ZyWALL/ USG Series

USG20-VPN / USG20W-VPN

VPN Firewalls

Version 4.16
Edition 1, 1/2016

User's Guide

Default Login Details	
LAN Port IP Address	https://192.168.1.1
User Name	admin
Password	1234

Copyright © 2016 ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the ZyWALL/USG and access the Web Configurator wizards. (See the wizard real time help for information on configuring each screen.) It also contains a connection diagram and package contents list.

- CLI Reference Guide

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

Note: It is recommended you use the Web Configurator to configure the ZyWALL/USG.

- Web Configurator Online Help

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

- More Information

  Go to support.zyxel.com to find other information on ZyWALL/USG.



Part I: User's Guide 17

Chapter 1
Introduction 19

1.1 Overview 19
1.1.1 Applications 19
1.2 Management Overview 21
1.3 Web Configurator 23
1.3.1 Web Configurator Access 23
1.3.2 Web Configurator Screens Overview 25
1.3.3 Navigation Panel 29
1.3.4 Tables and Lists 34

Chapter 2
Installation Setup Wizard 37

2.1 Installation Setup Wizard Screens 37
2.1.1 Internet Access Setup - WAN Interface 37
2.1.2 Internet Access: Ethernet 38
2.1.3 Internet Access: PPPoE 39
2.1.4 Internet Access: PPTP 41
2.1.5 Internet Access Setup - Second WAN Interface 42
2.1.6 Internet Access Succeed 43
2.1.7 Wireless Settings: SSID & Security 43
2.1.8 Internet Access - Device Registration 44

Chapter 3
Hardware, Interfaces and Zones 45

3.1 Hardware Overview 45
3.1.1 Front Panels 45
3.1.2 Rear Panels 46
3.1.3 Wall-mounting 47
3.2 Default Zones, Interfaces, and Ports 48
3.3 Stopping the USG 49

Chapter 4
Quick Setup Wizards 50

4.1 Quick Setup Overview 50
4.2 WAN Interface Quick Setup 51
4.2.1 Choose an Ethernet Interface 51
4.2.2 Select WAN Type 52
4.2.3 Configure WAN IP Settings 52
4.2.4 ISP and WAN and ISP Connection Settings 53
4.2.5 Quick Setup Interface Wizard: Summary 55

4.3 VPN Setup Wizard 56
4.3.1 Welcome 57
4.3.2 VPN Setup Wizard: Wizard Type 58
4.3.3 VPN Express Wizard - Scenario 58
4.3.4 VPN Express Wizard - Configuration 60
4.3.5 VPN Express Wizard - Summary 60
4.3.6 VPN Express Wizard - Finish 61
4.3.7 VPN Advanced Wizard - Scenario 62
4.3.8 VPN Advanced Wizard - Phase 1 Settings 63
4.3.9 VPN Advanced Wizard - Phase 2 65
4.3.10 VPN Advanced Wizard - Summary 66
4.3.11 VPN Advanced Wizard - Finish 66
4.4 VPN Settings for Configuration Provisioning Wizard: Wizard Type 67
4.4.1 Configuration Provisioning Express Wizard - VPN Settings 68
4.4.2 Configuration Provisioning VPN Express Wizard - Configuration 69
4.4.3 VPN Settings for Configuration Provisioning Express Wizard - Summary 70
4.4.4 VPN Settings for Configuration Provisioning Express Wizard - Finish 71
4.4.5 VPN Settings for Configuration Provisioning Advanced Wizard - Scenario 72
4.4.6 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 1 Settings 73
4.4.7 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 2 75
4.4.8 VPN Settings for Configuration Provisioning Advanced Wizard - Summary 75
4.4.9 VPN Settings for Configuration Provisioning Advanced Wizard- Finish 77
4.5 VPN Settings for L2TP VPN Settings Wizard 78
4.5.1 L2TP VPN Settings 79
4.5.2 L2TP VPN Settings 80
4.5.3 VPN Settings for L2TP VPN Setting Wizard - Summary 81
4.5.4 VPN Settings for L2TP VPN Setting Wizard Completed 82

Chapter 5
Dashboard 83

5.1 Overview 83
5.1.1 What You Can Do in this Chapter 83
5.2 Main Dashboard Screen 83
5.2.1 Device Information Screen 85
5.2.2 System Status Screen 86
5.2.3 VPN Status Screen 87
5.2.4 DHCP Table Screen 88
5.2.5 Number of Login Users Screen 89
5.2.6 System Resources Screen 90
5.2.7 CPU Usage Screen 91
5.2.8 Memory Usage Screen 92
5.2.9 Active Session Screen 93
5.2.10 Extension Slot Screen 94

