying NAT

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

.

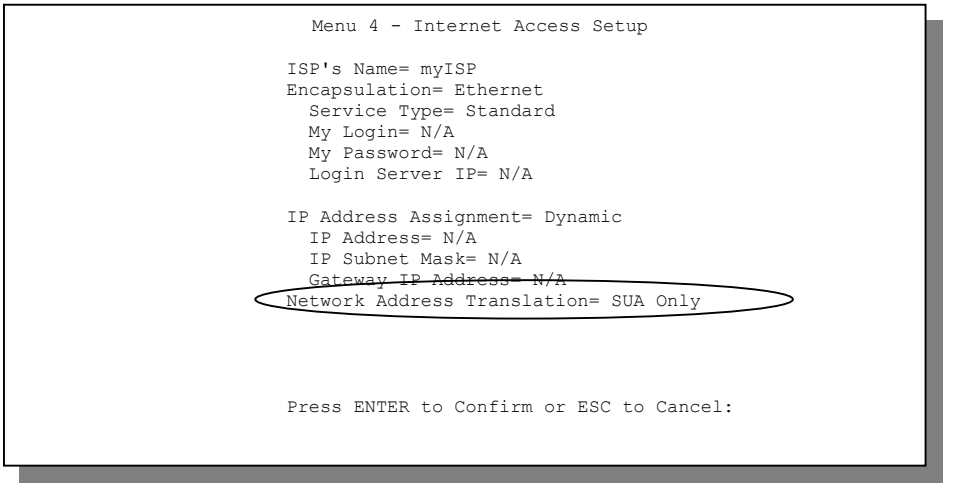


Figure 29-1 Menu 4: Applying NAT for Internet Access

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

Step 1. Enter 11 from the main menu.

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

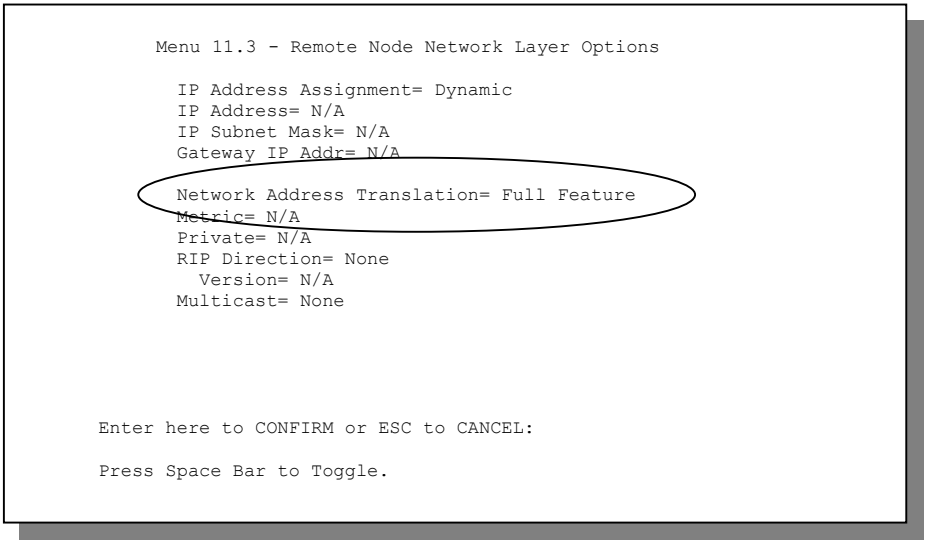


Figure 29-2 Menu 11.3: Applying NAT to the Remote Node

The following table describes the fields in this screen.

Table 29-1 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION	OPTIONS
Network Address Translation	When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see *section 29.2.1* for further discussion). You can configure any of the mapping types described in the *Web Configurator User's Guide.* Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL. When you select **Full Feature** you must configure at least one address mapping set!	**Full Feature**
	NAT is disabled when you select this option.	**None**
	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see *section 29.2.1*). Choose **SUA Only** if you have just one public WAN IP address for your ZyWALL.	**SUA Only**

29.2 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN and the DMZ. You can see two NAT address mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN and DMZ servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in the chapter on NAT web configurator screens for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

```
                    Menu 15 — NAT Setup

          1.    Address Mapping Sets
          2.    Server Set
          3.    Trigger Port Setup



                Enter Menu Selection Number:
```

Figure 29-3 Menu 15: NAT Setup

Configure DMZ and LAN IP addresses in NAT menus 15.1 and 15.2. DMZ IP addresses must be on subnets separate from LAN IP addresses.

29.2.1 Address Mapping Sets

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

```
                Menu 15.1 — Address Mapping Sets

            1.
          255. SUA (read only)









                Enter Menu Selection Number:
```

Figure 29-4 Menu 15.1: Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 29.1.1)*. The fields in this menu cannot be changed.

```
                        Menu 15.1.255 - Address Mapping Rules

  Set Name= SUA

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


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

Figure 29-5 Menu 15.1.255: SUA Address Mapping Rules

The following table explains the fields in this screen.

Menu 15.1.255 is read-only.

Table 29-2 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP	**Local Start IP** is the starting local IP address (ILA).	0.0.0.0
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the start IP is 0.0.0.0 and the end IP is 255.255.255.255.	255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0

Table 29-2 SUA Address Mapping Rules

FIELD	DESCRIPTION	XAMPLE
Global End IP	This is the ending global IP address (IGA).	
Type	These are the mapping types discussed above. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.		

User-Defined Address Mapping Sets

Now look at option 1 in menu 15.1. Enter 1 to bring up this menu. Look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

The entire set will be deleted if you leave the Set Name **field blank and press [ENTER] are the bottom of the screen.**

```
                        Menu 15.1.1 - Address Mapping Rules

 Set Name= NAT_SET

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

                  Action= Edit          Select Rule=

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

Figure 29-6 Menu 15.1.1: First Set

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

Ordering Your Rules

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

Table 29-3 Fields in Menu 15.1.1

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

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

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

An IP End address must be numerically greater than its corresponding IP Start address.

```
                Menu 15.1.1.1 Address Mapping Rule

          Type= One-to-One

          Local IP:
            Start=
            End  = N/A

          Global IP:
            Start=
            End  = N/A



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

Figure 29-7 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

The following table describes the fields in this screen.

Table 29-4 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the *Web Configurator User's* Guide. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 29.4.3* for an example.	**One-to-One**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	Enter the starting local IP address (ILA).	0.0.0.0
End	Enter the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.	N/A
Global IP		
Start	Enter the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.	0.0.0.0
End	Enter the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.	N/A

Table 29-4 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.		

29.3 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

Step 1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**

Step 2. Enter 2 to go to **Menu 15.2 - NAT Server Setup**.

Step 3. Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

Step 4. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

Step 5. Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

```
                    Menu 15.2 - NAT Server Setup


 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------------
   1.     Default          Default        0.0.0.0
   2.       21               25           192.168.1.33
   3.       0                0            0.0.0.0
   4.       0                0            0.0.0.0
   5.       0                0            0.0.0.0
   6.       0                0            0.0.0.0
   7.       0                0            0.0.0.0
   8.       0                0            0.0.0.0
   9.       0                0            0.0.0.0
  10.       0                0            0.0.0.0
  11.       0                0            0.0.0.0
  12.       1026             1026         RR Reserved

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

Figure 29-8 Menu 15.2: NAT Server Setup (ZyWALL 10)

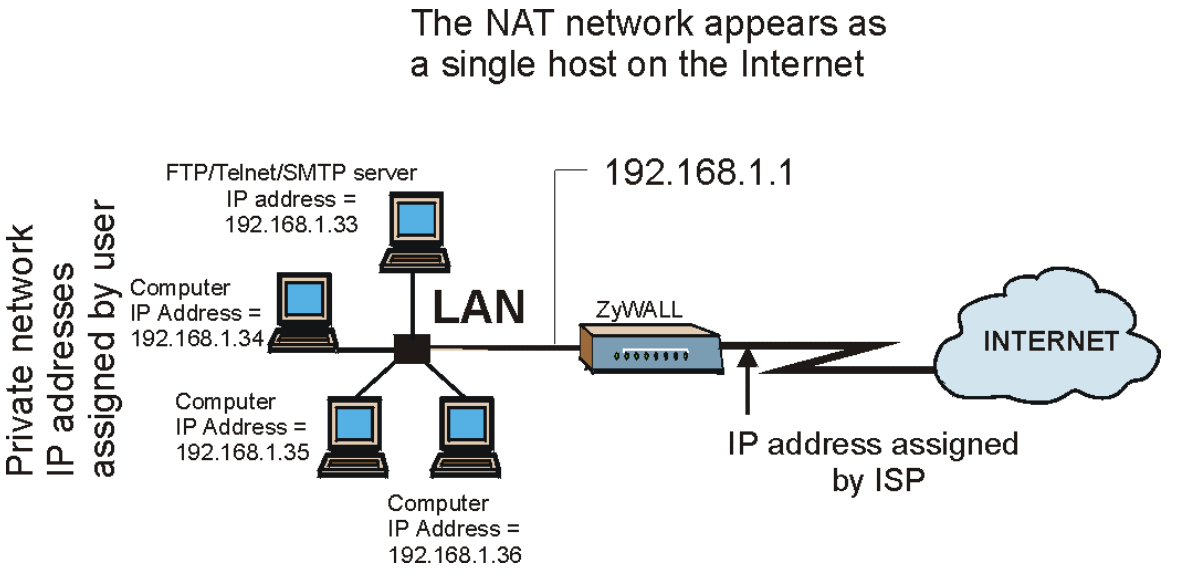


Figure 29-9 Multiple Servers Behind NAT Example

29.4 General NAT Examples

The following are some examples of NAT configuration.

29.4.1 Internet Access Only

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

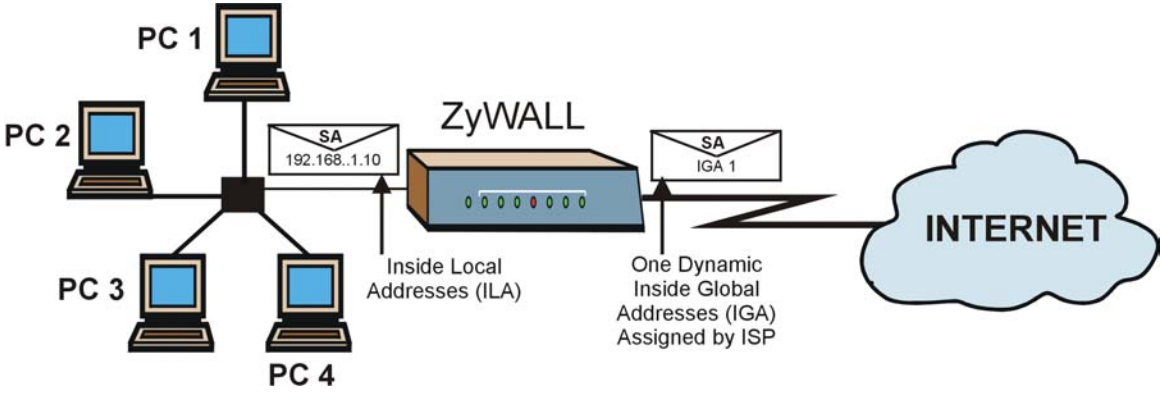


Figure 29-10 NAT Example 1

```
                Menu 4 - Internet Access Setup

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

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



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

Figure 29-11 Menu 4: Internet Access & NAT Example

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 29.4.* The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

29.4.2 Example 2: Internet Access with an Inside Server

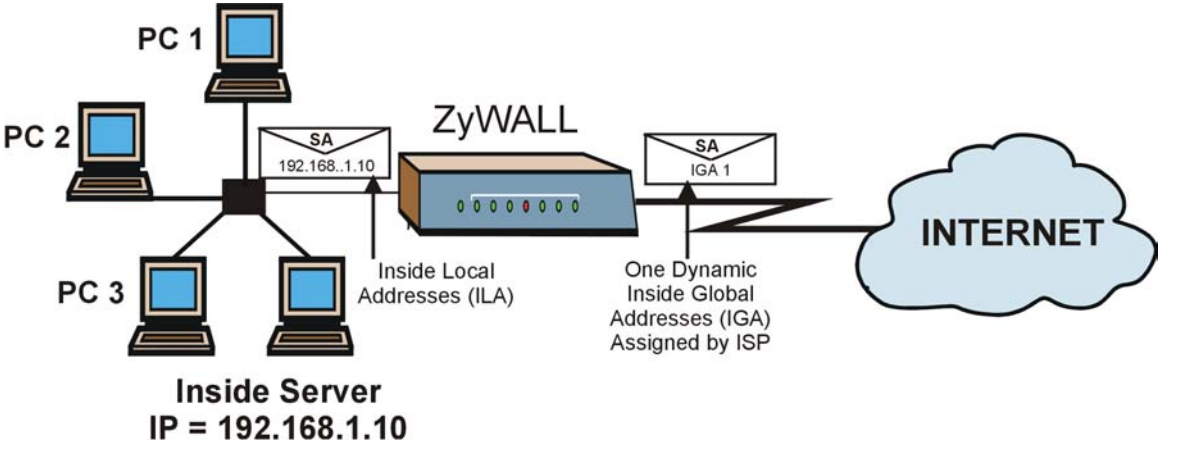


Figure 29-12 NAT Example 2

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

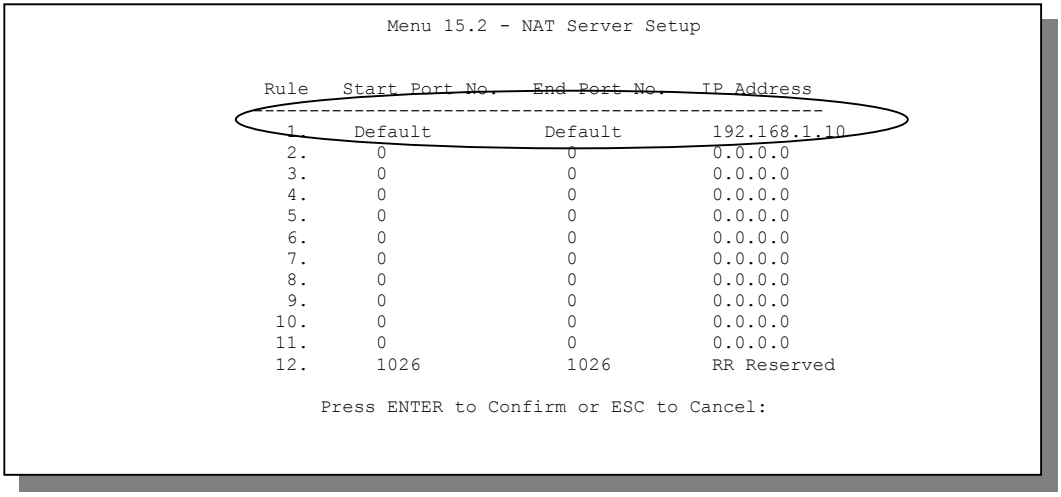


Figure 29-13 Menu 15.2: Specifying an Inside Server

29.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

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

Rule 1. Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 2. Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

Rule 4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

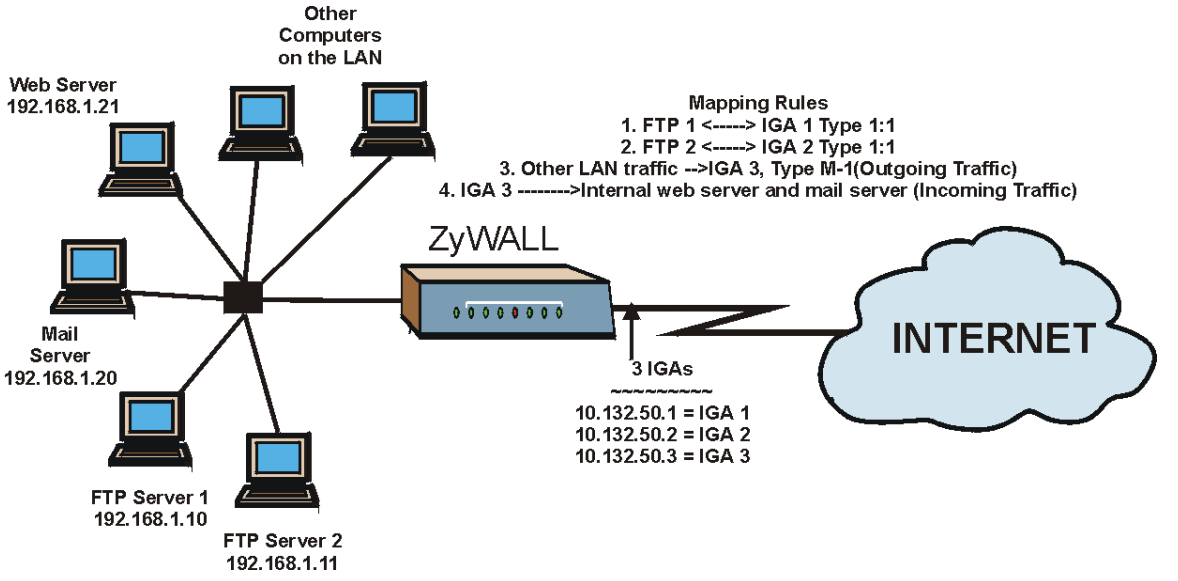


Figure 29-14 NAT Example 3

Step 1. In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in *Figure 29-15*.

Step 2. Then enter 15 from the main menu.

Step 3. Enter 1 to configure the Address Mapping Sets.

Step 4. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.

Step 5. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See *Figure 29-16).*

Step 6. Repeat the previous step for rules 2 to 4 as outlined above.

Step 7. When finished, menu 15.1.1 should look like as shown in *Figure 29-17.*

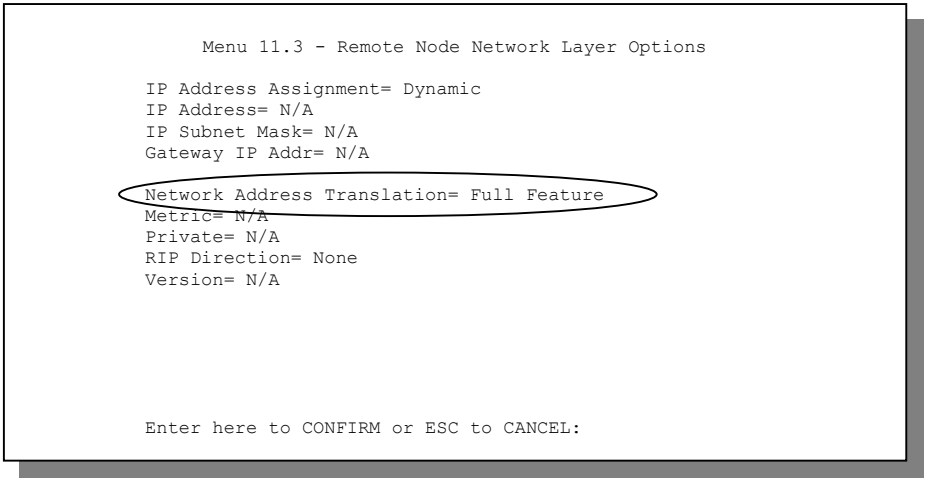


Figure 29-15 Example 3: Menu 11.3

The following figure shows how to configure the first rule.

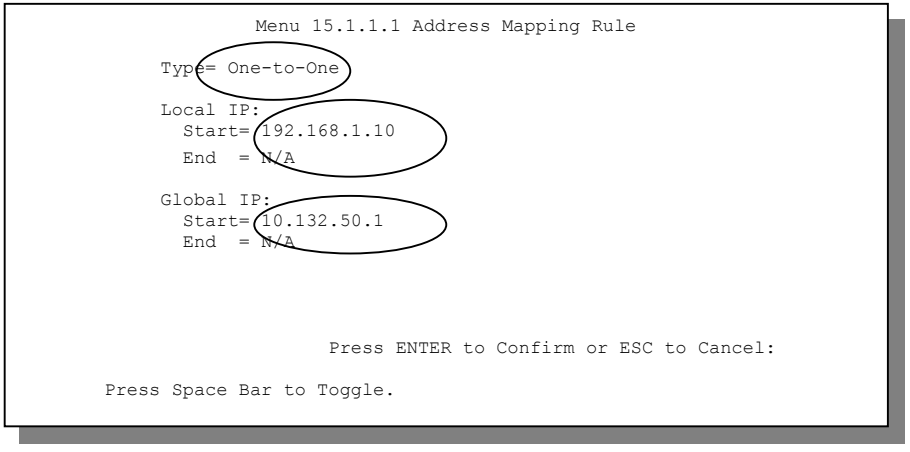


Figure 29-16 Example 3: Menu 15.1.1.1

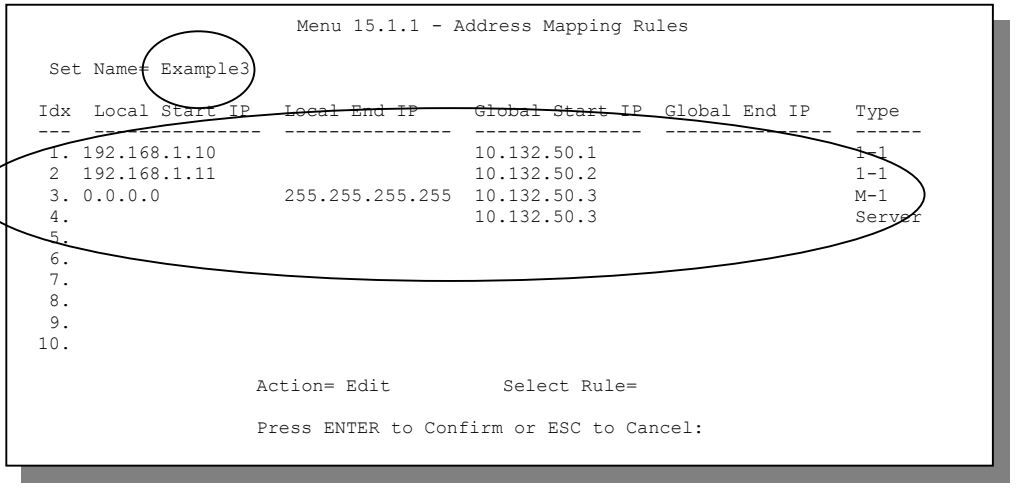


Figure 29-17 Example 3: Final Menu 15.1.1

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

Step 8. Enter 15 from the main menu.

Step 9. Now enter 2 from this menu and configure it as shown in *Figure 29-18*.

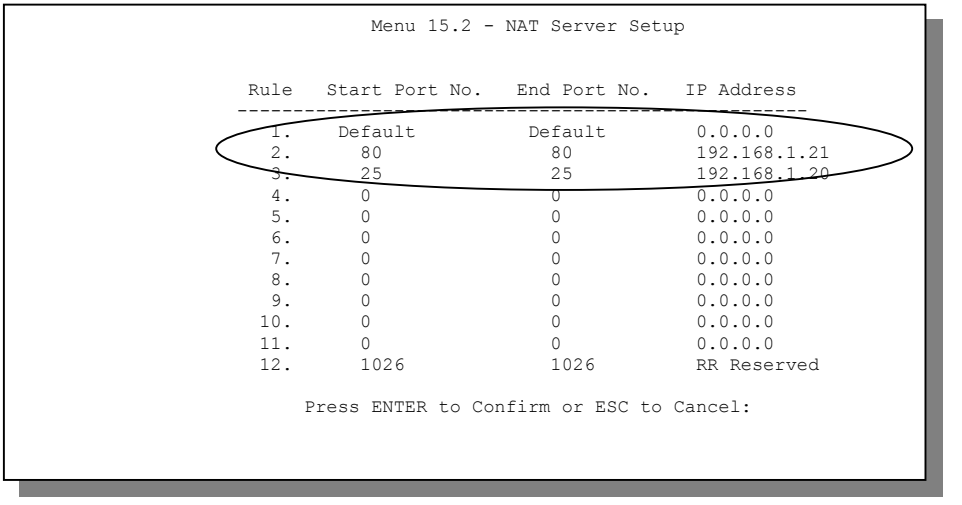


Figure 29-18 Example 3: Menu 15.2

29.4.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-One-to-One** mapping as port numbers do *not* change for **Many-One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

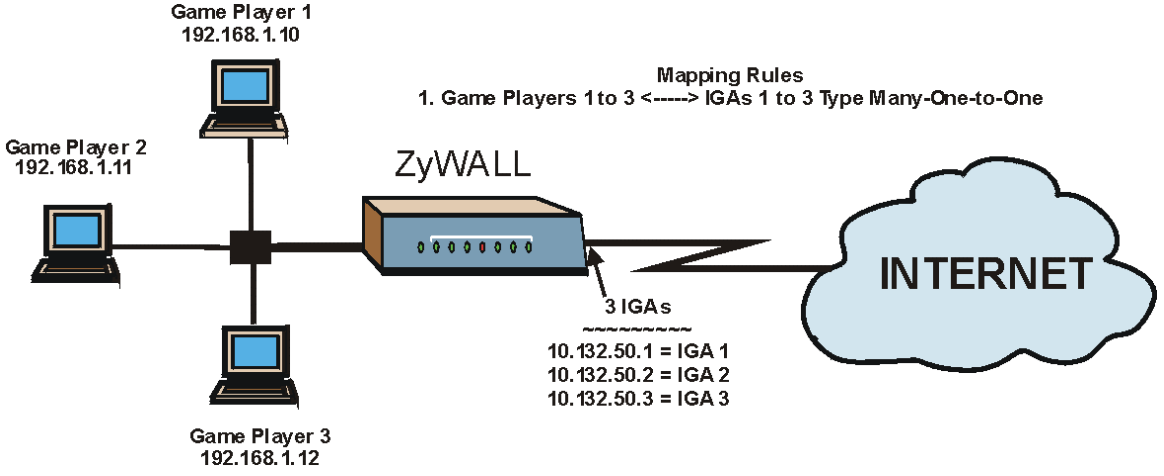


Figure 29-19 NAT Example 4

Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One **and** Many-One-to-One **mapping types.**

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