5.2.11 Interface Status Summary Screen 94
5.2.12 Secured Service Status Screen 95
5.2.13 Content Filter Statistics Screen 96
5.2.14 Top 5 IPv4/IPv6 Security Policy Rules that Blocked Traffic Screen 97
5.2.15 The Latest Alert Logs Screen 97

Part II: Technical Reference 99

Chapter 6
Monitor 101

6.1 Overview 101
6.1.1 What You Can Do in this Chapter 101
6.2 The Port Statistics Screen 102
6.2.1 The Port Statistics Graph Screen 103
6.3 Interface Status Screen 104
6.4 The Traffic Statistics Screen 106
6.5 The Session Monitor Screen 109
6.6 IGMP Statistics 110
6.7 The DDNS Status Screen 111
6.8 IP/MAC Binding 112
6.9 The Login Users Screen 112
6.10 Cellular Status Screen 113
6.11 The UPnP Port Status Screen 115
6.12 USB Storage Screen 116
6.13 Ethernet Neighbor Screen 117
6.14 Wireless 118
6.14.1 Wireless AP Information: Radio List 118
6.14.2 Radio List More Information 120
6.14.3 Wireless Station Info 121
6.14.4 Detected Device 122
6.15 The IPSec Monitor Screen 123
6.15.1 Regular Expressions in Searching IPSec SAs 124
6.16 The SSL Screen 124
6.17 The L2TP over IPSec Session Monitor Screen 125
6.18 The Content Filter Screen 126
6.19 The Anti-Spam Screens 128
6.19.1 Anti-Spam Report 128
6.19.2 The Anti-Spam Status Screen 130
6.20 Log Screens 131
6.20.1 View Log 131

Chapter 7 Licensing 134

7.1 Registration Overview 134
7.1.1 What you Need to Know 134
7.1.2 Registration Screen 135
7.1.3 Service Screen 135

Chapter 8 Wireless 137

8.1 Overview 137
8.1.1 What You Can Do in this Chapter 137
8.1.2 What You Need to Know 137
8.2 AP Management Screen 138
8.3 DCS Screen 139
8.4 Technical Reference 139
8.4.1 Dynamic Channel Selection 139

Chapter 9 Interfaces 141

9.1 Interface Overview 141
9.1.1 What You Can Do in this Chapter 141
9.1.2 What You Need to Know 142
9.1.3 What You Need to Do First 146
9.2 Port Role Screen 146
9.3 Ethernet Summary Screen 147
9.3.1 Ethernet Edit 149
9.3.2 Object References 164
9.3.3 Add/Edit DHCPv6 Request/Release Options 165
9.3.4 Add/Edit DHCP Extended Options 166
9.4 PPP Interfaces 167
9.4.1 PPP Interface Summary 168
9.4.2 PPP Interface Add or Edit 169
9.5 Cellular Configuration Screen 174
9.5.1 Cellular Choose Slot 177
9.5.2 Add / Edit Cellular Configuration 177
9.6 Tunnel Interfaces 183
9.6.1 Configuring a Tunnel 185
9.6.2 Tunnel Add or Edit Screen 186
9.7 VLAN Interfaces 189
9.7.1 VLAN Summary Screen 191
9.7.2 VLAN Add/Edit 193
9.8 Bridge Interfaces 202
9.8.1 Bridge Summary 204

9.8.2 Bridge Add/Edit 205
9.9 Virtual Interfaces 214
9.9.1 Virtual Interfaces Add/Edit 214
9.10 Interface Technical Reference 216
9.11 Trunk Overview 219
9.11.1 What You Need to Know 219
9.12 The Trunk Summary Screen 222
9.12.1 Configuring a User-Defined Trunk 223
9.12.2 Configuring the System Default Trunk 225

Chapter 10
Routing 227

10.1 Policy and Static Routes Overview 227
10.1.1 What You Can Do in this Chapter 227
10.1.2 What You Need to Know 228
10.2 Policy Route Screen 229
10.2.1 Policy Route Edit Screen 231
10.3 IP Static Route Screen 236
10.3.1 Static Route Add/Edit Screen 236
10.4 Policy Routing Technical Reference 238
10.5 Routing Protocols Overview 239
10.5.1 What You Need to Know 239
10.6 The RIP Screen 239
10.7 The OSPF Screen 241
10.7.1 Configuring the OSPF Screen 244
10.7.2 OSPF Area Add/Edit Screen 245
10.7.3 Virtual Link Add/Edit Screen 247
10.8 Routing Protocol Technical Reference 248

Chapter 11
DDNS 250

11.1 DDNS Overview 250
11.1.1 What You Can Do in this Chapter 250
11.1.2 What You Need to Know 250
11.2 The DDNS Screen 251
11.2.1 The Dynamic DNS Add/Edit Screen 252

Chapter 12
NAT 256

12.1 NAT Overview 256
12.1.1 What You Can Do in this Chapter 256
12.1.2 What You Need to Know 256
12.2 The NAT Screen 256

12.2.1 The NAT Add/Edit Screen 258
12.3 NAT Technical Reference 261

Chapter 13
HTTP Redirect 263

13.1 Overview 263
13.1.1 What You Can Do in this Chapter 263
13.1.2 What You Need to Know 263
13.2 The HTTP Redirect Screen 264
13.2.1 The HTTP Redirect Edit Screen 265

Chapter 14
ALG 267

14.1 ALG Overview 267
14.1.1 What You Need to Know 267
14.1.2 Before You Begin 270
14.2 The ALG Screen 270
14.3 ALG Technical Reference 272

Chapter 15
UPnP 274

15.1 UPnP and NAT-PMP Overview 274
15.2 What You Need to Know 274
15.2.1 NAT Traversal 274
15.2.2 Cautions with UPnP and NAT-PMP 275
15.3 UPnP Screen 275
15.4 Technical Reference 276
15.4.1 Turning on UPnP in Windows 7 Example 276
15.4.2 Using UPnP in Windows XP Example 278
15.4.3 Web Configurator Easy Access 280

Chapter 16
IP/MAC Binding 283

16.1 IP/MAC Binding Overview 283
16.1.1 What You Can Do in this Chapter 283
16.1.2 What You Need to Know 283
16.2 IP/MAC Binding Summary 284
16.2.1 IP/MAC Binding Edit 284
16.2.2 Static DHCP Edit 285
16.3 IP/MAC Binding Exempt List 286

Chapter 17
Layer 2 Isolation 288

17.1 Overview 288
17.1.1 What You Can Do in this Chapter 288
17.2 Layer-2 Isolation General Screen 289
17.3 White List Screen 289
17.3.1 Add/Edit White List Rule 290

Chapter 18
Inbound Load Balancing 292

18.1 Inbound Load Balancing Overview 292
18.1.1 What You Can Do in this Chapter 292
18.2 The Inbound LB Screen 293
18.2.1 The Inbound LB Add/Edit Screen 294
18.2.2 The Inbound LB Member Add/Edit Screen 296

Chapter 19
Web Authentication 298

19.1 Web Auth Overview 298
19.1.1 What You Can Do in this Chapter 298
19.1.2 What You Need to Know 299
19.2 Web Authentication Screen 299
19.2.1 Creating Exceptional Services 302
19.2.2 Creating/Editing an Authentication Policy 302
19.3 SSO Overview 303
19.4 SSO - USG Configuration 305
19.4.1 Configuration Overview 305
19.4.2 Configure the USG to Communicate with SSO 305
19.4.3 Enable Web Authentication 306
19.4.4 Create a Security Policy 307
19.4.5 Configure User Information 308
19.4.6 Configure an Authentication Method 309
19.4.7 Configure Active Directory 310
19.5 SSO Agent Configuration 311

Chapter 20
Security Policy 315

20.1 Overview 315
20.2 One Security 315
20.3 What You Can Do in this Chapter 319
20.3.1 What You Need to Know 319
20.4 The Security Policy Screen 321
20.4.1 Configuring the Security Policy Control Screen 322
20.4.2 The Security Policy Control Add/Edit Screen 325
20.5 The Session Control Screen 327