```
                        Menu 15.1.1.1 Address Mapping Rule

        Type= Many-One-to-One

        Local IP:
          Start= 192.168.1.10
          End  = 192.168.1.12

        Global IP:
          Start= 10.132.50.1
          End  = 10.132.50.3



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

Figure 29-20 Example 4: Menu 15.1.1.1: Address Mapping Rule

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

```
                        Menu 15.1.1 - Address Mapping Rules

 Set Name= Example4

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M-1-1
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                   Action= Edit          Select Rule=

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

Figure 29-21 Example 4: Menu 15.1.1: Address Mapping Rules

29.5 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from

the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

29.5.1 Trigger Port Forwarding Process

The following is an example of trigger port forwarding.

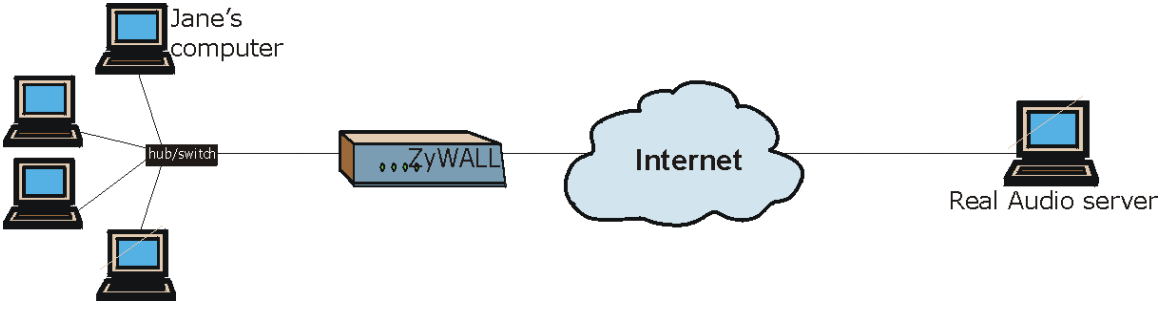


Figure 29-22 Trigger Port Forwarding Process: Example

1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the ZyWALL to record Jane's computer IP address. The ZyWALL associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The ZyWALL forwards the traffic to Jane's computer IP address.

5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyWALL times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

29.5.2 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is going coming from inside the ZyWALL and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 — Trigger Port Setup**, shown next.

```
                    Menu 15.3 - Trigger Port Setup

                              Incoming                  Trigger
 Rule       Name       Start Port   End Port     Start Port    End Port
-------------------------------------------------------------------------
    1.   Real Audio          6970        7170           7070        7070
    2.                          0           0              0           0
    3.                          0           0              0           0
    4.                          0           0              0           0
    5.                          0           0              0           0
    6.                          0           0              0           0
    7.                          0           0              0           0
    8.                          0           0              0           0
    9.                          0           0              0           0
   10.                          0           0              0           0
   11.                          0           0              0           0
   12.                          0           0              0           0

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

Figure 29-23 Menu 15.3—Trigger Port Setup

The following table describes the fields in this screen.

Table 29-5 Menu 15.3—Trigger Port Setup Description

FIELD	DESCRIPTION	EXAMPLE
Rule	This is the rule index number.	1
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.	Real Audio
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	6970
End Port	Enter a port number or the ending port number in a range of port numbers.	7170
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	7070
End Port	Enter a port number or the ending port number in a range of port numbers.	7070
Press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

Chapter 30
Introducing the ZyWALL Firewall

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

30.1 Using ZyWALL SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next**.**

```
                Menu 21 - Filter and Firewall Setup

 1. Filter Setup
 2. Firewall Setup
```

Figure 30-1 Menu 21: Filter and Firewall Setup

30.1.1 Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Use the web configurator to configure firewall rules. This screen varies by ZyWALL model.

```
                    Menu 21.2 - Firewall Setup

      The firewall protects against Denial of Service (DoS) attacks
when
      it is active.

      Your network is vulnerable to attacks when the firewall is
turned off.

     Refer to the User's Guide for details about the firewall default
     policies.

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

        Active: Yes
```

Figure 30-2 Menu 21.2: Firewall Setup

Configure the firewall rules using the web configurator or CLI commands.

Chapter 31
Filter Configuration

This chapter shows you how to create and apply filters.

31.1 Introduction to Filters

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

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

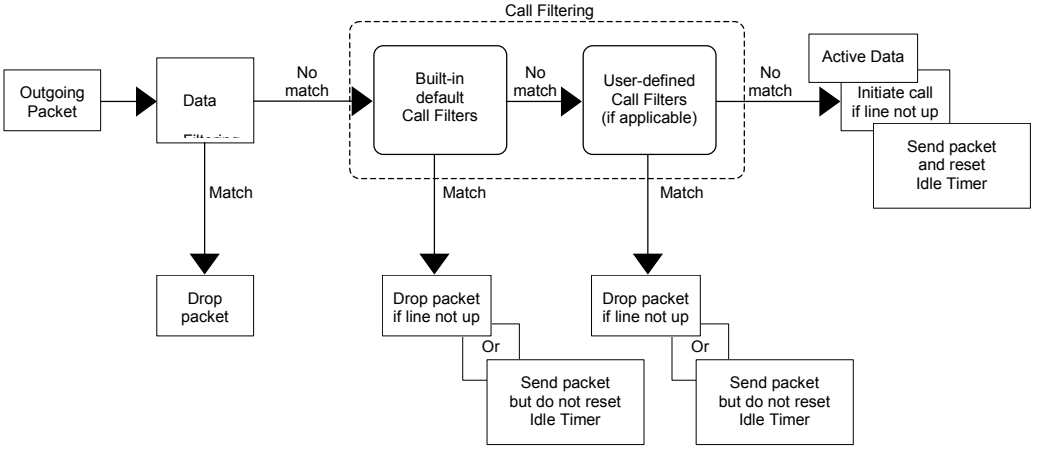


Figure 31-1 Outgoing Packet Filtering Process

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

31.1.1 The Filter Structure of the ZyWALL

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

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

The following figure illustrates the logic flow when executing a filter rule. See also *Figure 31-7* for the logic flow when executing an IP filter.

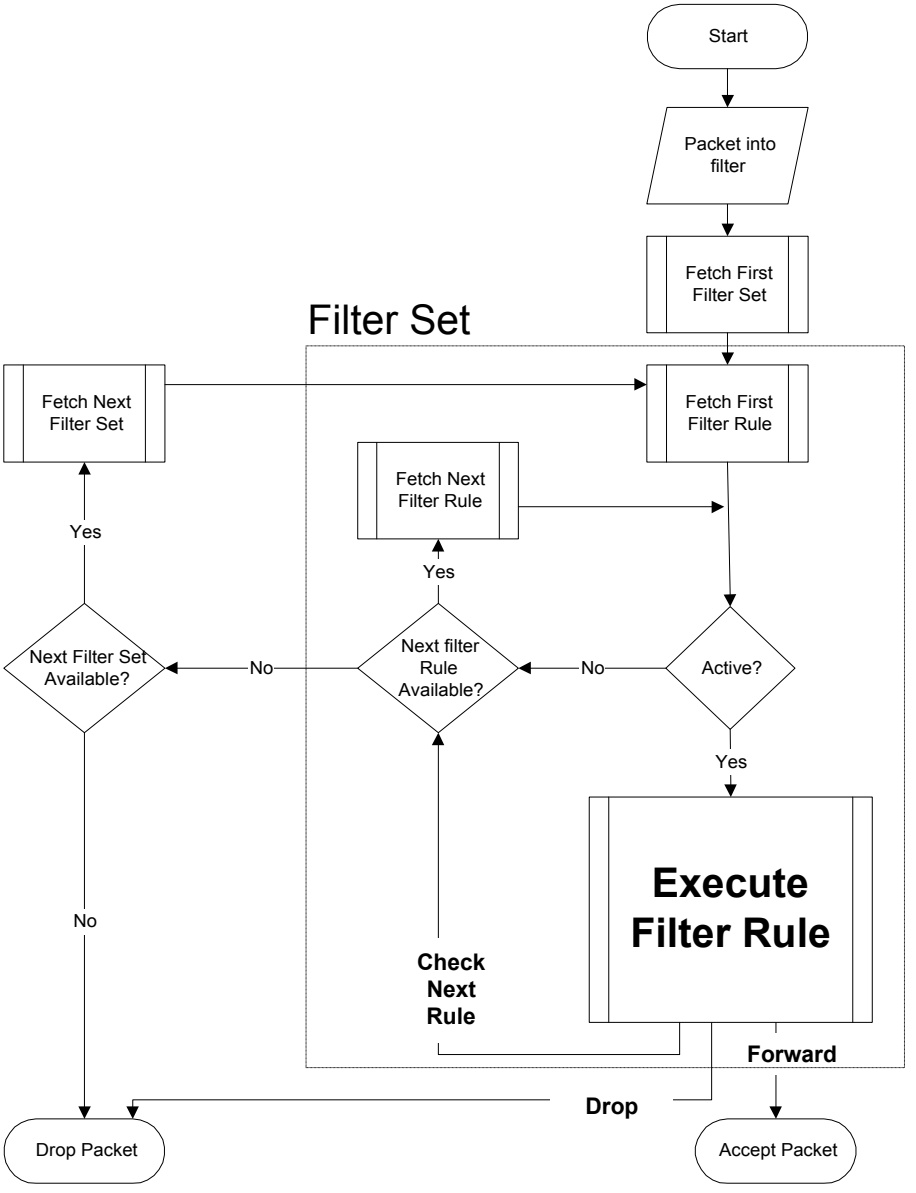


Figure 31-2 Filter Rule Process

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

31.2 Configuring a Filter Set

The ZyWALL includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

Step 1. Enter 21 in the main menu to open menu 21.

```
                Menu 21 - Filter and Firewall Setup

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




                                Enter Menu Selection Number:
```

Figure 31-4 Menu 21: Filter and Firewall Setup

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

```
                Menu 21.1 - Filter Set Configuration

Filter                                  Filter
Set #        Comments                   Set #        Comments
------  ------------------              ------  ------------------
  1     ________________                  7     ________________
  2     ________________                  8     ________________
  3     ________________                  9     ________________
  4     ________________                 10     ________________
  5     ________________                 11     ________________
  6     ________________                 12     ________________

              Enter Filter Set Number to Configure= 0

              Edit Comments= N/A

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

Figure 31-5 Menu 21.1: Filter Set Configuration

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

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

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

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

Table 31-1 Abbreviations Used in the Filter Rules Summary Menu

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

The protocol dependent filter rules abbreviation are listed as follows:

Table 31-2 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number
GEN	
Off	Offset
Len	Length

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

31.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

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

31.2.2 Configuring a TCP/IP Filter Rule

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

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next.

```
                    Menu 21.1.1.1 - TCP/IP Filter Rule

                Filter #: 1,1
                Filter Type= TCP/IP Filter Rule
                Active= Yes
                IP Protocol= 0      IP Source Route= No
                Destination: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 137
                             Port # Comp= Equal
                     Source: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #=
                             Port # Comp= None
                TCP Estab= No
                More= N/A             Log= None
                Action Matched= Drop
                Action Not Matched= Check Next Rule

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

Figure 31-6 Menu 21.1.1.1: TCP/IP Filter Rule

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

Table 31-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the filter rule or **No** to deactivate it.	**Yes** **No**
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.	0-255
IP Source Route	Press [SPACE BAR] and then [ENTER] to select **Yes** to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.	**Yes** **No**
Destination		
IP Address	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the **Destination: IP Addr**.	0.0.0.0

Table 31-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given **in Destination: Port #**.	**None** **Less** **Greater** **Equal** **Not Equal**
Source		
IP Address	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the **Source: IP Addr**.	0.0.0.0
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in **Source: Port #**.	**None** **Less** **Greater** **Equal** **Not Equal**
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select **Yes**, to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored.	**Yes** **No**
More	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	**Yes** **No**

Table 31-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**
When you have **Menu 21.1.1.1 - TCP/IP Filter Rule** configured, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.		