20.5.1 The Session Control Add/Edit Screen 329
20.6 Security Policy Example Applications 330

Chapter 21
IPSec VPN 333

21.1 Virtual Private Networks (VPN) Overview 333
21.1.1 What You Can Do in this Chapter 335
21.1.2 What You Need to Know 336
21.1.3 Before You Begin 337
21.2 The VPN Connection Screen 338
21.2.1 The VPN Connection Add/Edit (IKE) Screen 339
21.3 The VPN Gateway Screen 345
21.3.1 The VPN Gateway Add/Edit Screen 347
21.4 VPN Concentrator 354
21.4.1 VPN Concentrator Requirements and Suggestions 354
21.4.2 VPN Concentrator Screen 355
21.4.3 The VPN Concentrator Add/Edit Screen 355
21.5 USG IPSec VPN Client Configuration Provisioning 356
21.6 IPSec VPN Background Information 358

Chapter 22
SSL VPN 368

22.1 Overview 368
22.1.1 What You Can Do in this Chapter 368
22.1.2 What You Need to Know 368
22.2 The SSL Access Privilege Screen 369
22.2.1 The SSL Access Privilege Policy Add/Edit Screen 370
22.3 The SSL Global Setting Screen 373
22.3.1 How to Upload a Custom Logo 374
22.4 USG SecuExtender 375
22.4.1 Example: Configure USG for SecuExtender 376

Chapter 23
SSL User Screens 379

23.1 Overview 379
23.1.1 What You Need to Know 379
23.2 Remote SSL User Login 380
23.3 The SSL VPN User Screens 383
23.4 Bookmarking the USG 384
23.5 Logging Out of the SSL VPN User Screens 385
23.6 SSL User Application Screen 385
23.7 SSL User File Sharing 386
23.7.1 The Main File Sharing Screen 386

23.7.2 Opening a File or Folder 387
23.7.3 Downloading a File 388
23.7.4 Saving a File 388
23.7.5 Creating a New Folder 389
23.7.6 Renaming a File or Folder 389
23.7.7 Deleting a File or Folder 390
23.7.8 Uploading a File 390

Chapter 24
USG SecuExtender (Windows) 392

24.1 The USG SecuExtender Icon 392
24.2 Status 392
24.3 View Log 393
24.4 Suspend and Resume the Connection 394
24.5 Stop the Connection 394
24.6 Uninstalling the USG SecuExtender 394

Chapter 25
L2TP VPN 396

25.1 Overview 396
25.1.1 What You Can Do in this Chapter 396
25.1.2 What You Need to Know 396
25.2 L2TP VPN Screen 397
25.2.1 Example: L2TP and USG Behind a NAT Router 399

Chapter 26
BWM (Bandwidth Management) 401

26.1 Overview 401
26.1.1 What You Can Do in this Chapter 401
26.1.2 What You Need to Know 401
26.2 The Bandwidth Management Screen 405
26.2.1 The Bandwidth Management Add/Edit Screen 407

Chapter 27
Content Filtering 416

27.1 Overview 416
27.1.1 What You Can Do in this Chapter 416
27.1.2 What You Need to Know 416
27.1.3 Before You Begin 417
27.2 Content Filter Profile Screen 418
27.3 Content Filter Profile Add or Edit Screen 420
27.3.1 Content Filter Add Profile Category Service 421
27.3.2 Content Filter Add Filter Profile Custom Service 428

27.4 Content Filter Trusted Web Sites Screen 431
27.5 Content Filter Forbidden Web Sites Screen 432
27.6 Content Filter Technical Reference 433

Chapter 28
Anti-Spam 435

28.1 Overview 435
28.1.1 What You Can Do in this Chapter 435
28.1.2 What You Need to Know 435
28.2 Before You Begin 436
28.3 The Anti-Spam Profile Screen 437
28.3.1 The Anti-Spam Profile Add or Edit Screen 438
28.4 The Mail Scan Screen 440
28.5 The Anti-Spam Black List Screen 442
28.5.1 The Anti-Spam Black or White List Add/Edit Screen 444
28.5.2 Regular Expressions in Black or White List Entries 445
28.6 The Anti-Spam White List Screen 445
28.7 The DNSBL Screen 447
28.8 Anti-Spam Technical Reference 449

Chapter 29
Object 453

29.1 Zones Overview 453
29.1.1 What You Need to Know 453
29.1.2 The Zone Screen 454
29.2 User/Group Overview 455
29.2.1 What You Need To Know 456
29.2.2 User/Group User Summary Screen 458
29.2.3 User/Group Group Summary Screen 461
29.2.4 User/Group Setting Screen 462
29.2.5 User/Group MAC Address Summary Screen 467
29.2.6 User /Group Technical Reference 468
29.3 AP Profile Overview 469
29.3.1 Radio Screen 470
29.3.2 SSID Screen 476
29.4 MON Profile 485
29.4.1 Overview 485
29.4.2 MON Profile 485
29.5 Address Overview 488
29.5.1 What You Need To Know 488
29.5.2 Address Summary Screen 488
29.6 Service Overview 492
29.6.1 What You Need to Know 493

29.6.2 The Service Summary Screen 493
29.6.3 The Service Group Summary Screen 495
29.7 Schedule Overview 497
29.7.1 What You Need to Know 497
29.7.2 The Schedule Summary Screen 498
29.7.3 The Schedule Group Screen 501
29.8 AAA Server Overview 502
29.8.1 Directory Service (AD/LDAP) 503
29.8.2 RADIUS Server 503
29.8.3 ASAS 503
29.8.4 What You Need To Know 504
29.8.5 Active Directory or LDAP Server Summary 505
29.8.6 RADIUS Server Summary 509
29.9 Auth. Method Overview 511
29.9.1 Before You Begin 511
29.9.2 Example: Selecting a VPN Authentication Method 511
29.9.3 Authentication Method Objects 512
29.10 Certificate Overview 514
29.10.1 What You Need to Know 514
29.10.2 Verifying a Certificate 516
29.10.3 The My Certificates Screen 517
29.10.4 The Trusted Certificates Screen 524
29.10.5 Certificates Technical Reference 529
29.11 ISP Account Overview 529
29.11.1 ISP Account Summary 529
29.12 SSL Application Overview 532
29.12.1 What You Need to Know 532
29.12.2 The SSL Application Screen 534

Chapter 30 System 538

30.1 Overview 538
30.1.1 What You Can Do in this Chapter 538
30.2 Host Name 539
30.3 USB Storage 539
30.4 Date and Time 540
30.4.1 Pre-defined NTP Time Servers List 543
30.4.2 Time Server Synchronization 543
30.5 Console Port Speed 544
30.6 DNS Overview 545
30.6.1 DNS Server Address Assignment 545
30.6.2 Configuring the DNS Screen 545
30.6.3 Address Record 548

30.6.4 PTR Record 549
30.6.5 Adding an Address/PTR Record 549
30.6.6 CNAME Record 549
30.6.7 Adding a CNAME Record 550
30.6.8 Domain Zone Forwarder 550
30.6.9 Adding a Domain Zone Forwarder 550
30.6.10 MX Record 551
30.6.11 Adding a MX Record 552
30.6.12 Security Option Control 552
30.6.13 Editing a Security Option Control 552
30.6.14 Adding a DNS Service Control Rule 553
30.7 WWW Overview 554
30.7.1 Service Access Limitations 554
30.7.2 System Timeout 555
30.7.3 HTTPS 555
30.7.4 Configuring WWW Service Control 556
30.7.5 Service Control Rules 559
30.7.6 Customizing the WWW Login Page 560
30.7.7 HTTPS Example 563
30.8 SSH 570
30.8.1 How SSH Works 571
30.8.2 SSH Implementation on the USG 572
30.8.3 Requirements for Using SSH 572
30.8.4 Configuring SSH 572
30.8.5 Secure Telnet Using SSH Examples 573
30.9 Telnet 574
30.9.1 Configuring Telnet 574
30.10 FTP 576
30.10.1 Configuring FTP 576
30.11 SNMP 577
30.11.1 SNMPv3 and Security 578
30.11.2 Supported MIBs 578
30.11.3 SNMP Traps 578
30.11.4 Configuring SNMP 579
30.12 Authentication Server 581
30.12.1 Add/Edit Trusted RADIUS Client 582
30.13 CloudCNM Screen 583
30.14 Language Screen 586
30.15 IPv6 Screen 586
30.16 ZyXEL One Network (ZON) Utility 587
30.16.1 ZyXEL One Network (ZON) System Screen 588

Chapter 31
Log and Report 590

31.1 Overview 590
31.1.1 What You Can Do In this Chapter 590
31.2 Email Daily Report 590
31.3 Log Setting Screens 592
31.3.1 Log Settings 593
31.3.2 Edit System Log Settings 594
31.3.3 Edit Log on USB Storage Setting 597
31.3.4 Edit Remote Server Log Settings 599
31.3.5 Log Category Settings Screen 601

Chapter 32
File Manager 605

32.1 Overview 605
32.1.1 What You Can Do in this Chapter 605
32.1.2 What you Need to Know 605
32.2 The Configuration File Screen 607
32.3 The Firmware Package Screen 611
32.4 The Shell Script Screen 613