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

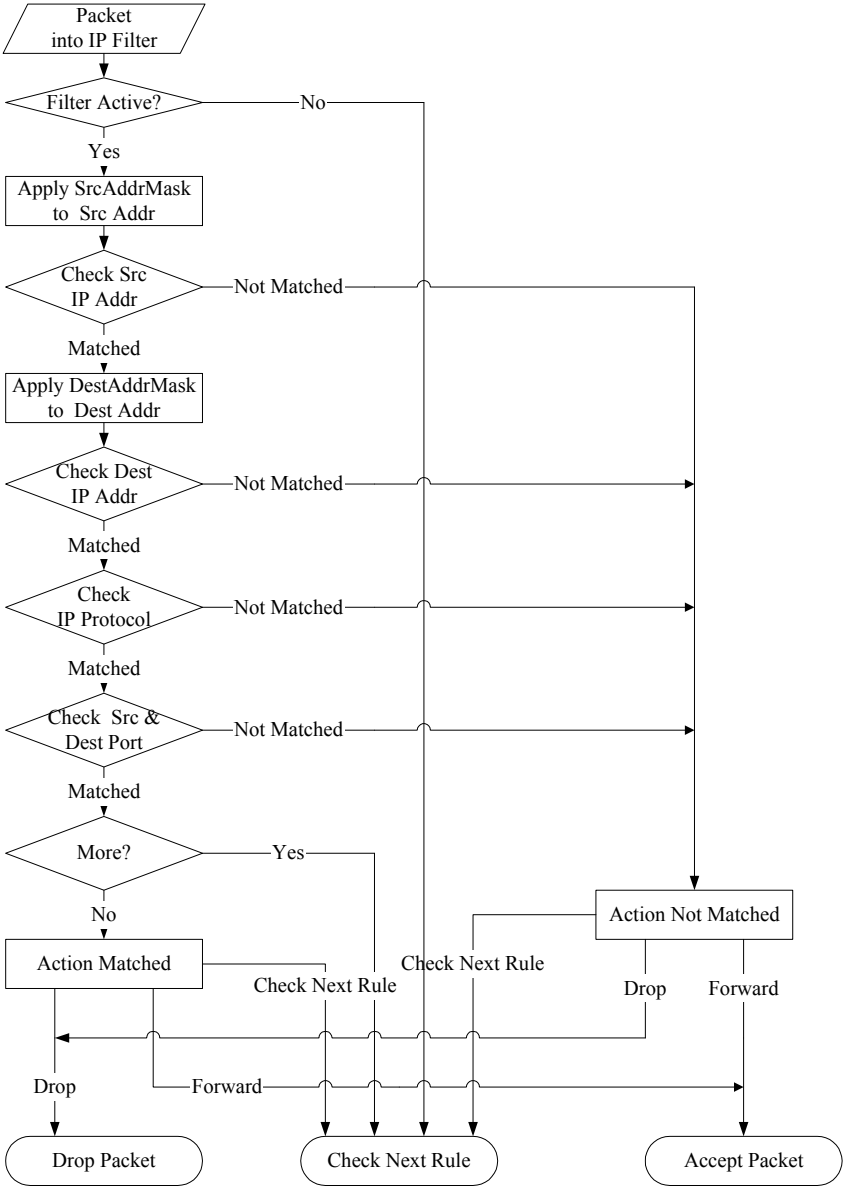


Figure 31-7 Executing an IP Filter

31.2.3 Configuring a Generic Filter Rule

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

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

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.4.1 and press [ENTER] to open Generic Filter Rule, as shown below.

```
                  Menu 21.1.4.1 - Generic Filter Rule

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



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

Figure 31-8 Menu 21.1.4.1: Generic Filter Rule

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

Table 31-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	

Table 31-4 Generic Filter Rule Menu Fields

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

31.3 Example Filter

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

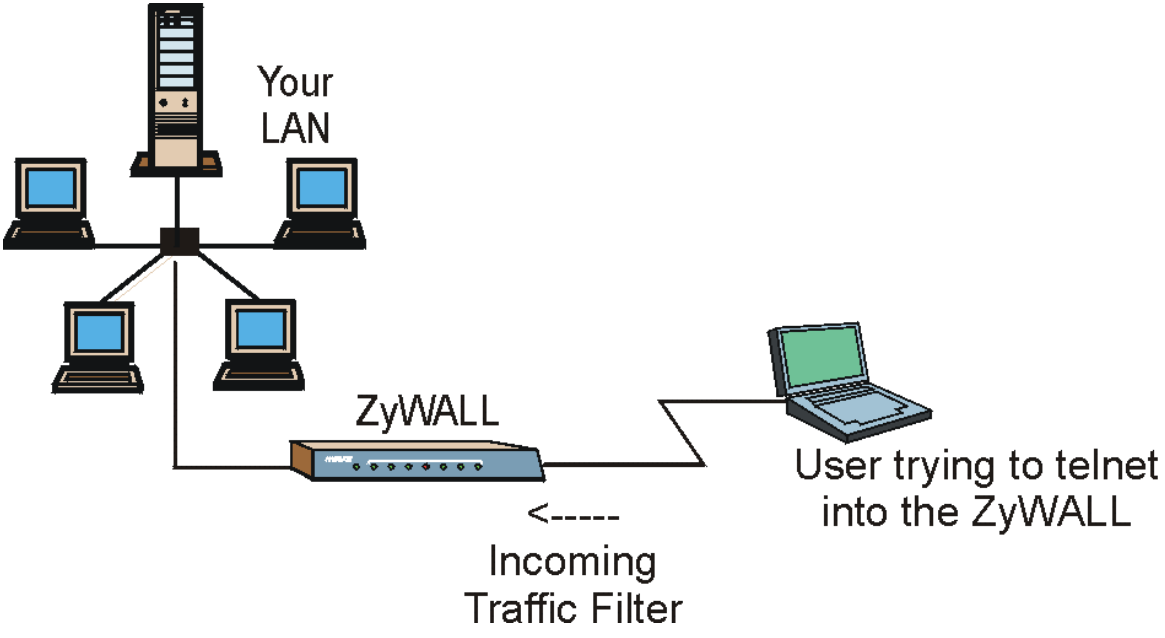


Figure 31-9 Telnet Filter Example

Step 1. Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.

Step 2. Enter 1 to open **Menu 21.1 - Filter Set Configuration**.

Step 3. Enter the index of the filter set you wish to configure (say 3) and press [ENTER].

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

Step 5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.

Step 6. Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

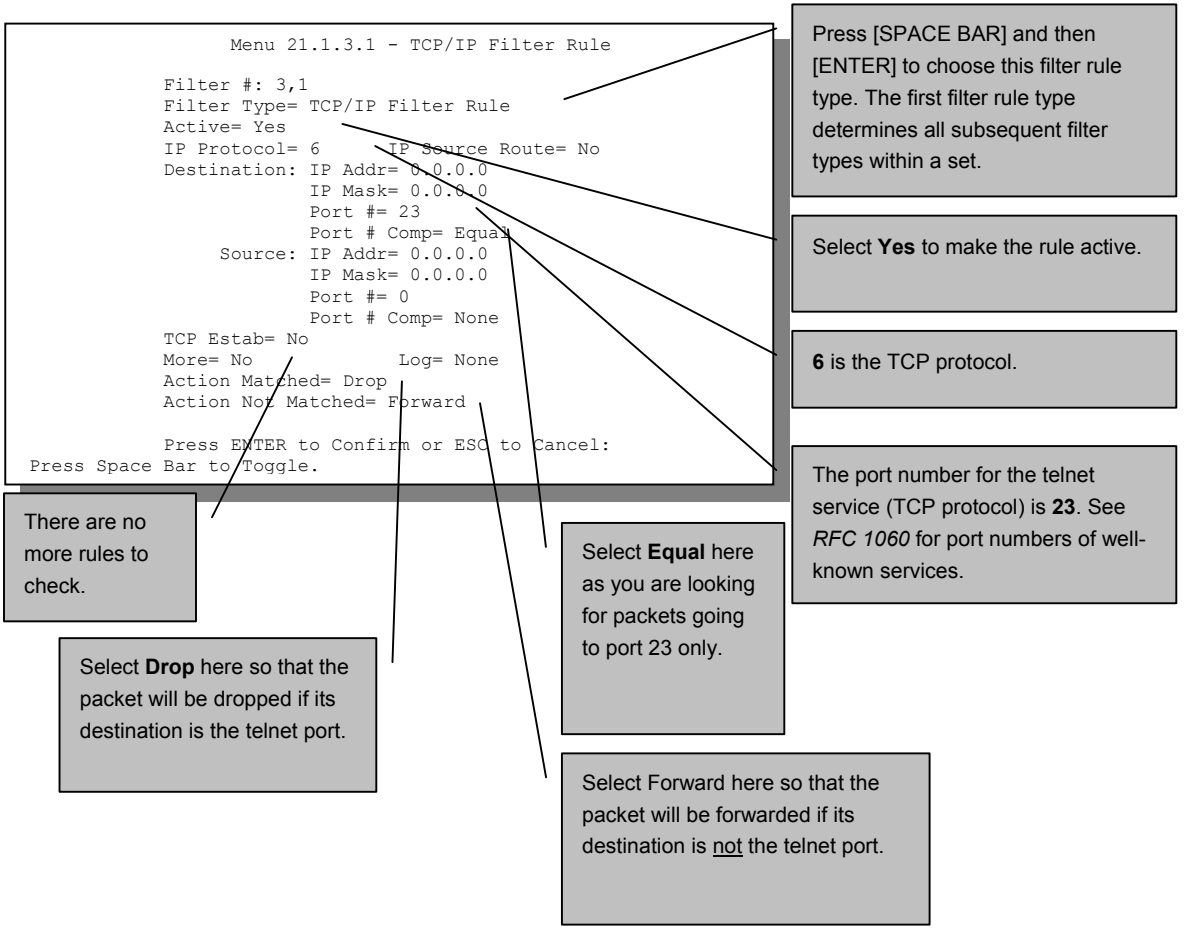


Figure 31-10 Example Filter: Menu 21.1.3.1

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

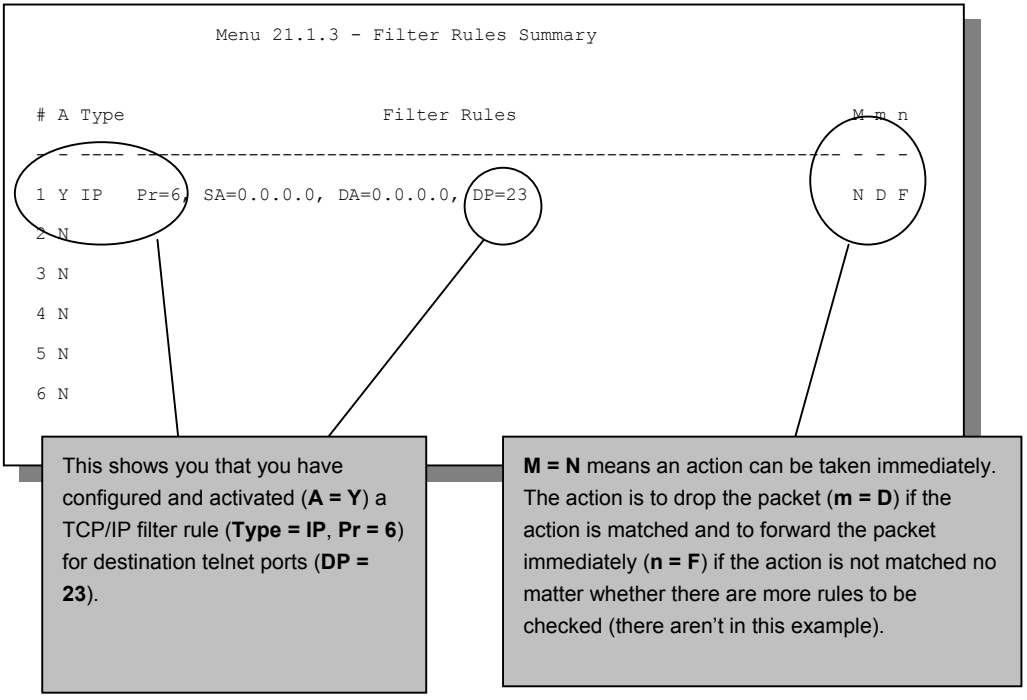


Figure 31-11 Example Filter Rules Summary: Menu 21.1.3

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

Step 1. Enter 11 from the main menu to go to menu 11.

Step 2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].

Step 3. This brings you to menu 11.5. Apply a filter set (our example filter set 3) as shown in *Figure 31-15*.

Step 4. Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

31.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network

Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyWALL applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyWALL is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

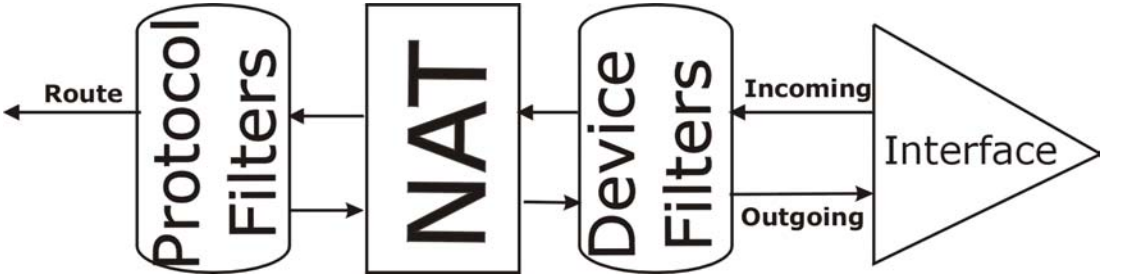


Figure 31-12 Protocol and Device Filter Sets

31.5 Firewall Versus Filters

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

31.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

If you do not activate the firewall, it is advisable to apply filters.

31.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

```
                    Menu 3.1 - LAN Port Filter Setup

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



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

Figure 31-13 Filtering LAN Traffic

31.6.2 Applying DMZ Filters

DMZ traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 5.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections. The DMZ port is not available on all models.

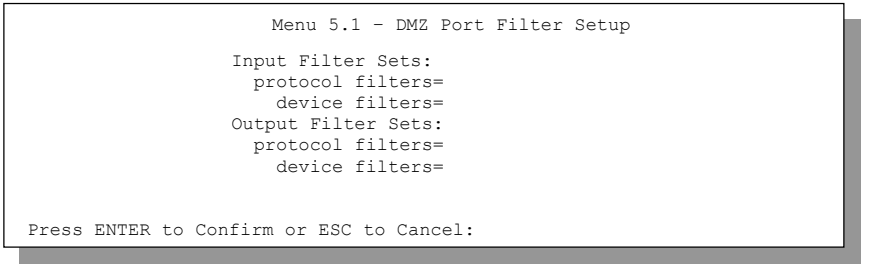


Figure 31-14Filtering DMZ Traffic

31.6.3 Applying Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

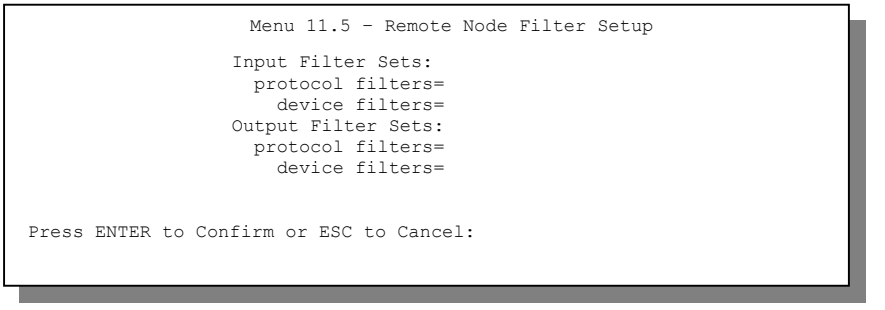


Figure 31-15 Filtering Remote Node Traffic

Chapter 32
SNMP Configuration

This chapter explains SNMP configuration menu 22.

SNMP is only available if TCP/IP is configured.

32.1 SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **Menu 22 - SNMP Configuration** as shown next. The "community" for **Get**, **Set** and **Trap** fields is SNMP terminology for password.

```
                    Menu 22 - SNMP Configuration

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

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

Figure 32-1 Menu 22: SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 32-1 SNMP Configuration Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Get Community	Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station.	**Public**
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.	**Public**
Trusted Host	If you enter a trusted host, your ZyWALL will only respond to SNMP messages from this address. A blank (default) field means your ZyWALL will respond to all SNMP messages it receives, regardless of source.	0.0.0.0

Table 32-1 SNMP Configuration Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Trap Community	Type the Trap community, which is the password sent with each trap to the SNMP manager.	**Public**
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

32.2 SNMP Traps

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

Table 32-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

Part XIII:

SMT System Maintenance

This part covers system information and diagnosis, firmware and configuration file maintenance, as well as providing information on the system maintenance and information functions and how to configure remote management.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 33
System Information & Diagnosis

This chapter covers SMT menus 24.1 to 24.4. DMZ applies to the ZyWALL 100. Wireless LAN and dial-backup apply to the ZyWALL 100, 10W and 30W (see Table 1-1 Model Specific Features in the Web Configuration User's Guide).

33.1 Introduction to System Status

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

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

```
                Menu 24 - System Maintenance

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



                     Enter Menu Selection Number:
```

Figure 33-1 Menu 24: System Maintenance

33.2 System Status

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

monitor your ZyWALL. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

To get to the System Status:

Step 1. Enter number 24 to go to **Menu 24 - System Maintenance**.

Step 2. In this menu, enter 1 to open System Maintenance - Status.

Step 3. There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.

```
                    Menu 24.1 - System Maintenance - Status          03:06:17
                                                                Sat. Jan. 01, 2000

 Port   Status        TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
  WAN   Down             0           0       0         0         0     0:00:00
  LAN   Down           463         792       0         0         0     0:00:00
  DMZ   Down             0           0       0         0         0     0:00:00
 WLAN   Down             0           0       0         0         0     0:00:00

 Port   Ethernet Address        IP Address          IP Mask       DHCP
  WAN  00:a0:c5:01:23:46          0.0.0.0          0.0.0.0     Client
  LAN  00:a0:c5:01:23:45        192.168.1.1    255.255.255.0     Server
  DMZ  00:a0:c5:01:23:47          0.0.0.0          0.0.0.0       None
 WLAN  00:00:00:00:00:00

      System up Time:     3:06:20


                                Press Command:

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

Figure 33-2 Menu 24.1: System Maintenance: Status (ZyWALL 100)

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

Table 33-1 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Port	Identifies a port (WAN, LAN, DMZ or WLAN) on the ZyWALL. DMZ not available on all models.