Chapter 33
Diagnostics 616

33.1 Overview 616
33.1.1 What You Can Do in this Chapter 616
33.2 The Diagnostic Screen 616
33.2.1 The Diagnostics Files Screen 617
33.3 The Packet Capture Screen 618
33.3.1 The Packet Capture Files Screen 621
33.4 The Core Dump Screen 621
33.4.1 The Core Dump Files Screen 622
33.5 The System Log Screen 623
33.6 The Network Tool Screen 623
33.7 The Wireless Frame Capture Screen 624
33.7.1 The Wireless Frame Capture Files Screen 626

Chapter 34
Packet Flow Explore 628

34.1 Overview 628
34.1.1 What You Can Do in this Chapter 628
34.2 The Routing Status Screen 628
34.3 The SNAT Status Screen 633

Chapter 35
Shutdown 636

35.1 Overview 636
35.1.1 What You Need To Know 636
35.2 The Shutdown Screen 636

Chapter 36 Troubleshooting....637

36.1 Resetting the USG 645
36.2 Getting More Troubleshooting Help 646

Appendix A Customer Support 647

Appendix B Legal Information....653

Appendix C Product Features....662

Index 666

PART I
User's Guide

1 Introduction

1.1 Overview

"USG" in this User's Guide refers to all USG models in the series.

Table 1 USG Models

USG20-VPN
USG20W-VPN

USG20W-VPN has built-in Wi-Fi functionality

- See Table 12 on page 48 for default port / interface name mapping. See Table 13 on page 49 for default interface / zone mapping.

See the product's datasheet for detailed information on a specific model.

1.1.1 Applications

These are some USG application scenarios.

Security Router

Security includes a Stateful Packet Inspection (SPI) firewall, Content Filtering (CF) and Anti-Spam (AS).

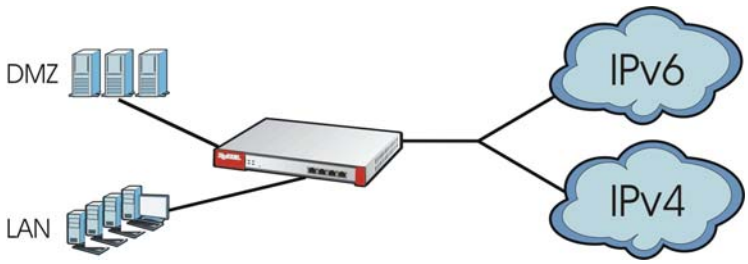
Figure 1 Applications: Security RouterApplications: Security Router



IPv6 Routing

The USG supports IPv6 Ethernet, PPP, VLAN, and bridge routing. You may also create IPv6 policy routes and IPv6 objects. The USG can also route IPv6 packets through IPv4 networks using different tunneling methods.

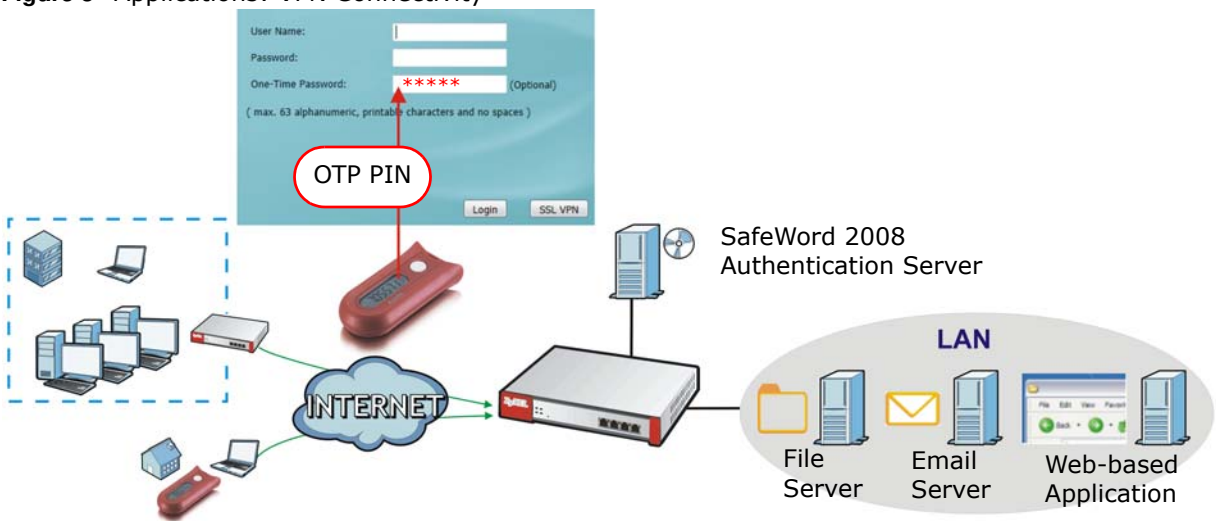
Figure 2 Applications: IPv6 Routing



VPN Connectivity

Set up VPN tunnels with other companies, branch offices, telecommuters, and business travelers to provide secure access to your network. You can also purchase the USG OTPv2 One-Time Password System for strong two-factor authentication for Web Configurator, Web access, SSL VPN, and ZyXEL IPSec VPN client user logins.

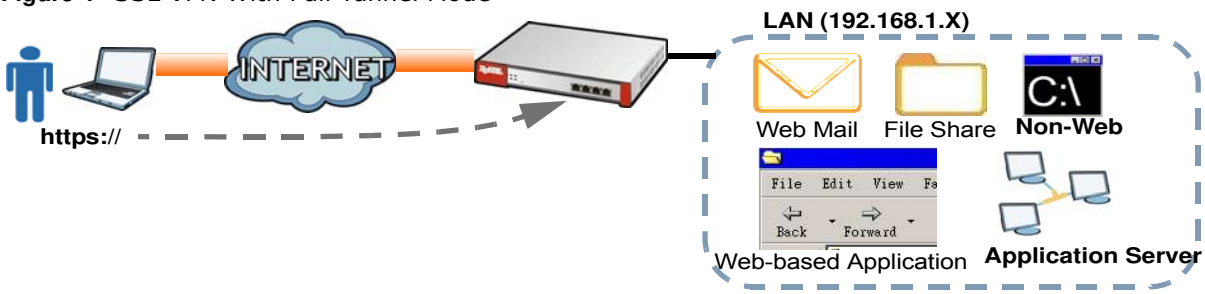
Figure 3 Applications: VPN Connectivity



SSL VPN Network Access

SSL VPN lets remote users use their web browsers for a very easy-to-use VPN solution. A user just browses to the USG's web address and enters his user name and password to securely connect to the USG's network. Here full tunnel mode creates a virtual connection for a remote user and gives him a private IP address in the same subnet as the local network so he can access network resources in the same way as if he were part of the internal network.

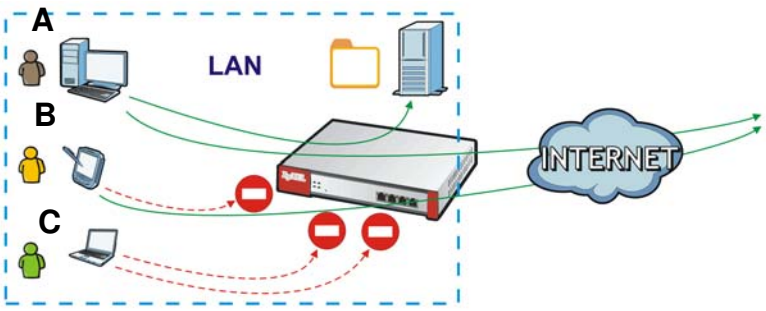
Figure 4 SSL VPN With Full Tunnel Mode



User-Aware Access Control

Set up security policies to restrict access to sensitive information and shared resources based on the user who is trying to access it. In the following figure user A can access both the Internet and an internal file server. User B has a lower level of access and can only access the Internet. User C is not even logged in, so and cannot access either the Internet or the file server.