Table 33-1 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Status	Shows the port speed and duplex setting if you're using **Ethernet Encapsulation** and **Down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using **PPPoE Encapsulation**.
TxPkts	The number of transmitted packets on this port.
RxPkts	The number of received packets on this port.
Cols	The number of collisions on this port.
Tx B/s	Shows the transmission speed in Bytes per second on this port.
Rx B/s	Shows the reception speed in Bytes per second on this port.
Up Time	Total amount of time the line has been up.
Ethernet Address	The Ethernet address of the port listed on the left.
IP Address	The IP address of the port listed on the left.
IP Mask	The IP mask of the port listed on the left.
DHCP	The DHCP setting of the port listed on the left.
System up Time	The total time the ZyWALL has been on.
ZyNOS F/W Version	The ZyNOS Firmware version and the date created.
Some ZyWALL models include some or all of the following fields.	
Name	This is the ZyWALL's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	The ZyNOS Firmware version and the date created.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

33.3 System Information and Console Port Speed

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

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

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

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

```
Menu 24.2 - System Information and Console Port Speed

      1. System Information
      2. Console Port Speed



            Please enter selection:
```

Figure 33-3 Menu 24.2: System Information and Console Port Speed

33.3.1 System Information

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

```
Menu 24.2.1 - System Maintenance - Information

                Name:
                Routing: IP
                ZyNOS F/W Version: V3.60(WH.0)B7 | 11/7/2002
                Country Code: 255

                LAN
                  Ethernet Address: 00:A0:C5:00:00:01
                  IP Address: 192.168.1.1
                  IP Mask: 255.255.255.0
                  DHCP: Server




                    Press ESC or RETURN to Exit:
```

Figure 33-4 Menu 24.2.1: System Maintenance: Information (ZyWALL 10W)

Table 33-2 Fields in System Maintenance: Information

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

33.3.2 Console Port Speed

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

```
Menu 24.2.2 – System Maintenance – Change Console Port Speed

                Console Port Speed: 115200




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

Figure 33-5 Menu 24.2.2: System Maintenance: Change Console Port Speed

33.4 Log and Trace

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

33.4.1 Viewing Error Log

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

Step 1. Select option 24 from the main menu to open **Menu 24 - System Maintenance**.

Step 2. From menu 24, select option 3 to open **Menu 24.3 - System Maintenance - Log and Trace**.

Step 3. Select the first option from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

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

```
Menu 24.3 - System Maintenance - Log and Trace


    1. View Error Log
    2. UNIX Syslog

    4. Call-Triggering Packet


             Please enter selection
```

Figure 33-6 Menu 24.3: System Maintenance: Log and Trace

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

```
      0 Wed Aug 22 21:23:26 2001 PP17  INFO  getDateTime fail: no server available
      1 Wed Aug 22 21:23:26 2001 PP17  INFO  adjtime task pause 60 seconds
      2 Wed Aug 22 21:23:54 2001 PINI  INFO  SMT Session Begin
      3 Wed Aug 22 21:24:26 2001 PP0d  INFO  No DNS server available
      4 Wed Aug 22 21:24:26 2001 PP17  WARN  Wrong domain name
      5 Wed Aug 22 21:24:26 2001 PP0d  INFO  No DNS server available
      6 Wed Aug 22 21:24:26 2001 PP17  INFO  Last errorlog repeat 8 Times
      7 Wed Aug 22 21:24:26 2001 PP17  INFO  getDateTime fail: no server available
      8 Wed Aug 22 21:24:26 2001 PP17  INFO  adjtime task pause 1 day
     10 Thu Aug 23 08:26:59 2001 PINI -WARN  SNMP TRAP 0: cold start
     11 Thu Aug 23 08:26:59 2001 PINI  INFO  main: init completed
     12 Thu Aug 23 08:27:04 2001 PP17  INFO  adjtime task pause 1 day
     13 Thu Aug 23 08:27:28 2001 PINI  INFO  SMT Session Begin
     14 Thu Aug 23 08:27:40 2001 PINI  WARN  system name is not configured
     15 Thu Aug 23 08:27:41 2001 PP0d  INFO  LAN promiscuous mode <0>
     16 Thu Aug 23 08:32:40 2001 PINI  INFO  SMT Session End
     17 Thu Aug 23 08:33:07 2001 PINI  INFO  SMT Session Begin
     18 Thu Aug 23 09:01:12 2001 PINI  INFO  SMT Session End
     19 Thu Aug 23 09:02:09 2001 PINI  INFO  SMT Session Begin
   Clear Error Log (y/n):
```

Figure 33-7 Examples of Error and Information Messages

33.4.2 UNIX Syslog

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

```
            Menu 24.3.2 - System Maintenance - UNIX Syslog

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









          Press ENTER to Confirm or ESC to Cancel
```

Figure 33-8 Menu 24.3.2: System Maintenance: UNIX Syslog (ZyWALL 100)

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

Table 33-3 System Maintenance Menu Syslog Parameters

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to your UNIX manual for more details.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

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

1. CDR

CDR Message Format

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

        L02 Call Terminated
        C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
```

2. Packet triggered

Packet triggered Message Format

```
SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
        String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
        Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
        Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f707172
7374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

3. Filter log

Filter log Message Format

```
        SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD

IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop
(D).
        Src: Source Address
        Dst: Destination Address
        prot: Protocol (“TCP”,”UDP”,”ICMP”)
spo: Source port
dpo: Destination port
Mar 03 10:39:43 202.132.155.97 ZyXEL:
GEN[ffffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[fffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170  dpo=00021]}S04>R01mF
```

4. PPP log

PPP Log Message Format

```
SdcmdSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing
```

5. Firewall log

```
Firewall Log Message Format
SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule | action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol (“TCP”,”UDP”,”ICMP”, ”IGMP”, ”GRE”, ”ESP”)
rule: <a,b> where a means "set" number; b means "rule" number.
Action: nothing(N) block (B) forward (F)
08-01-2000       11:48:41 Local1.Notice    192.168.10.10    RAS: FW 172.21.1.80     :137  -
>172.21.1.80     :137  |UDP|default permit:<2,0>|B
08-01-2000       11:48:41 Local1.Notice    192.168.10.10    RAS: FW 192.168.77.88   :520  -
>192.168.77.88   :520  |UDP|default permit:<2,0>|B
08-01-2000       11:48:39 Local1.Notice    192.168.10.10    RAS: FW 172.21.1.50     ->172.21.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-2000       11:48:39 Local1.Notice    192.168.10.10    RAS: FW 172.21.1.25     ->172.21.1.25
|IGMP<2>|default permit:<2,0>|B
```

33.4.3 Call-Triggering Packet

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

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

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

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

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

Figure 33-9 Call-Triggering Packet Example

33.5 Diagnostic

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

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

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

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

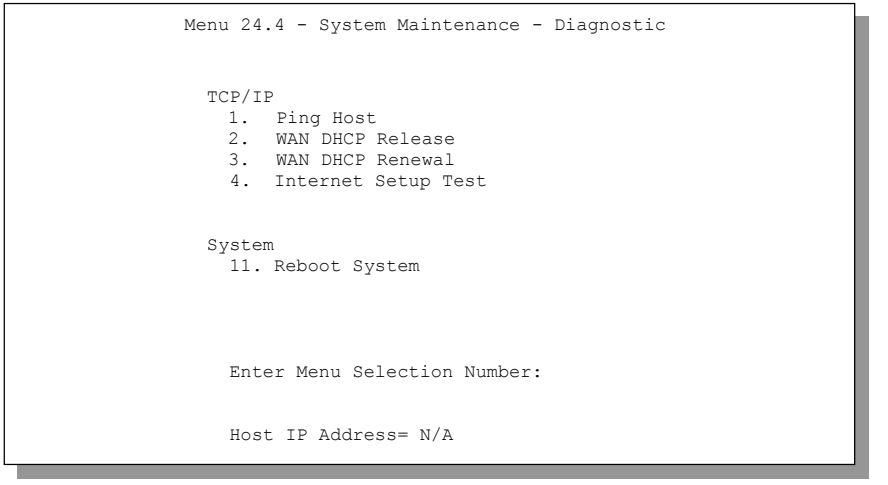


Figure 33-10 Menu 24.4: System Maintenance: Diagnostic

33.5.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in *Figure 33-11*. LAN DHCP has already been discussed. The ZyWALL can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.3 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

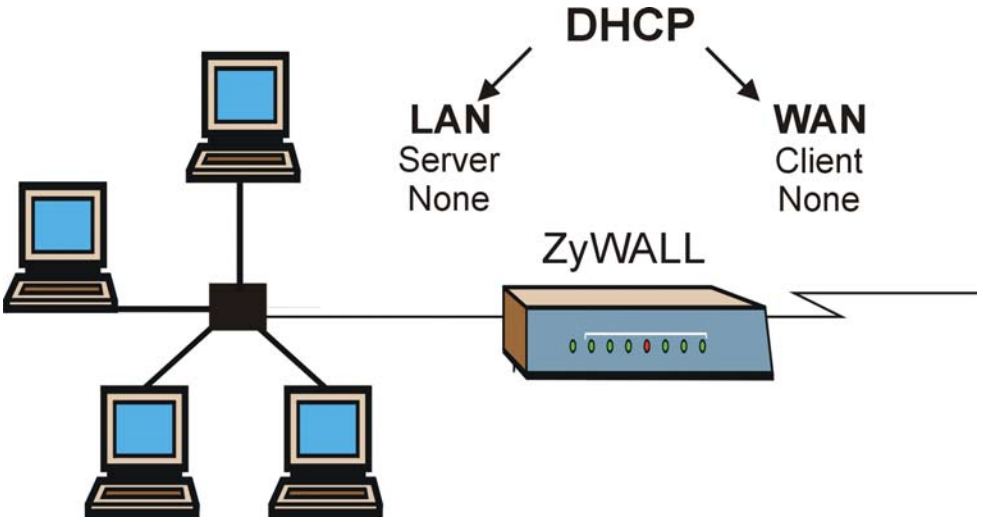


Figure 33-11 WAN & LAN DHCP

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

Table 33-4 System Maintenance Menu Diagnostic

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

Chapter 34
Firmware and Configuration File Maintenance

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

34.1 Introduction

Use the instructions in this chapter to change the ZyWALL's configuration file or upgrade its firmware. After you configure your ZyWALL, you can backup the configuration file to a computer. That way if you later misconfigure the ZyWALL, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the ZyWALL to the original default settings. The firmware determines the ZyWALL's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site to use to upgrade your ZyWALL's performance.

34.2 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the ZyWALL's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyWALL.

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

This is a sample FTP session saving the current configuration to the computer file “config.cfg”.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyWALL only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

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

Table 34-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyWALL. Uploading the rom-0 file replaces the entire ROM file system, including your ZyWALL configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyWALL.	*.bin

34.3 Backup Configuration

The ZyWALL displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current ZyWALL configuration to your computer. Backup is highly recommended once your ZyWALL is functioning properly. FTP is the

preferred method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the ZyWALL to the computer, while upload means from your computer to the ZyWALL.

34.3.1 Backup Configuration

Follow the instructions as shown in the next screen.

```
              Menu 24.5 - System Maintenance - Backup Configuration

To transfer the configuration file to your workstation, follow the procedure
below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current router configuration to
   your workstation.

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


                                Press ENTER to Exit:
```

Figure 34-1 Telnet into Menu 24.5

34.3.2 Using the FTP Command from the Command Line

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your ZyWALL.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Use "get" to transfer files from the ZyWALL to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the ZyWALL to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.

Step 7. Enter "quit" to exit the ftp prompt.

34.3.3 Example of FTP Commands from the Command Line

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

Figure 34-2 FTP Session Example

34.3.4 GUI-based FTP Clients

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

Table 34-2 General Commands for GUI-based FTP Clients

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

Table 34-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Initial Local Directory	Specify the default local directory (path).

34.3.5 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

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

34.3.6 Backup Configuration Using TFTP

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

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

Step 1. Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the configuration file is "rom-0" (rom-zero, not capital o).

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

34.3.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

Where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyWALL IP address, "get" transfers the file source on the ZyWALL (rom-0, name of the configuration file on the ZyWALL) to the file destination on the computer and renames it config.rom.

34.3.8 GUI-based TFTP Clients

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

Table 34-3 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyWALL. 192.168.1.1 is the ZyWALL's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the ZyWALL and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyWALL. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to *section 34.3.5* to read about configurations that disallow TFTP and FTP over WAN.

34.3.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.5 and enter "y" at the following screen.

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

Figure 34-3 System Maintenance: Backup Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
You can enter ctrl-x to terminate operation any
time.
Starting XMODEM download...
```

Figure 34-4 System Maintenance: Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

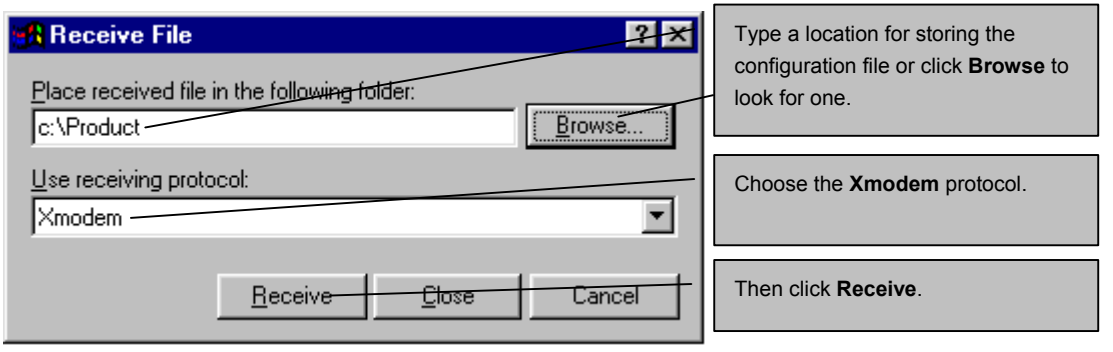


Figure 34-5 Backup Configuration Example

Step 4. After a successful backup you will see the following screen. Press any key to return to the SMT menu.

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

Figure 34-6 Successful Backup Confirmation Screen

34.4 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your ZyWALL since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

WARNING!

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL. When the Restore Configuration process is complete, the ZyWALL will automatically restart.

34.4.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

```
            Menu 24.6 -- System Maintenance - Restore Configuration

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

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

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


Press ENTER to Exit:
```

Figure 34-7 Telnet into Menu 24.6

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyWALL.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Find the “rom” file (on your computer) that you want to restore to your ZyWALL.

Step 7. Use “put” to transfer files from the ZyWALL to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the ZyWALL. See earlier in this chapter for more information on filename conventions.

Step 8. Enter “quit” to exit the ftp prompt. The ZyWALL will automatically restart after a successful restore process.

34.4.2 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Figure 34-8 Restore Using FTP Session Example

Refer to *section 34.3.5* to read about configurations that disallow TFTP and FTP over WAN.

34.4.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.6 and enter "y" at the following screen.

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

Figure 34-9 System Maintenance: Restore Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
Starting XMODEM download (CRC mode) ...
CCCCCCCCC
```

Figure 34-10 System Maintenance: Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

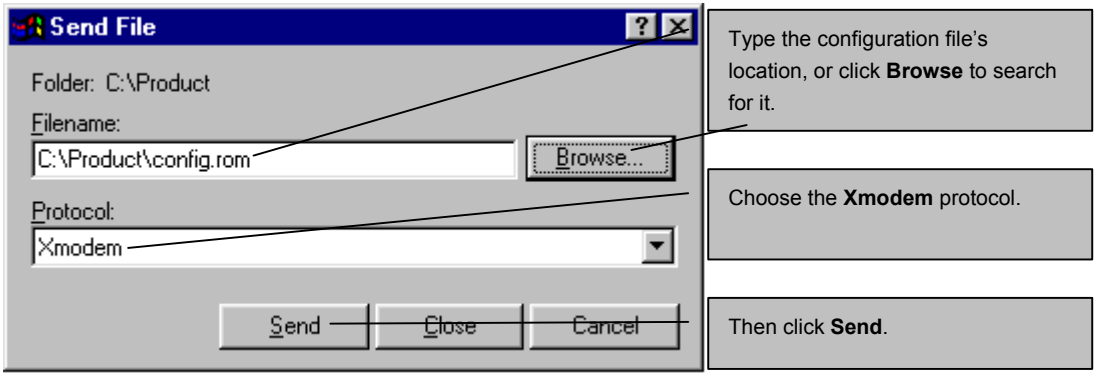


Figure 34-11 Restore Configuration Example

Step 4. After a successful restoration you will see the following screen. Press any key to restart the ZyWALL and return to the SMT menu.

```
Save to ROM
Hit any key to start system reboot.
```

Figure 34-12 Successful Restoration Confirmation Screen

34.5 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

WARNING!

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL.

34.5.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

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

```
            Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

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

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

Press ENTER to Exit:
```

Figure 34-13 Telnet Into Menu 24.7.1: Upload System Firmware

34.5.2 Configuration File Upload

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

```
        Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

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

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

Press ENTER to Exit:
```

Figure 34-14 Telnet Into Menu 24.7.2: System Maintenance

To upload the firmware and the configuration file, follow these examples

34.5.3 FTP File Upload Command from the DOS Prompt Example

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyWALL.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Use “put” to transfer files from the computer to the ZyWALL, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyWALL and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyWALL and renames it “rom-0”. Likewise “get rom-0 config.rom”

transfers the configuration file on the ZyWALL to your computer and renames it "config.rom." See earlier in this chapter for more information on filename conventions.

Step 7. Enter "quit" to exit the ftp prompt.

34.5.4 FTP Session Example of Firmware File Upload

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

Figure 34-15 FTP Session Example of Firmware File Upload

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

Refer to *section 34.3.5* to read about configurations that disallow TFTP and FTP over WAN.

34.5.5 TFTP File Upload

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

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

Step 1. Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the firmware is “ras”.

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

34.5.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyWALL’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyWALL).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

34.5.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyWALL. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyWALL via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

34.5.8 Uploading Firmware File Via Console Port

Step 1. Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 - System Maintenance - Upload System Firmware**, and then follow the instructions as shown in the following screen.

```
            Menu 24.7.1 - System Maintenance - Upload System Firmware


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

        Warning: Proceeding with the upload will erase the current system
        firmware.
                        Do You Wish To Proceed:(Y/N)
```

Figure 34-16 Menu 24.7.1 As Seen Using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

34.5.9 Example Xmodem Firmware Upload Using HyperTerminal

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

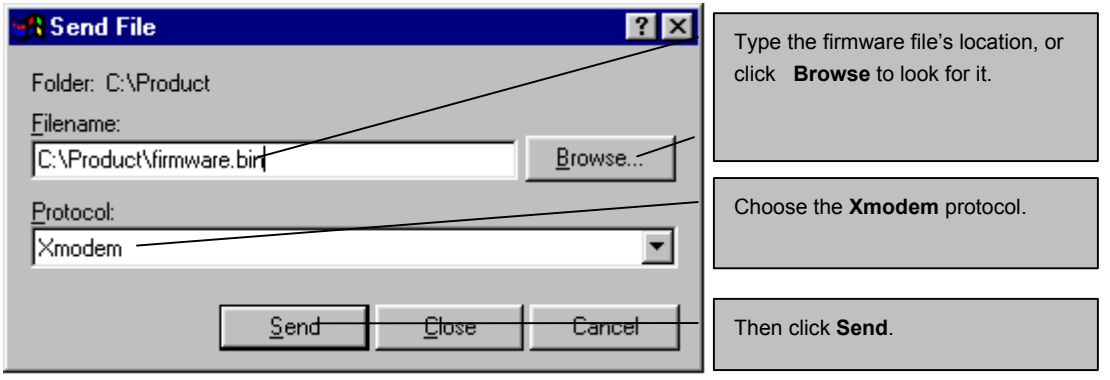


Figure 34-17 Example Xmodem Upload

After the firmware upload process has completed, the ZyWALL will automatically restart.

34.5.10 Uploading Configuration File Via Console Port

Step 1. Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 - System Maintenance - Upload System Configuration File**. Follow the instructions as shown in the next screen.

```
          Menu 24.7.2 - System Maintenance - Upload System Configuration File


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

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

Figure 34-18 Menu 24.7.2 As Seen Using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

Step 3. Enter “atgo” to restart the ZyWALL.

34.5.11 Example Xmodem Configuration Upload Using HyperTerminal

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

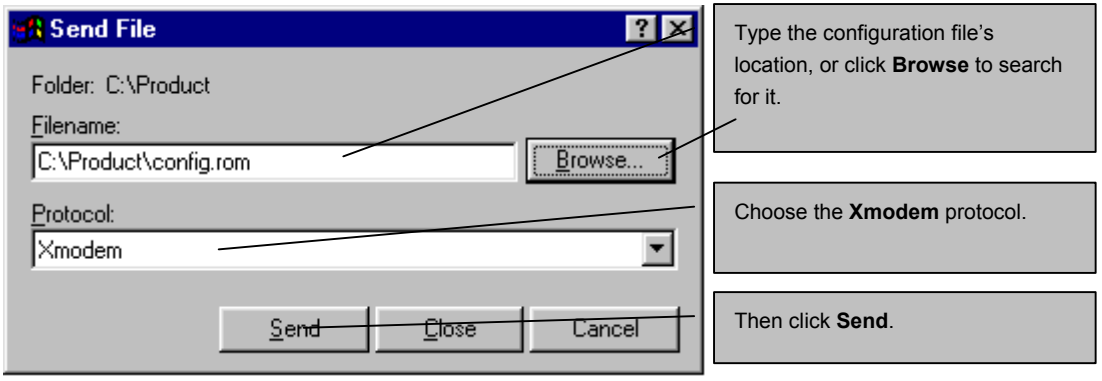


Figure 34-19 Example Xmodem Upload

After the configuration upload process has completed, restart the ZyWALL by entering "atgo".

Chapter 35
System Maintenance Menus 8 to 10

This chapter leads you through SMT menus 24.8 to 24.10. The Real Time Chip (RTC) applies to the ZyWALL 100, 50, 30W and 10W.

35.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or zyxel.com for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

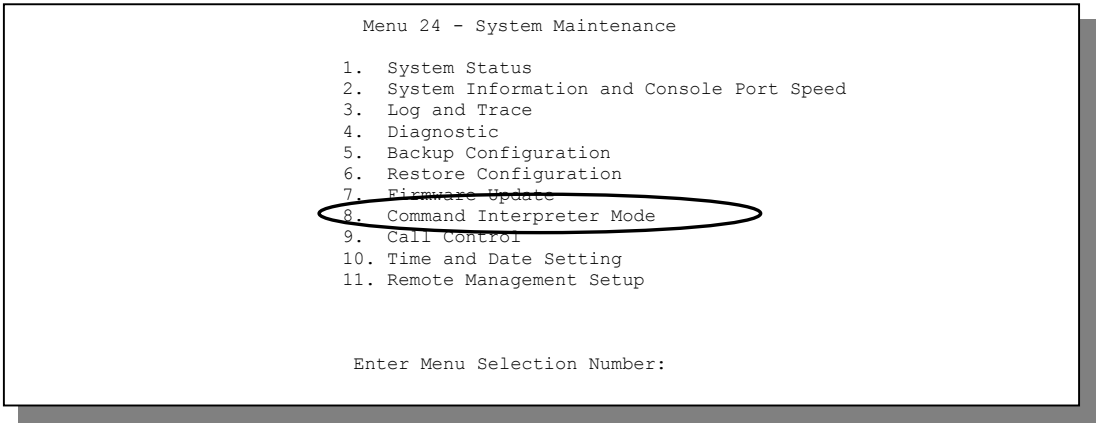


Figure 35-1 Command Mode in Menu 24

35.1.1 Command Syntax

The command keywords are in `courier new` font.

Enter the command keywords exactly as shown, do not abbreviate.

The required fields in a command are enclosed in angle brackets <>.

The optional fields in a command are enclosed in square brackets `[]`.

The `|` symbol means "or".

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

35.1.2 Command Usage

A list of commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            ether           aux
ip              ipsec           bridge          bm
8021x
```

Figure 35-2 Valid Commands

Table 35-1 Valid Commands

COMMAND	DESCRIPTION
sys	The system commands display device information and configure device settings.
exit	This command returns you to the SMT main menu.
ether	These commands display Ethernet information and configure Ethernet settings.

Table 35-1 Valid Commands

aux	These commands display dial backup information and control dial backup connections.
ip	These commands display IP information and configure IP settings.
ipsec	These commands display IPSec information and configure IPSec settings.
bridge	These commands display bridge information.
bm	These commands configure bandwidth management settings and display bandwidth management information.
8021x	These commands configure 802.1x settings and display 802.1x information.

35.2 Call Control Support

The ZyWALL provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the ZyWALL within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

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

```
Menu 24.9 - System Maintenance - Call Control

        1.Budget Management
        2.Call History



          Enter Menu Selection Number:
```

Figure 35-3 Call Control

35.2.1 Budget Management

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

```
                        Menu 24.9.1 - Budget Management

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









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

Figure 35-4 Budget Management

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

Table 35-2 Budget Management

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

35.2.2 Call History

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

```
                        Menu 24.9.2 - Call History

    Phone Number    Dir    Rate      #call        Max         Min         Total
 1.
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.
                        Enter Entry to Delete(0 to exit):
```

Figure 35-5 Call History

The following table describes the fields in this screen.

Table 35-3 Call History Fields

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

35.3 Time and Date Setting

The Real Time Chip (RTC) keeps track of the time and date (Not available on all models). There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL. Menu 24.10 allows you to update the time and date settings of your ZyWALL. The real time is then displayed in the ZyWALL error logs and firewall logs.

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

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

Figure 35-6 Menu 24: System Maintenance

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

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


Use Time Server when Bootup= NTP (RFC-1305)
Time Server Address= tick.stdtime.gov.tw

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

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

Time Zone= GMT+0800

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

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

Figure 35-7 Menu 24.10 System Maintenance: Time and Date Setting

The following table describes the fields in this screen.

Table 35-4 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your timeserver sends when you turn on the ZyWALL. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** the default, is similar to **Time (RFC-868)**. **None** enter the time manually.
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format.

Table 35-4 Time and Date Setting Fields

FIELD	DESCRIPTION
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose **Yes**.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Yes** in the **Daylight Saving** field.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Yes** in the **Daylight Saving** field.
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

35.3.1 Resetting the Time

The ZyWALL resets the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the ZyWALL starts up, if there is a timeserver configured in menu 24.10.

iii. 24-hour intervals after starting.

Chapter 36
Remote Management

This chapter covers remote management found in SMT menu 24.11.

36.1 Remote Management

Remote management allows you to determine which services/protocols can access which ZyWALL interface (if any) from which computers.

You may manage your ZyWALL from a remote location via:

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

When you Choose WAN only **or** ALL **(LAN & WAN), you still need to configure a firewall rule to allow access.**

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

```
            Menu 24.11 - Remote Management Control

TELNET Server:     Port = 23         Access = LAN only
                   Secured Client IP = 0.0.0.0

FTP Server:        Port = 21         Access = LAN only
                   Secured Client IP = 0.0.0.0

Web Server:        Port = 80         Access = LAN only
                   Secured Client IP = 0.0.0.0

SNMP Service:      Port = 161        Access = LAN only
                   Secured Client IP = 0.0.0.0

DNS Service:       Port = 53         Access = LAN only
                   Secured Client IP = 0.0.0.0


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

Figure 36-1 Menu 24.11 – Remote Management Control

The following table describes the fields in this screen.

Table 36-1 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server SNMP Service DNS Service	Each of these read-only labels denotes a service that you may use to remotely manage the ZyWALL.	
Server Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.	23
Server Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**.	**LAN Only** (default)
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyWALL. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

36.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
6. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

Part XIV:

SMT Advanced Management

This part provides information on how to configure IP Policy Routing, call scheduling, and VPN/IPSec.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 37
IP Policy Routing

This chapter covers setting and applying policies used for IP routing. IP Policy Routing applies to the ZyWALL 100.

37.1 Introduction to IP Policy Routing

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. This feature is not available on all models.

37.2 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or ToS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

37.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination

address and port, ToS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.
The actions that can be taken include:

- Routing the packet to a different gateway (and hence the outgoing interface).
- Setting the ToS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with six policies in each set.

37.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.

```
                Menu 25 - IP Routing Policy Setup

Policy                                  Policy
Set #          Name                     Set #          Name
------  ------------------              ------  ------------------
  1     test                              7     ________________
  2     ________________                  8     ________________
  3     ________________                  9     ________________
  4     ________________                 10     ________________
  5     ________________                 11     ________________
  6     ________________                 12     ________________


                Enter Policy Set Number to Configure= 0

                Edit Name= N/A

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

Figure 37-2 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

Step 1. Type 25 in the main menu to open **Menu 25 – IP Routing Policy Setup.**

Step 2. Type the index of the policy set you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator "|" means the action is taken on criteria matched and separator "=" means the action is taken on criteria not matched.

```
                    Menu 25.1 - IP Routing Policy Setup

 # A                          Criteria/Action
 - - ------------------------------------------------------------------------
 1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
     SP=20-25,DP=20-25,P=6,T=NM,PR=0              |GW=192.168.1.1,T=MT,PR=0
 2 N ____________________________________________________________________________
     ____________________________________________________________________________
 3 N ____________________________________________________________________________
     ____________________________________________________________________________
 4 N ____________________________________________________________________________
     ____________________________________________________________________________
 5 N ____________________________________________________________________________
     ____________________________________________________________________________
 6 N ____________________________________________________________________________
     ____________________________________________________________________________

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

Figure 37-4 Menu 25.1: Sample IP Routing Policy Setup

Table 37-1 IP Routing Policy Setup

ABBREVIATION		MEANING
Criterion	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17…)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address

Table 37-1 IP Routing Policy Setup

ABBREVIATION	MEANING
T	Outgoing Type of service
P	Outgoing Precedence
Service NM	Normal
MD	Minimum Delay
MT	Maximum Throughput
MR	Maximum Reliability
MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.

```
                    Menu 25.1.1 - IP Routing Policy

Policy Set Name= test
Active= Yes
Criteria:
  IP Protocol    = 6
  Type of Service= Normal          Packet length= 40
  Precedence     = 0                 Len Comp= N/A
  Source:
    addr start= 1.1.1.1            end= 1.1.1.1
    port start= 20                 end= 20
  Destination:
    addr start= 2.2.2.2            end= 2.2.2.2
    port start= 20                 end= 20
Action= Matched
  Gateway addr   = 192.168.1.1     Log= No
  Type of Service= Max Thruput
  Precedence     = 0

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

Figure 37-5 IP Routing Policy

Table 37-2 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in **Menu 25 – IP Routing Policy Setup**.

Table 37-2 IP Routing Policy

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the policy.
Criteria	
IP Protocol	Enter a number that represents an IP layer 4 protocol, for example, UDP=17, TCP=6, ICMP=1 and Don't care=0.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput** or **Max Reliable**.
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from **0** to **7** or **Don't Care**.
Packet Length	Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source addr start / end	 Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination addr start / end	 Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria **Matched** or **Not Matched**.
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the ZYWALL if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **No Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Precedence	Set the new outgoing packet precedence value. Values are 0 to 7 or **No Change**.
Log	Press [SPACE BAR] and then [ENTER] to select **Yes** to make an entry in the system log when a policy is executed.

Table 37-2 IP Routing Policy

FIELD	DESCRIPTION
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

37.5 Applying an IP Policy

This section shows you where to apply the IP policies after you design them.

37.5.1 Ethernet IP Policies

From **Menu 3 – Ethernet Setup**, type 2 to go to **Menu 3.2 – TCP/IP and DHCP Ethernet Setup**. You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, for example, 2, 4, 7, 9.

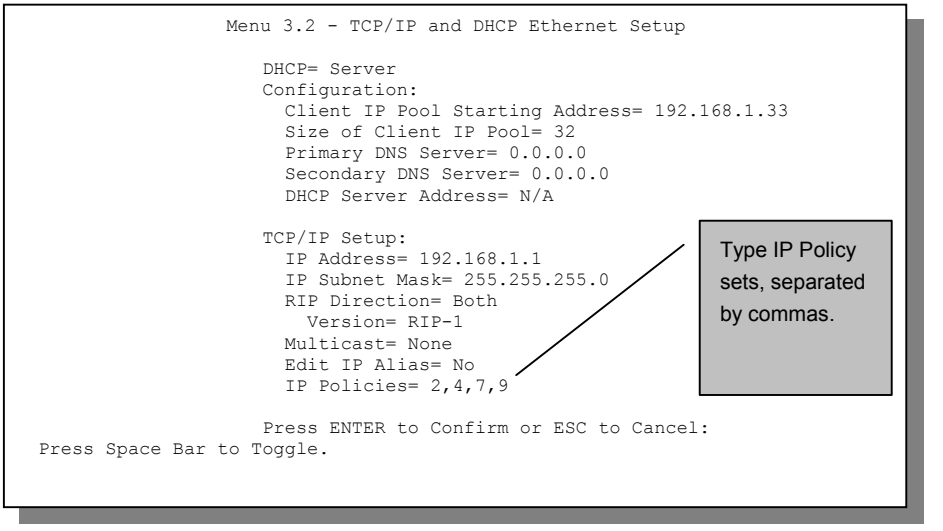


Figure 37-6 Menu 3.2: TCP/IP and DHCP Ethernet Setup

37.6 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

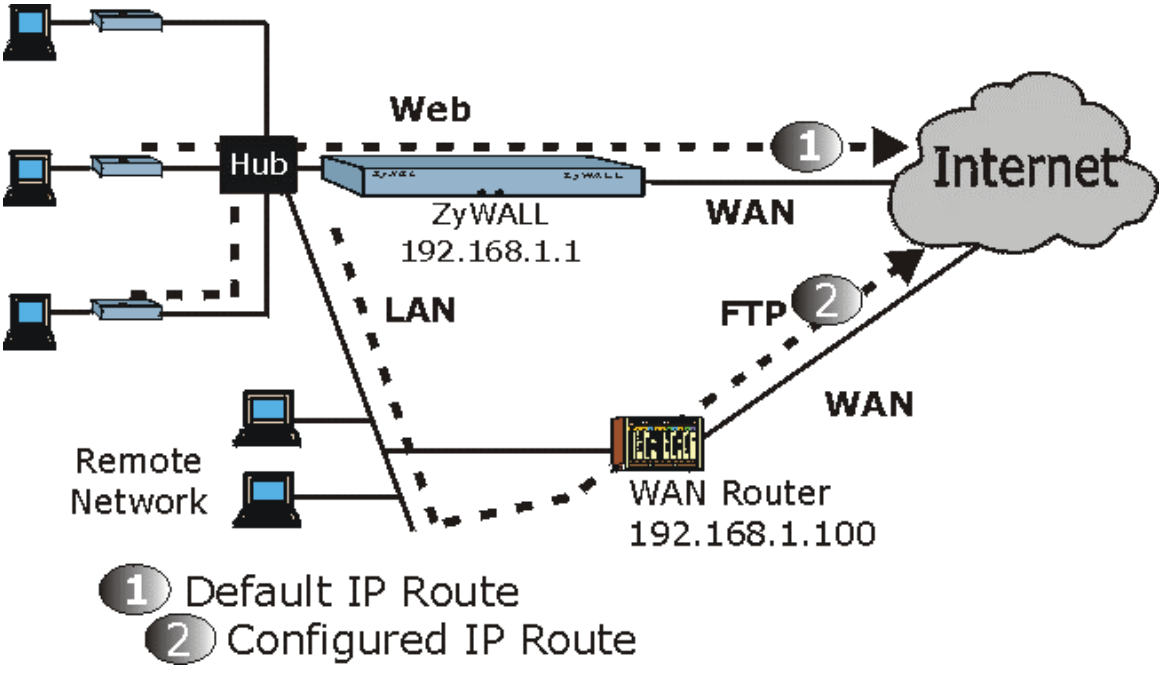


Figure 37-7 Example of IP Policy Routing

To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the ZyWALL, follow the steps as shown next.

Step 1. Create a routing policy set in menu 25.

Step 2. Create a rule for this set in **Menu 25.1.1 - IP Routing Policy** as shown next.

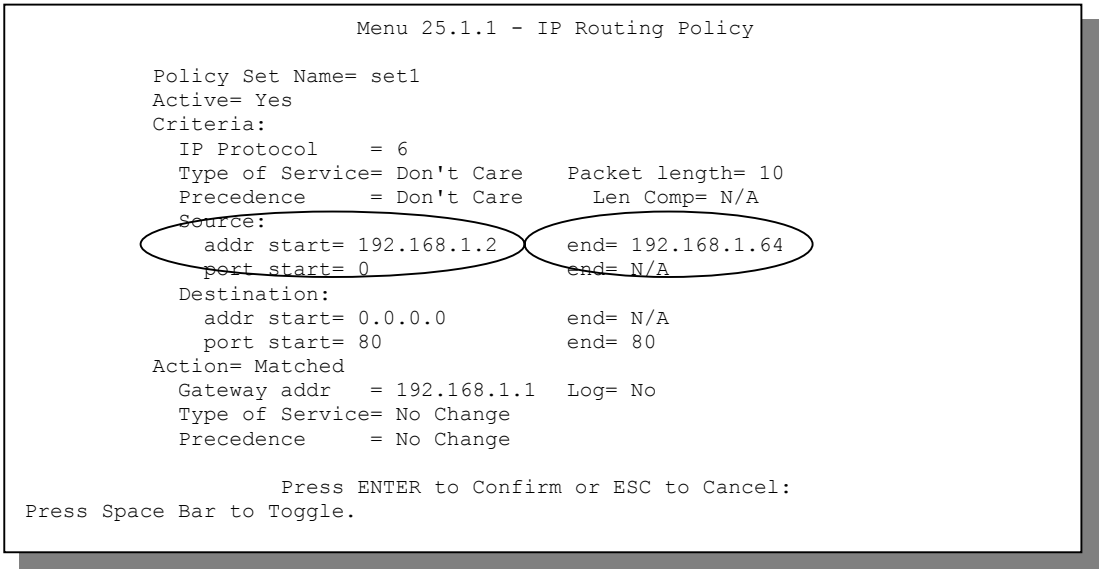


Figure 37-8 IP Routing Policy Example

Step 3. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 4. Create another policy set in menu 25.

Step 5. Create a rule in menu 25.1.1 for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

```
                        Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set2

          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care      Packet length= 10
            Precedence     = Don't Care        Len Comp= N/A
            Source:
              addr start= 0.0.0.0            end= N/A
              port start= 0                  end= N/A
            Destination:
              addr start= 0.0.0.0            end= N/A
              port start= 20                 end= 21
          Action= Matched
            Gateway addr  =192.168.1.100     Log= No
            Type of Service= No Change
            Precedence     = No Change

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

Figure 37-9 IP Routing Policy

Step 6. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 7. Apply both policy sets in menu 3.2 as shown next.

```
                Menu 3.2 - TCP/IP and DHCP Ethernet Setup

                DHCP Setup
                  DHCP= Server
                  Client IP Pool Starting Address= 192.168.1.33
                  Size of Client IP Pool= 64
                  Primary DNS Server= 0.0.0.0
                  Secondary DNS Server= 0.0.0.0
                  Remote DHCP Server= N/A
                TCP/IP Setup:
                  IP Address= 192.168.1.1
                  IP Subnet Mask= 255.255.255.0
                  RIP Direction= Both
                    Version= RIP-1
                  Multicast= None
                  IP Policies= 1,2
                  Edit IP Alias= No

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

Figure 37-10 Applying IP Policies

Chapter 38
Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

38.1 Introduction to Call Scheduling

The call scheduling feature allows the ZyWALL to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 - Schedule Setup** as shown next.

```
                          Menu 26 - Schedule Setup

     Schedule                              Schedule
      Set #              Name               Set #              Name
     ------       -------------------       ------      -------------------
        1           _______________           7           _______________
        2           _______________           8           _______________
        3           _______________           9           _______________
        4           _______________           10          _______________
        5           _______________           11          _______________
        6           _______________           12          _______________

                       Enter Schedule Set Number to Configure=

                       Edit Name=

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

Figure 38-1 Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node, then set 1 will take precedence over set 2, 3 and 4 as the ZyWALL, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] or [DEL] in the Edit Name field.

To set up a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

```
                        Menu 26.1 - Schedule Set Setup

                Active= Yes
                Start Date(yyyy/mm/dd) = 2000 - 01 - 01
                How Often= Once
                Once:
                  Date(yyyy/mm/dd)= 2000 - 01 - 01
                Weekdays:
                  Sunday= N/A
                  Monday= N/A
                  Tuesday= N/A
                  Wednesday= N/A
                  Thursday= N/A
                  Friday= N/A
                  Saturday= N/A
                Start Time (hh:mm)= 00 : 00
                Duration (hh:mm)= 00 : 00
                Action= Forced On

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

Figure 38-2 Schedule Set Setup

If a connection has been already established, your ZyWALL will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 38-1Schedule Set Setup Fields

FIELD	DESCRIPTION	OPTIONS
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.	**Yes** **No**
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.	
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	**Once** **Weekly**
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.	

Table 38-1Schedule Set Setup Fields

FIELD	DESCRIPTION	OPTIONS
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].	**Yes** **No** **N/A**
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On** **Forced Down** **Enable Dial-On-Demand** **Disable Dial-On-Demand**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the Main Menu and then enter the target remote node index. Press [SPACE BAR] and then [ENTER] to select **PPPoE** in the **Encapsulation** field to make the schedule sets field available as shown next.

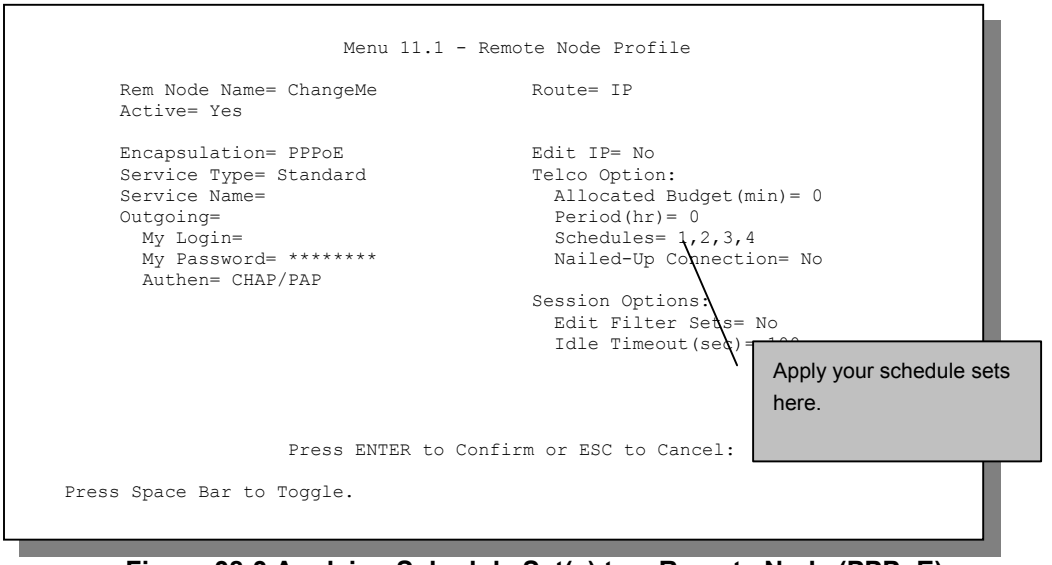


Figure 38-3 Applying Schedule Set(s) to a Remote Node (PPPoE)

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

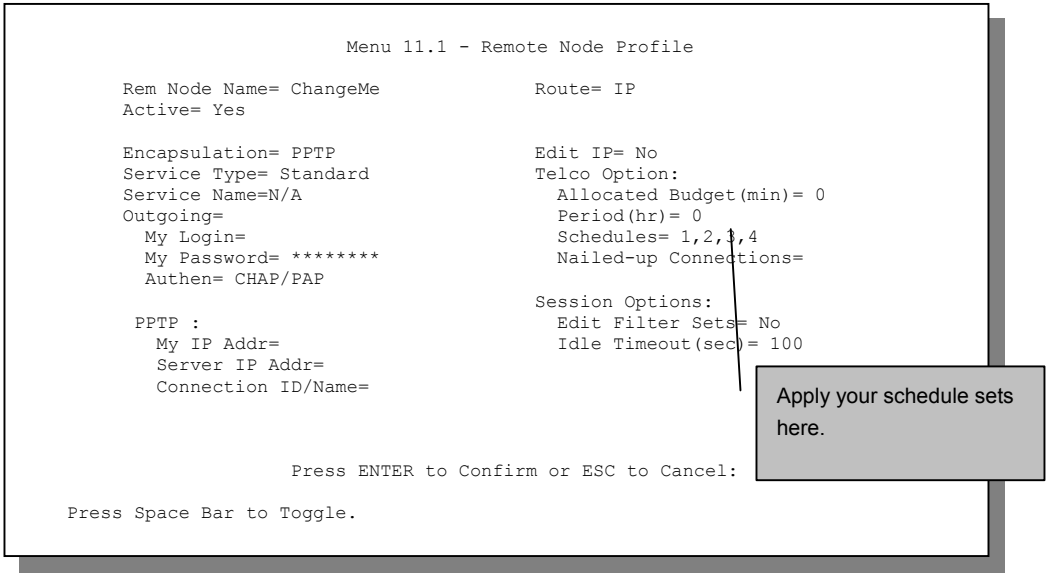


Figure 38-4 Applying Schedule Set(s) to a Remote Node (PPTP)

Chapter 39
VPN/IPSec Setup

This chapter introduces the VPN SMT menus.

39.1 Introduction

The VPN/IPSec main SMT menu has these main submenus:

1. Define VPN policies in menu 27.1 submenus, including security policies, endpoint IP addresses, peer IPSec router IP address and key management.
2. **Menu 27.2 - SA Monitor** allows you to manage (refresh or disconnect) your SA connections.

This is an overview of the VPN menu tree.

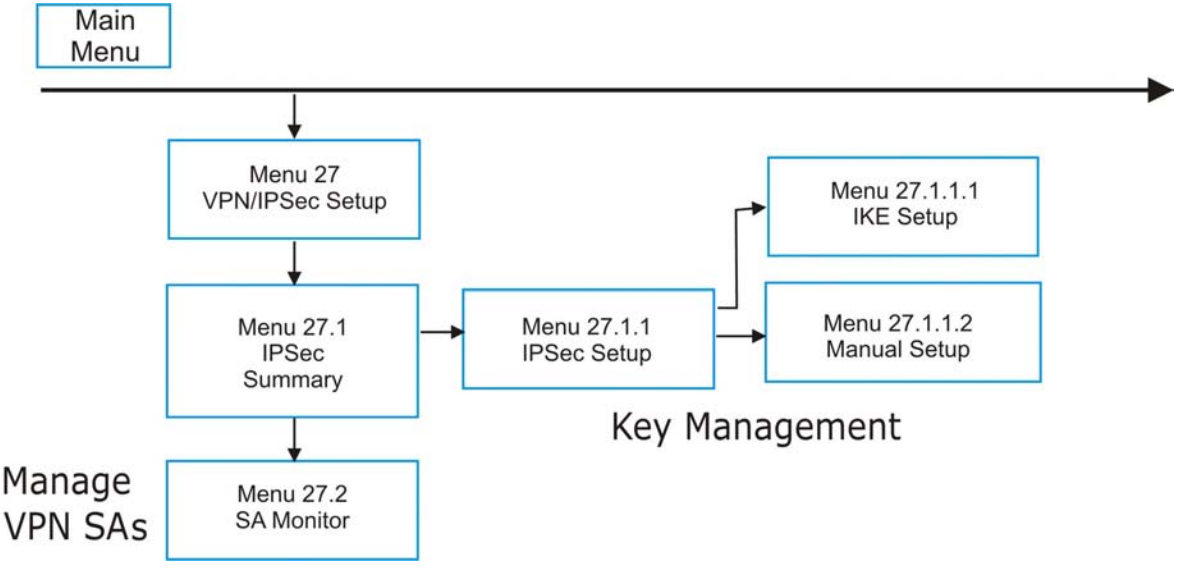


Figure 39-1 VPN SMT Menu Tree

From the main menu, enter 27 to display the first VPN menu (shown next).

```
                              Menu 27 - VPN/IPSec Setup

                          1. IPSec Summary
                          2. SA Monitor




                                 Enter Menu Selection Number:
```

Figure 39-2 Menu 27: VPN/IPSec Setup

39.2 IPSec Summary Screen

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 — IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

```
                              Menu 27.1 - IPSec Summary

#  Name       A  Local Addr Start    - Local Addr End    Encap    IPSec Algorithm
   Key Mgt       Remote Addr Start   - Remote Addr End           Secure GW Addr
-  ------     -  -----------------   ---------------     ------   ------------------
1    Taiwan   Y  192.168.1.35        192.168.1.38        Tunnel   ESP DES MD5
       IKE      172.16.2.40         172.16.2.46                  193.81.13.2
2      zw50   N  1.1.1.1            1.1.1.1             Tunnel   AH SHA1
       IKE      4.4.4.4             255.255.0.0                  zw50test.zyxel.
3     China   N  192.168.1.40       192.168.1.42        Tunnel   ESP DES MD5
       IKE      N/A                 N/A                          0.0.0.0
4

5



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

Figure 39-3 Menu 27.1: IPSec Summary

Table 39-1 Menu 27.1: IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
#	This is the VPN policy index number.	1
Name	This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here.	Taiwan
A	**Y** signifies that this VPN rule is active.	**Y**
Local Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the LAN behind your ZyWALL. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the LAN behind your ZyWALL.	192.168.1.35
Local Addr End	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Local Addr Start** field. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the LAN behind your ZyWALL.	192.168.1.38
Encap	This field displays **Tunnel** mode or **Transport** mode. See earlier for a discussion of these. You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.	**Tunnel**

Table 39-1 Menu 27.1: IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption. **AH** (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits)**.** Both **AH** and **ESP** increase the ZyWALL's processing requirements and communications latency (delay). You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.	**ESP DES MD5**
Key Mgt	This field displays the SA's type of key management, (**IKE** or **Manual**).	**IKE**
Remote Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.	172.16.2.40

Table 39-1 Menu 27.1: IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Remote Addr End	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Remote Addr Start** field. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.	172.16.2.46
Secure GW Addr	This is the WAN IP address or the domain name (up to the first 15 characters are displayed) of the IPSec router with which you are making the VPN connection. This field displays **0.0.0.0** when you configure the **Secure Gateway Addr** field in SMT 27.1.1 to 0.0.0.0.	193.81.13.2
Select Command	Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Go To Rule**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, Delete or **Go To** commands. Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt. Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a VPN rule is deleted, subsequent rules do not move up in the page list. Use **Go To Rule** to view the page where your desired rule is listed. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).	**None**
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].	3
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

39.3 IPSec Setup

Select **Edit** in the **Select Command** field; type the index number of a rule in the **Select Rule** field and press [ENTER] to edit the VPN using the menu shown next.

```
                Menu 27.1.1 - IPSec Setup

Index= 1          Name= Taiwan
Active= Yes       Keep Alive= No    NAT Traversal= No
Local ID type             Content:
My IP Addr= 0.0.0.0
Peer ID type              Content:
Secure Gateway Address= zw50test.zyxel.com.tw
Protocol= 0
Local:         Addr Type= SINGLE
           IP Addr Start= 1.1.1.1         End= N/A
              Port Start= 0               End= N/A
Remote:        Addr Type= SUBNET
           IP Addr Start= 4.4.4.4         End= 255.255.0.0
              Port Start= 0               End= N/A
Enable Replay Detection = No
Key Management= IKE
Edit Key Management Setup= No



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

Figure 39-4 Menu 27.1.1: IPSec Setup

You must also configure menu 27.1.1.1 or menu 27.1.1.2 to fully configure and use a VPN.

Table 39-2 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Index	This is the VPN rule index number you selected in the previous menu.	**1**
Name	Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed in **Menu 27.1 - IPSec Summary**.	Taiwan
Active	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall.	**Yes**

Table 39-2 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Keep Alive	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to have the ZyWALL automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.	**No**
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. The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with **Manual** key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.	**No**
Local ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER]. Select **IP** to identify this ZyWALL by its IP address. Select **DNS** to identify this ZyWALL by a domain name. Select **E-mail** to identify this ZyWALL by an e-mail address.	
Content	When you select **IP** in the **Local ID type** field, type the IP address of your computer in the local **Content** field. The ZyWALL automatically uses the IP address in the **My IP Address** field (refer to the My IP Address field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. ➢ When there is a NAT router between the two IPSec routers. ➢ When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID type** field, type a domain name or e-mail address by which to identify this ZyWALL in the local Content field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.	

Table 39-2 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
My IP Addr	Enter the IP address of your ZyWALL. The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0. The VPN tunnel has to be rebuilt if this IP address changes.	0.0.0.0
Peer ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER]. Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.	
Content	When you select **IP** in the **Peer ID type** field, type the IP address of the computer with which you will make the VPN connection in the peer **Content** field. The ZyWALL automatically uses the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description) if you configure the peer **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the peer **Content** field or use the **DNS** or **E-mail** ID type in the following situations. ➢ When there is a NAT router between the two IPSec routers. ➢ When you want the ZyWALL to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Peer ID type** field, type a domain name or e-mail address by which to identify the remote IPSec router in the peer **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.	
Secure Gateway Address	Type the IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**, see later).	Zw50test.com.tw
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.	0

Table 39-2 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.	
Addr Type	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Select **RANGE** for a specific range of IP addresses. Select **SUBNET** to specify IP addresses on a network by their subnet mask.	**SINGLE**
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a static IP address on the LAN behind your ZyWALL. When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyWALL. When the **Addr Type** is configured to **SUBNET**, this is a (static) IP address on the LAN behind your ZyWALL.	192.168.1.35
End	When the **Addr Type** field is configured to **Single**, this field is **N/A**. When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Addr Type** field is configured to **SUBNET**, this is a subnet mask on the LAN behind your ZyWALL.	192.168.1.38
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. You cannot create a VPN tunnel if you try to connect using a port number that does not match this port number or range of port numbers. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3	0
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.	N/A

Table 39-2 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields are **N/A** when the **Secure Gateway Address** field is configured to 0.0.0.0. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.	
Addr Type	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Use **RANGE** for a specific range of IP addresses. Use **SUBNET** to specify IP addresses on a network by their subnet mask.	**SUBNET**
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a static IP address on the network behind the remote IPSec router. When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field is configured to **SUBNET**, enter a static IP address on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.	4.4.4.4
End	When the **Addr Type** field is configured to **Single**, this field is **N/A**. When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field is configured to **SUBNET**, enter a subnet mask on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.	255.255.0.0
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Someone behind the remote IPSec router cannot create a VPN tunnel when attempting to connect using a port number that does not match this port number or range of port numbers. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.	0

Table 39-2 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.	
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to **Yes**. Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to enable replay detection.	**No**
Key Management	Press [SPACE BAR] to choose either **IKE** or **Manual** and then press [ENTER]. **Manual** is useful for troubleshooting if you have problems using **IKE** key management.	**IKE**
Edit Key Management Setup	Press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to a key management menu for configuring your key management setup (described later). If you set the **Key Management** field to **IKE**, this will take you to **Menu 27.1.1.1 – IKE Setup**. If you set the **Key Management** field to **Manual**, this will take you to **Menu 27.1.1.2 – Manual Setup**.	**No**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

39.4 IKE Setup

To edit this menu, the **Key Management** field **Menu 27.1.1 – IPSec Setup** must be set to **IKE**. Move the cursor to the **Edit Key Management Setup** field in **Menu 27.1.1 – IPSec Setup**; press [SPACE BAR] to select **Yes** and then press [ENTER] to display **Menu 27.1.1.1 – IKE Setup**.

```
                    Menu 27.1.1.1 - IKE Setup

              Phase 1
                Negotiation Mode= Main
                Pre-Shared Key=
                Encryption Algorithm = DES
                Authentication Algorithm = SHA1
                SA Life Time (Seconds)= 28800
                Key Group= DH1

              Phase 2
                Active Protocol  = ESP
                Encryption Algorithm  = DES
                Authentication Algorithm  = SHA1
                SA Life Time (Seconds)= 28800
                Encapsulation  = Tunnel
                Perfect Forward Secrecy (PFS)= None


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

Figure 39-5 Menu 27.1.1.1: IKE Setup

Table 39-3 Menu 27.1.1.1: IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Phase 1		
Negotiation Mode	Press [SPACE BAR] to choose from **Main** or **Aggressive** and then press [ENTER]. See earlier for a discussion of these modes. Multiple SAs connecting through a secure gateway must have the same negotiation mode.	**Main**
Pre-Shared Key	ZyWALL gateways authenticate an IKE VPN session by matching pre-shared keys. Pre-shared keys are best for small networks with fewer than ten nodes. Enter your pre-shared key here. Enter up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated. 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.	

Table 39-3 Menu 27.1.1.1: IKE Setup

FIELD	DESCRIPTION	EXAMPLE
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. ZyWALL **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 slightly increased latency and decreased throughput. Press [SPACE BAR] to choose from **3DES** or **DES** and then press [ENTER].	**DES**
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 slightly slower. Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].	**SHA1**
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). 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.	28800 (default)
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.	**DH1**
Phase 2		
Active Protocol	Press [SPACE BAR] to choose from **ESP** or **AH** and then press [ENTER]. See earlier for a discussion of these protocols.	**ESP**
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Select **NULL** to set up a tunnel without encryption.	**DES**
Authentication Algorithm	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].	**MD5**
SA Life Time (Seconds)	Define the length of time before an IPSec Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).	28800 (default)
Encapsulation	Press [SPACE BAR] to choose from **Tunnel** mode or **Transport** mode and then press [ENTER]. See earlier for a discussion of these.	**Tunnel**

Table 39-3 Menu 27.1.1.1: IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Press [SPACE BAR] and choose from **DH1** or **DH2** 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 (more secure, yet slower).	**None**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

39.5 Manual Setup

You only configure **Menu 27.1.1.2 – Manual Setup** when you select **Manual** in the **Key Management** field in **Menu 27.1.1 – IPSec Setup**. Manual key management is useful if you have problems with **IKE** key management.

39.5.1 Active Protocol

This field is a combination of mode and security protocols used for the VPN. See the *Web Configurator User's Guide* for more information on these parameters.

Table 39-4 Active Protocol: Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

39.5.2 Security Parameter Index (SPI)

To edit this menu, move the cursor to the **Edit Manual Setup** field in **Menu 27.1.1 – IPSec Setup** press [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 27.1.1.2 – Manual Setup**.

```
                Menu 27.1.1.2 - Manual Setup
Active Protocol= ESP Tunnel

ESP Setup
  SPI=
  Encryption Algorithm= DES
    Key1=
    Key2= N/A
    Key3= N/A
  Authentication Algorithm= MD5
    Key= N/A

AH Setup
  SPI (Decimal)= N/A
  Authentication Algorithm= N/A
    Key=

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

Figure 39-6 Menu 27.1.1.2: Manual Setup

Table 39-5 Menu 27.1.1.2: Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Active Protocol	Press [SPACE BAR] to choose from **ESP Tunnel**, **ESP Transport**, **AH Tunnel** or **AH Transport** and then press [ENTER]. Choosing an **ESP** combination causes the **AH Setup** fields to be non-applicable (**N/A**)	**ESP Tunnel**
ESP Setup	The **ESP Setup** fields are **N/A** if you chose an **AH Active Protocol**.	
SPI	The **SPI** must be unique and from one to four integers ("0" to "9").	1234
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Fill in the **Key1** field below when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter any encryption keys.	**DES**
Key1	Enter a unique eight-character key. Any character may be used, including spaces, but trailing spaces are truncated. Fill in the **Key1** field when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**.	89abcde
Key2	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).	
Key3	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).	

Table 39-5 Menu 27.1.1.2: Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].	**MD5**
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.	123456789abcde
AH Setup	The **AH Setup** fields are **N/A** if you chose an **ESP Active Protocol**.	
SPI (Decimal)	The **SPI** must be from one to four unique decimal characters ("0" to "9") long.	**N/A**
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].	**N/A**
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.	**N/A**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Chapter 40
SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

40.1 Introduction

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See the *Web Configurator User's Guide on* keep alive to have the ZyWALL renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

40.2 Using SA Monitor

1. Use the **Refresh** function to display active VPN connections.
2. Use the **Disconnect** function to cut off active connections.

Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.

```
                        Menu 27.2 - SA Monitor

 #                  Name                    Encap.     IPSec ALgorithm
---   --------------------------------   ---------   ----------------
001    Taiwan : 3.3.3.1 - 3.3.3.3.100      Tunnel     ESP DES MD5
002
003
004
005
006
007
008
009
010
                  Select Command= Refresh
                  Select Connection= N/A

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

Figure 40-1 Menu 27.2: SA Monitor

Table 40-1 Menu 27.2: SA Monitor

FIELD	DESCRIPTION	EXAMPLE
#	This is the security association index number.	
Name	This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a public static IP address. When the secure gateway IP address is 0.0.0.0 (as discussed in the last chapter), there may be different connections using this same VPN rule. In this case, the name is followed by the remote IP address as configured in **Menu 27.1.1. – IPSec Setup**. Individual connections using the same VPN rule may be terminated without affecting other connections using the same rule.	**Taiwan**
Encap.	This field displays **Tunnel** mode or **Transport** mode. See previous for discussion.	**Tunnel**
IPSec ALgorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption. An incoming SA may have an **AH** in addition to **ESP**. The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits). Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay).	**ESP DES MD5**
Select Command	Press [SPACE BAR] to choose from **Refresh**, **Disconnect**, **None**, **Next Page**, or **Previous Page** and then press [ENTER]. You must select a connection in the next field when you choose the **Disconnect** command. **Refresh** displays current active VPN connections. **None** allows you to jump to the “Press ENTER to Confirm…” prompt. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).	**Refresh**
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].	**1**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Part XV:

Appendices and Index

This part provides information about hardware specifications, safety warnings, how to change a ZyWALL 100 fuse and an index of key terms.

Appendix A Troubleshooting

This chapter covers potential problems and possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem. Please see our included disk for further information. DMZ applies to the ZyWALL 100.

Problems Starting Up the ZyWALL

Chart 1 Troubleshooting the Start-Up of Your ZyWALL

<table>
<tr><th>PROBLEM</th><th colspan="2">CORRECTIVE ACTION</th></tr>
<tr><td rowspan="3">None of the LEDs turn on when you turn on the ZyWALL.</td><td colspan="2">Make sure that you have the included power adaptor or cord connected to the ZyWALL and to an appropriate power source.</td></tr>
<tr><td colspan="2">Replace the fuse if it is burnt out (see the appendices for more on changing a fuse).</td></tr>
<tr><td colspan="2">If the error persists, you may have a hardware problem. In this case, you should contact your vendor.</td></tr>
<tr><td rowspan="4">Cannot access the ZyWALL via the console port.</td><td colspan="2">1. Check to see if the ZyWALL is connected to your computer’s console port.</td></tr>
<tr><td rowspan="3">2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:</td><td>VT100 terminal emulation</td></tr>
<tr><td>9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.</td></tr>
<tr><td>No parity, 8 data bits, 1 stop bit, data flow set to none.</td></tr>
</table>

Problems with the LAN Interface

Chart 2 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL from the LAN.	Check your Ethernet cable type and connections. Refer to the *Quick Start Guide* or *Compact Guide* for LAN connection instructions.
	Make sure the computer's Ethernet adapter is installed and functioning properly.
Cannot ping any computer on the LAN.	Check the 10M/100M LAN LEDs on the front panel. One of these LEDs should be on. If they are both off, check the cables between your ZyWALL and hub or the station.
	Verify that the IP address and the subnet mask of the ZyWALL and the computers are on the same subnet.

Problems with the DMZ Interface

The DMZ interface is not available on all models.

Chart 3 Troubleshooting the DMZ Interface

PROBLEM	CORRECTIVE ACTION
Cannot access servers on the DMZ from the LAN.	Check your Ethernet cable type and connections. Refer to the *Quick Start Guide* or *Compact Guide* for DMZ connection instructions.
	Make sure the Ethernet adapters on the LAN computer and the DMZ server are installed and functioning properly.
	Verify that the IP address of the DMZ port and the LAN port are on separate subnets.
	Make sure that NAT is configured for your DMZ servers.
Cannot ping any computer on the DMZ.	Check the 10M/100M DMZ LEDs on the front panel. One of these LEDs should be on. If they are both off, check the cables between your ZyWALL and hub or the station.
	Verify that the IP address and the subnet mask of the ZyWALL and the servers are on the same subnet.

Problems with the WAN Interface

Chart 4 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot get WAN IP address from the ISP.	The ISP provides the WAN IP address after authentication. Authentication may be through the user name and password, the MAC address or the host name. Use the following corrective actions to make sure the ISP can authenticate your connection.
	You need a username and password if you're using PPPoE or PPTP encapsulation. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (the user name and password are case sensitive). Refer to the *WAN Screens* chapter (web configurator) or the *Internet Access* chapter (SMT).
	If your ISP requires MAC address authentication, you should clone the MAC address from your computer on the LAN as the ZyWALL's WAN MAC address. Refer to the *WAN Screens* chapter (web configurator) or the *WAN and Dial Backup Setup* chapter (SMT). It is recommended that you clone your computer's MAC address, even if your ISP presently does not require MAC address authentication.
	If your ISP requires host name authentication, configure your computer's name as the ZyWALL's system name. Refer to the *Wizard Setup* chapter (web configurator) or the *General Setup* chapter (SMT).

Problems with Internet Access

Chart 5 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
Cannot access the Internet.	Connect your cable/DSL modem with the ZyWALL using the appropriate cable. Check with the manufacturer of your cable/DSL device about your cable requirement because some devices may require crossover cable and others a regular straight-through cable.
	Refer to the *WAN Screens* chapter (web configurator) or the *Internet Access* chapter (SMT) and verify your settings.

Problems with the Password

Chart 6 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL.	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	Use the Reset button to restore the factory default configuration file. This will restore all of the factory defaults including the password. See *t*he *Resetting the ZyWALL* section in the *Introducing the Web Configurator* chapter for details.

Problems with Remote Management

Chart 7 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL from the LAN or WAN.	Refer to the *Remote Management Limitations* section in the *Remote Management* chapter for scenarios when remote management may not be possible.
	When NAT is enabled: ➢ Use the ZyWALL's WAN IP address when configuring from the WAN. ➢ Use the ZyWALL's LAN IP address when configuring from the LAN.
	Refer to the *Problems with the LAN Interface* section for instructions on checking your LAN connection.
	Refer to the *Problems with the WAN Interface* section for instructions on checking your WAN connection.

Appendix B
Hardware Specifications

Chart 8 General Specifications

Power Specification (ZyWALL 100)	100-240 VAC, 50/60Hz
Power Specification (ZyWALL 10,10W, 30W, 50)	I/P AC 120V / 60Hz; O/P DC 12V 1200 mA
Power Consumption (ZyWALL 100)	16 Watts maximum
Power Current (ZyWALL 100)	1.9 Amps
Fuse Rating (ZyWALL 100)	0.5 Amps, 250 VAC
MTBF	100000 hrs (Mean Time Between Failures)
Operation Temperature	0º C ~ 40º C
Ethernet Specification for WAN (Not on all models)	10/100Mbps Half / Full Auto-negotiation
Ethernet Specification for WAN (Not on all models)	10Mbps Half / Full Auto-negotiation
Ethernet Specification for DMZ (Not on all models)	10/100Mbps Half / Full Auto-negotiation
Ethernet Specification for LAN	10/100Mbps Half / Full Auto-negotiation

Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The ZyWALL is DCE when you connect a computer to the console port. The ZyWALL is DTE when you connect a modem to the dial backup port.

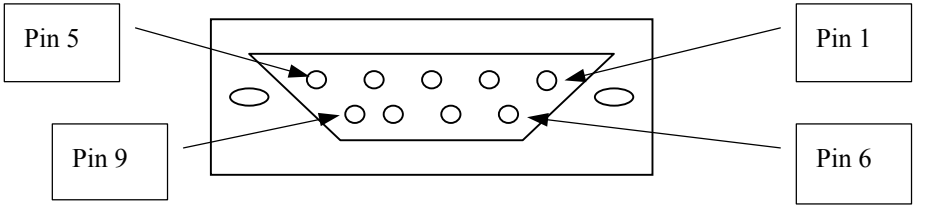


Diagram 1 Console/Dial Backup Port Pin Layouts [1]

Chart 9 Console/Dial Backup Port Pin Assignments

CONSOLE Port RS – 232 (Female) DB-9F	DIAL BACKUP RS – 232 (Male) DB-9M (Not on all models)
Pin 1 = NON	Pin 1 = NON
Pin 2 = DCE-TXD	Pin 2 = DTE-RXD
Pin 3 = DCE –RXD	Pin 3 = DTE-TXD
Pin 4 = DCE –DSR	Pin 4 = DTE-DTR
Pin 5 = GND	Pin 5 = GND
Pin 6 = DCE –DTR	Pin 6 = DTE-DSR
Pin 7 = DCE –CTS	Pin 7 = DTE-RTS
Pin 8 = DCE –RTS	Pin 8 = DTE-CTS
PIN 9 = NON	PIN 9 = NON.
The CON/AUX port also has these pin assignments. The CON/AUX switch changes the setting in the firmware only and does not change the CON/AUX port's pin assignments.	ZyWALLs with a CON/AUX port also have a 9-pin adaptor for the console cable with these pin assignments on the male end.

[1] Products without flow control only use pins 2,3 and 5.

Chart 10 Ethernet Cable Pin Assignments

WAN/LAN/DMZ Ethernet Cable Pin Layout: Straight-Through			Crossover		
(Switch)		(Adapter)	(Switch)		(Switch)
1 IRD +	———	1 OTD +	1 IRD +		1 IRD +
2 IRD -	———	2 OTD -	2 IRD -		2 IRD -
3 OTD +	———	3 IRD +	3 OTD +		3 OTD +
6 OTD -	———	6 IRD -	6 OTD -		6 OTD -

Power Adaptor Specifications (ZyWALL 10/10W/30W/50)

Chart 11 North American AC Power Adaptor Specifications

AC Power Adapter model AD48-1201200DUY
Input power: AC120Volts/60Hz/0.25A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: North American standards
Safety standards: UL, CUL (UL 1950, CSA C22.2 No.234-M90)
AC Power Adapter model AD48-1201200DUY
Input power: AC120Volts/60Hz
Output power: DC12Volts/1.2A
Power consumption: 9 W
Plug: North American standards
Safety standards: UL, CUL (UL1950, CSA C22.2 NO. 234-M90)

Chart -12 European Union AC Power Adaptor Specifications

AC Power Adapter model AD-1201200DV
Input power: AC230Volts/50Hz/0.2A

Chart -12 European Union AC Power Adaptor Specifications

Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: European Union standards
Safety standards: TUV, CE (EN 60950)
AC Power Adapter model JAD-121200E
Input power: AC230Volts/50Hz,
Output power: DC12Volts/1.2A
Power consumption: 9 W
Plug: European Union standards
Safety standards: TUV, CE (EN 60950)

Chart 13 UK AC Power Adaptor Specifications

AC Power Adapter model AD-1201200DK
Input power: AC230Volts/50Hz/0.2A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: United Kingdom standards
Safety standards: TUV, CE (EN 60950, BS7002)

Chart 14 Japan AC Power Adaptor Specifications

AC Power Adapter model JOD-48-1124
Input power: AC100Volts/ 50/60Hz/ 27VA
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: Japan standards
Safety standards: T-Mark

Chart 15 Australia and New Zealand AC Power Adaptor Specifications

AC Power Adapter model AD-1201200Ds or AD-121200DS
Input power: AC240Volts/50Hz/0.2A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: Australia and New Zealand standards
Safety standards: NATA (AS 3260)

Appendix C
Safety Warnings and Instructions

1. Be sure to read and follow all warning notices and instructions.
2. The maximum recommended ambient temperature for the ZyWALL is 40º Celsius (104º Fahrenheit). Care must be taken to allow sufficient air circulation or space between units when the ZyWALL is installed inside a closed rack assembly. The operating ambient temperature of the rack environment might be greater than room temperature.
3. Installation in a rack without sufficient airflow can be unsafe.
4. Racks should safely support the combined weight of all equipment.
5. The connections and equipment that supply power to the ZyWALL should be capable of operating safely with the maximum power requirements of the ZyWALL. In case of a power overload, the supply circuits and supply wiring should not become hazardous. The input rating of the ZyWALL is printed on the nameplate.
6. The power cord or power adaptor must plug in to the right supply voltage, i.e. 110VAC for North America and 230VAC for Europe. Make sure that the supplied AC voltage is correct and stable.
7. Installation in restricted access areas must comply with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
8. Do not allow anything to rest on the power cord and do not locate the product where anyone can walk on the power cord.
9. Do not service the product by yourself. Opening or removing covers can expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.
10. Generally, when installed after the final configuration, the product must comply with the applicable safety standards and regulatory requirements of the country in which it is installed. If necessary, consult the appropriate regulatory agencies and inspection authorities to ensure compliance.
11. A rare condition can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate building are interconnected, the voltage potential can cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action before interconnecting the products.

Appendix D
Removing and Installing a ZyWALL 100 Fuse

This appendix shows you how to remove and install fuses for the ZYWALL 100.

The ZYWALL 100 uses a 0.5 Amp, 250 VAC fuse. The ZYWALL-100 comes from the factory; with two fuses installed in the fuse housing. If you need to install a new fuse, follow the procedure below.

Removing a Fuse

Disconnect all power from the ZYWALL 100 before you begin this procedure.

Step 1. Place the rear panel of the ZYWALL 100 in front of you.

Step 2. Remove the power cord from the back of the unit.

Step 3. The fuse housing is located between the power switch and the power port. Use a small flat-head screwdriver to carefully pry out the fuse housing.

Step 4. A burnt-out fuse is blackened, darkened or cloudy inside its glass casing. A working fuse has a completely clear glass casing. Pull gently, but firmly, to remove the burnt out fuse from the fuse housing. Dispose of the burnt-out fuse.

Installing a Fuse

Step 1. The ZyWALL 100 is shipped from the factory with one spare fuse included in a box-like section of the fuse housing. Push the middle part of the box-like section to access the spare fuse. Put another spare fuse in its place in order to always have one on hand.

Step 2. Push the replacement fuse into the fuse housing until you hear a click.

Step 3. Firmly, but gently, push the fuse housing back into the ZYWALL 100 until you hear a click.

Step 4. Plug the power cord back into the unit.

Index

1

10/100 Mbps Ethernet WAN 1-2

A

Access Point..... 6-5, 24-7
Action for Matched Packets..... 12-10
Active..... 23-7, 23-9, 27-3
Address Assignment 3-8, 3-9
Allocated Budget 23-8, 27-6
Application-level Firewalls..... 11-1
Applications 1-8
AT command 23-3, 23-4, 34-2
Attack Alert..... 12-20, 12-21, 12-22
Attack Types 11-6
Authen..... 23-7, 27-6
Authentication..... 23-7, 27-5, 27-6
Authentication Protocol 27-5
Auto-crossover 10/100 Mbps Ethernet LAN ... 1-2
Auto-negotiating 10/100 Mbps Ethernet DMZ 1-2
Auto-negotiating 10/100 Mbps Ethernet LAN. 1-2
Auxiliary 1-2

B

Backup 20-9, 34-2
Backup WAN..... 1-2
Bandwidth Borrowing..... 18-8
Bandwidth Class 18-1
Bandwidth Filter 18-2, 18-15
Bandwidth Management 1-3, 18-1
Bandwidth Management Statistics..... 18-16
Bandwidth Manager Class Configuration.... 18-14
Bandwidth Manager Class Setup 18-12
Bandwidth Manager Monitor..... 18-18
Bandwidth Manager Summary 18-10
Blocking Time 12-21, 12-24
Borrow Bandwidth from Parent Class 18-15
Broadband Access Security Gateway xxix
Brute-force Attack, ... 11-6
Budget Management..... 35-4
BW Budget 18-15
Bypass Triangle Route..... 12-6

C

Cable Modem .....C, 11-2
Call Back Delay..... 23-6
Call Control 35-3
Call History..... 35-5
Call Scheduling..... 1-4, 38-1
  Max Number of Schedule Sets 38-1
  PPPoE 38-3
  Precedence 38-1

Call-Trigerring Packet 33-10
Canada iv
Caution iv
Certifications iii
Changing the Password 21-7
Channel ID 6-5, 24-7
CHAP 23-7, 27-6
Class Name 18-15
Command Interpreter Mode 35-1
Command Line 34-3
Community 32-1
Configuration 5-1, 20-4
Configuration File
  Backup 34-2
  Maintenance 34-1
Connection ID/Name 27-7
Console Port ..... F, 33-3, 33-4, 33-5
  Configuration File Upload 34-17
  File Backup 34-7
  File Upload 34-16
  Restoring Files 34-10
Console/Dial Backup Port Pin Assignments ..... F
Content Filtering 1-3, 13-1
  Categories 13-1
  Customizing 13-11
  Days and Times 13-1
  Exempt Computers 13-9
  Filter List 13-1
  Keywords 13-14
  Restrict Web Features 13-1
  Update List 13-8
Copyright ii
Custom Ports
  Creating/Editing 12-11
Customer Support vi

D

DDNS
  Configuration 22-2
DDNS Type 22-3
Default 20-9
Default Policy Log 12-7
DeMilitarized Zone 7-1
Denial of Service ... 11-2, 11-3, 12-20, 12-21, 30-2
Denial of Services
  Thresholds 12-22
Destination Address 12-4, 12-10
DHCP 3-1, 3-9, 4-2, 5-1, 5-4, 20-4, 24-3
DHCP (Dynamic Host Configuration Protocol) . 1-5
DHCP Ethernet Setup 24-2
Diagnostic 33-11
DIAL BACKUP ..... F
Dial Timeout 23-5
Disclaimer ii
DMZ 7-1

And the Firewall 7-1
IP Alias 25-3
IP Alias Setup ..... See IP Alias Setup
Port Filter Setup 25-1
Setup 25-1, 25-2
TCP/IP Setup ..... See TCP/IP
DMZ Setup 7-1, 25-1
DNS 16-11
Primary Server 5-4, 24-3
Secondary Server 5-4, 24-3
Domain Name 3-1, 3-9, 9-7, 33-3, 33-5
DoS
Basics 11-3
Types 11-4
DoS (Denial of Service) 1-3
Drop Timeout 23-6
DSL Modem ..... C, 1-8, 27-4
DTR 8-21, 23-5
Dynamic DNS 4-2, 22-2
Dynamic DNS Support 1-4
DYNDNS Wildcard 4-2

E

e.g. ..... See Syntax Conventions
EAP 6-3
ECHO 9-7
Edit IP 23-7, 27-4
EMAIL 22-3
E-mail Address 22-3
Enable Wildcard 22-3
Enable Wireless LAN 6-5
Encapsulation 26-2, 27-3, 27-7
Enter ..... See Syntax Conventions
Entering Information 21-2
ESS ID 6-1
ESSID 24-7
Ethernet 3-2, 3-6
Ethernet Cable Pin Assignments ..... G
Ethernet Encapsulation . 9-7, 26-1, 27-2, 27-3, 27-7, 27-11
Ethernet Specification for DMZ ..... E
Ethernet Specification for WAN ..... E
Extended Service Set IDentification 6-5, 24-7

F

Factory Default 23-2
Factory LAN Defaults 5-1
Fail Tolerance 27-14
Fairness-based Scheduler 18-5
FCC iii
Filename Conventions 34-1
Filter 23-15, 24-1, 25-1, 27-10, 31-1
Applying 31-16
Configuration 31-1
Configuring 31-4
DMZ 31-17
Example 31-13

Generic Filter Rule 31-11
Generic Rule 31-11
NAT 31-15
Remote Node 31-18
Structure 31-2
TCP/IP Rule 31-7
Filters
Executing a Filter Rule 31-2
IP Filter Logic Flow 31-9
Finger 9-7
Firewall 1-3
Access Methods 12-1
Activating 30-2
Address Type 12-11
Alerts 12-19
Connection Direction 12-4
Creating/Editing Rules 12-8
Custom Ports ..... See Custom Ports
Enabling 12-1
Firewall Vs Filters 11-12
Guidelines For Enhancing Security 11-11
Introduction 11-2
LAN to WAN Rules 12-4
Policies 12-1
Rule Checklist 12-2
Rule Logic 12-2
Rule Security Ramifications 12-3
Services 12-17
SMT Menus 30-1
Types 11-1
When To Use 11-12
Firmware File
Maintenance 20-5, 20-7, 34-1
Flow Control 21-1
Fragmentation Threshold 6-3
FTP 4-2, 5-1, 9-6, 9-7, 16-1, 16-4, 34-3, 36-3
File Upload 34-13
GUI-based Clients 34-4
Restoring Files 34-8
FTP File Transfer 34-12
FTP Restrictions 16-1, 34-5, 36-3
FTP Server 1-6, 29-14
Full Network Management 1-6
Fuse
Rating ..... E
Replacement ..... K
Type ..... K

G

Gateway IP Addr 27-9
Gateway IP Address 26-2, 28-2
General Setup 3-1, 4-1, 22-1
General Specifications ..... E
Global 9-1

H

Half-Open Sessions 12-20
Hidden Menus 21-2
Host 4-5, 22-3
HTTP 9-7, 11-1, 11-3, 11-4, 39-9, 39-10
HyperTerminal 34-17, 34-18
HyperTerminal program 34-7, 34-10

I

i.e. ..... See Syntax Conventions
ICMP echo 11-6
Idle Timeout 23-8, 27-5, 27-6
IEEE 802.11b 1-3
IEEE 802.1x 1-3
IGMP 5-2
Incoming Protocol Filters 24-6
Industry Canada iv
Initial Screen 21-1
Inside 9-1
Inside Global Address 9-1
Inside Local Address 9-1
Installing Fuses ..... K
Interactive Applications 37-2
Internet Access 26-1
  ISP's Name 26-1
Internet Access Setup ..... C, 26-1, 29-2
Internet Control Message Protocol (ICMP) ... 11-6
Internet Security Gateway 1-1
Introduction to Filters 31-1
IP address 23-7, 23-10
IP Address 3-8, 3-9, 5-2, 5-4, 9-6, 9-8, 20-4, 24-4, 24-5, 26-2, 27-8, 37-3
  Remote 23-10
IP Address Assignment 27-8
IP Address Assignment 26-2
IP Alias 1-5, 24-5
IP Alias Setup 24-5
IP Multicast 1-5
  Internet Group Management Protocol (IGMP) 1-5
IP Policies 24-4, 37-6
IP Policy Routing 1-5
IP Policy Routing (IPPR)
  Applying an IP Policy 37-6
  Ethernet IP Policies 37-6
  Gateway 37-5
IP Pool 5-4, 24-3
IP Pool Setup 5-1
IP Ports 11-4, 39-9, 39-10
IP Protocol 37-5
IP Routing Policy 37-4
IP Routing Policy (IPPR) 37-1
  Benefits 37-1
  Cost Savings 37-1
  Criteria 37-1
  Load Sharing 37-1

Setup 37-2
IP Spoofing 11-4, 11-7
IP Static Route 28-1, 28-2
Active 28-2
Destination IP Address 28-2
IP Subnet Mask 28-2
Name 28-2
Route Number 28-2
IP Subnet Mask 23-10, 24-5
Remote 23-10
IPSec standard 1-3
IPSec VPN Capability 1-3
ISP's Name 26-1

K

Key Fields For Configuring Rules 12-3

L

LAN IP Address 19-7, 19-11
LAN Port Filter Setup 24-1
LAN Setup 5-1, 8-1, 24-1, 24-2
LAN TCP/IP 5-1
LAN to WAN Rules 12-4
LAND 11-4, 11-6
Local 9-1
Log 33-6
Log Facility 33-8
Logging 1-6
Login Name ..... See My Login Name
Login Screen ..... See Password
Logs 19-1

M

MAC Address 23-2
MAC Address Filter Action 6-7
MAC Address Filtering 6-6
MAC service data unit 6-5, 24-7
Main Menu 21-3
Main Menu Commands 21-2
Management Information Base (MIB) 16-8
Many to Many No Overload ..... See NAT
Many to Many Overload ..... See NAT
Many to One ..... See NAT
Maximize Bandwidth Usage 18-5, 18-12
Maximum Incomplete High 12-23
Maximum Incomplete Low 12-23
Max-incomplete High 12-20
Max-incomplete Low 12-20, 12-23
Mean Time Between Failures ..... E
Metric 8-1, 10-3, 23-11, 27-6, 27-9, 28-2
MSDU 6-5, 24-7
MTBF ..... See Mean Time Between Failures
Multicast 5-2, 5-5, 23-11, 24-4, 27-10
My IP Addr 27-7
My Login 23-7, 27-3
My Login Name 26-2
My Password 23-7, 26-2, 27-4

My Server IP Addr 27-7
My WAN Address 23-10

N

Nailed-up Connection 27-5
Nailed-Up Connection 23-8, 27-6
Nailed-Up Connections 27-8
NAT . 3-6, 3-9, 9-6, 9-7, 9-8, 9-9, 23-11, 27-9, 31-15
  Application 9-3
  Applying NAT in the SMT Menus 29-1
  Configuring 29-4
  Definitions 9-1
  Examples 29-11
  How NAT Works 9-2
  Mapping Types 9-4
  NAT Unfriendly Application Programs ... 29-17
  Ordering Rules 29-7
  Server Sets 9-6
  What NAT does 9-2
NAT Traversal 17-1, 17-2, 17-3
NetBIOS commands 11-7
Network Address Translation 26-3
Network Address Translation (NAT) 1-5, 29-1
Network Management 9-7
NNTP 9-7
Notice iii

O

Offline 22-3
One Minute High 12-23
One Minute Low 12-22
One to One ..... See NAT
One-Minute High 12-21
Online Registration v
Operation Temperature ..... E
Outgoing Protocol Filters 24-6
Outside 9-1

P

Packet Filtering 1-4, 11-12
Packet Filtering Firewalls 11-1
Packing List Card xxix
PAP 23-7, 27-6
Password ..... 4-4, 21-1, 21-2, 21-7, 32-1. See My Password
PCMCIA Port 1-3
Period(hr) 23-8, 27-6
Ping 33-13
Ping of Death 11-4
Point-to-Point Tunneling Protocol .... 3-4, 9-7. See PPTP
Policy-based Routing 37-1
POP3 ..... 9-7, 11-3, 11-4
Port Configuration 12-12
Port Forwarding 1-5
Port Numbers 9-7
Power Adaptor Specifications ..... G
Power Consumption ..... E

Power Current ..... E
Power Specification ..... E
PPP 23-8
PPPoE 1-4, 3-2, 3-6
PPPoE Encapsulation 26-1, 26-5, 27-2, 27-4, 27-5, 27-6, 27-11
PPTP 3-2, 3-4, 3-5, 3-6, 9-7
  Client 26-3, 26-4
  Configuring a Client 26-3, 26-4
PPTP Encapsulation 1-4, 3-4, 27-6
Precedence 37-2, 37-5
Priority 18-15
Priority-based Scheduler 18-5
Private 10-3, 23-11, 27-9, 28-3
Private IP Address 3-8
Proportional Bandwidth Allocation 18-2
Protocol Filters 24-6
  Incoming 24-6
  Outgoing 24-6
Protocol/Port 19-7, 19-10
Public Servers 7-1

Q

Quality of Service 37-1
Quick Start Guide 2-1

R

RADIUS 1-3, 6-8
  Shared Secret Key 6-9
RADIUS Message Types 6-8
RAS 37-2
Read Me First xxix
Real Time Chip 1-2
Related Documentation xxix
Relay 24-3
Rem IP Address 23-10
Rem Node Name 23-6, 23-9, 27-3
Remote Authentication Dial In User Service .. See RADIUS
Remote Management 36-1
Remote Management and NAT 16-2
Remote Management Limitations 16-1, 36-3
Remote Node 27-1
  Profile (Traffic Redirect Field) 27-12
Remote Node Filter 23-14, 27-10
Removing and Installing Fuses ..... K
Repairs v
Replacement v
Reports 19-6
Required fields 21-2
Reset Button 1-2
Resetting the Time 35-8
Restore 20-9
Restore Configuration 34-8
retry count 23-5
retry interval 23-5
Return Material Authorization Number v
RIP 5-2, 23-11, 24-4, 24-5, 27-10

Direction 24-5
Version 24-5, 27-10
RoadRunner Support 1-6
Root Class 18-12
Route 27-4
Routing Policy 37-1
RTC ..... See Real Time Chip. See Real Time Chip
RTS Threshold 6-1
RTS/CTS handshake 6-5, 24-7
Rule Summary 12-16
Rules 12-1, 12-5
Checklist 12-2
Creating Custom 12-1
Key Fields 12-3
LAN to WAN 12-4
Logic 12-2
Predefined Services 12-17
Source and Destination Addresses 12-10

S

SA Monitor 40-1
Safety Instructions ..... J
Saving the State 11-7
Schedule Sets
Duration 38-2
Scheduler 18-4, 18-12
Schedules 27-6, 27-7
Security Association 40-1
Security Ramifications 12-3
Select ..... See Syntax Conventions
Server 4-6, 9-5, 26-2, 27-4, 29-4, 29-6, 29-8, 29-9, 29-10, 29-12, 29-13, 35-7
Server IP 27-4
Service ..... v, 12-3
Service Name 27-3
Service Set 6-5, 24-7
Service Type ..... C, 12-12, 26-2, 27-3
Services 9-6, 9-7
Set Up a Schedule 38-2
SMT ..... 21-2. See System Management Terminal
SMT Menus at a Glance 21-5
SMTP 9-7
Smurf 11-6
SNMP 9-7, 16-7
Community 32-1
Configuration 32-1
Get 16-8
Manager 16-8
MIBs 16-8
Trap 16-8
Trusted Host 32-1
SNMP (Simple Network Management Protocol) 1-5
Source & Destination Addresses 12-10
Source Address 12-3, 12-10
Source-Based Routing 37-1

Stateful Inspection 1-3, 11-1, 11-2, 11-7, 11-8
Process 11-8
ZyWALL 11-9
Static Route..... 10-1
SUA 9-6, 9-7, 9-9
SUA (Single User Account) .. See NAT. See NAT
Sub-class Layers 18-12
Subnet Mask3-9, 5-2, 5-4, 12-11, 23-10, 24-4, 26-2, 27-9, 28-2
Support Disk xxix
SYN Flood..... 11-4, 11-5
SYN-ACK 11-5
Syntax Conventions xxx
Syslog 12-12
Syslog IP Address..... 33-8
System Information 33-1, 33-3, 33-4
System Maintenance 19-3, 33-1, 33-2, 33-4, 33-5, 33-6, 33-7, 33-8, 33-11, 33-12, 33-13, 34-2, 34-5, 34-14, 34-16, 35-1, 35-3, 35-4, 35-5, 35-7
System Management Terminal 21-2
System Name 4-1, 22-1
System Status..... 33-1
System Timeout 16-2

T

TCP Maximum Incomplete ... 12-21, 12-23, 12-24
TCP Security..... 11-10
TCP/IP ...5-4, 11-3, 11-4, 16-3, 23-10, 24-2, 24-4, 25-2, 27-8, 31-6, 31-7, 31-9, 31-12, 31-15
Setup.....24-4
TCP/IP and DHCP Setup.....24-2
TCP/IP filter rule 31-6
Teardrop 11-4
Telnet.....16-2
Telnet Configuration 16-3
Terminal Emulation.....21-1
TFTP.....34-5
File Upload.....34-14
GUI-based Clients 34-6
TFTP and FTP over WAN 34-5
TFTP and FTP over WAN Will Not Work When…. 34-5
TFTP and FTP Over WAN} 16-1, 36-3
TFTP Restrictions..... 16-1, 34-5, 36-3
Three-Way Handshake 11-5
Threshold Values.....12-20
Time and Date 1-2
Time and Date Setting 35-6, 35-7
Time Zone 4-5, 35-8
Timeout 23-8, 26-4, 26-5, 27-6
ToS (Type of Service) 37-1, 37-2
Trace.....33-6
Traceroute.....11-7
Tracing 1-6
Trademarks.....ii
Traffic Redirect 1-5, 8-14
Setup.....27-12

Trigger Port Forwarding 29-18
Process 29-19
Process Example 29-19
Trivial File Transfer Protocol..... See TFTP
Troubleshooting .....A
Internet Access.....C
LAN Interface .....B
WAN Interface.....C
Trusted Network .....See LAN
Type of Service 37-1, 37-4, 37-5

U

UDP/ICMP Security 11-10
Universal Plug and Play..... 1-4
Universal Plug and Play (UPnP)..... 17-1, 17-3
UNIX Syslog.....33-7, 33-8
Upload Firmware 34-11
UPnP 1-4
UPnP Examples 17-4
Upper Layer Protocols 11-10, 11-11
Use Server Detected IP 22-4
User Name 4-3, 22-3
User Profiles..... 6-10
User Specified IP Addr 22-4

V

Virtual Private Network 1-3
VPN 8-6
VPN Application..... 1-9
VT100..... 21-1

W

WAN DHCP 33-12, 33-13
WAN Setup..... 3-9, 23-1
WAN to LAN Rules 12-5
Warranty v
Web..... 16-5
Web Configurator 2-1, 2-3, 11-2, 11-11, 12-3, 30-2
Web Site Hits..... 19-7, 19-8
WEP Encryption 6-5
Wireless LAN 1-3
Wireless LAN MAC Address Filtering 1-4
Wireless LAN Setup 24-6
Wizard Setup 3-1, 3-2, 3-8
www.dyndns.org..... 22-3
www.zyxel.com v

X

Xmodem
File Upload 34-17
XMODEM Protocol..... 34-3

Z

ZyNOS.....33-3, 33-5, 34-2
ZyNOS F/W Version 33-3, 33-5, 34-2
ZyWALL Firewall Application 11-3
ZyXEL Limited Warranty
Note v
ZyXEL website.....v

ZyXEL's Firewall Introduction 11-2