Figure 5 Applications: User-Aware Access Control



Load Balancing

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

Figure 6 Applications: Multiple WAN Interfaces



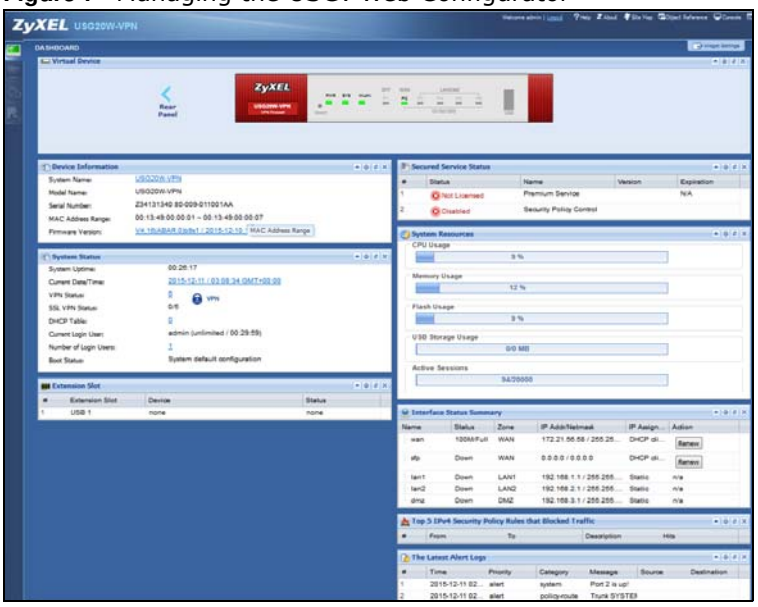
1.2 Management Overview

You can manage the USG in the following ways.

Web Configurator

The Web Configurator allows easy USG setup and management using an Internet browser. This User's Guide provides information about the Web Configurator.

Figure 7 Managing the USG: Web Configurator



Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the USG. Access it using remote management (for example, SSH or Telnet) or via the physical or Web Configurator console port. See the Command Reference Guide for CLI details. The default settings for the console port are:

Table 2 Console Port Default Settings

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	Off

FTP

Use File Transfer Protocol for firmware upgrades and configuration backup/restore.

SNMP

The device can be monitored and/or managed by an SNMP manager. See Section 30.11 on page 577.

Cloud CNM

Use the CloudCNM screen (see Section 30.13 on page 583) to enable and configure management of the USG by a Central Network Management system.

1.3 Web Configurator

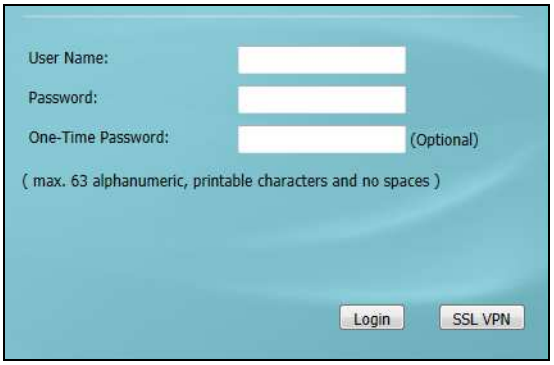
In order to use the Web Configurator, you must:

- Use one of the following web browser versions or later: Internet Explorer 7, Firefox 3.5, Chrome 9.0
- Allow pop-up windows (blocked by default in Windows XP Service Pack 2)
- Enable JavaScripts, Java permissions, and cookies

The recommended screen resolution is 1024 x 768 pixels.

1.3.1 Web Configurator Access

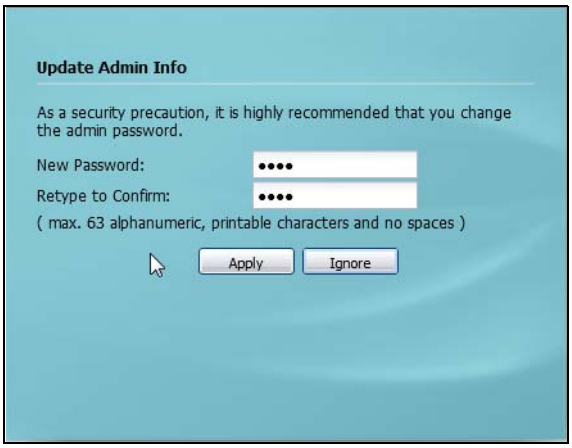
1. Make sure your USG hardware is properly connected. See the Quick Start Guide.
2. In your browser go to http://192.168.1.1. By default, the USG automatically routes this request to its HTTPS server, and it is recommended to keep this setting. The Login screen appears.



3. Type the user name (default: "admin") and password (default: "1234").

   If you have a OTP (One-Time Password) token generate a number and enter it in the One-Time Password field. The number is only good for one login. You must use the token to generate a new number the next time you log in.

4. Click Login. If you logged in using the default user name and password, the Update Admin Info screen appears. Otherwise, the dashboard appears.



5 The Network Risk Warning screen displays any unregistered or disabled security services. Select how often to display the screen and click OK.

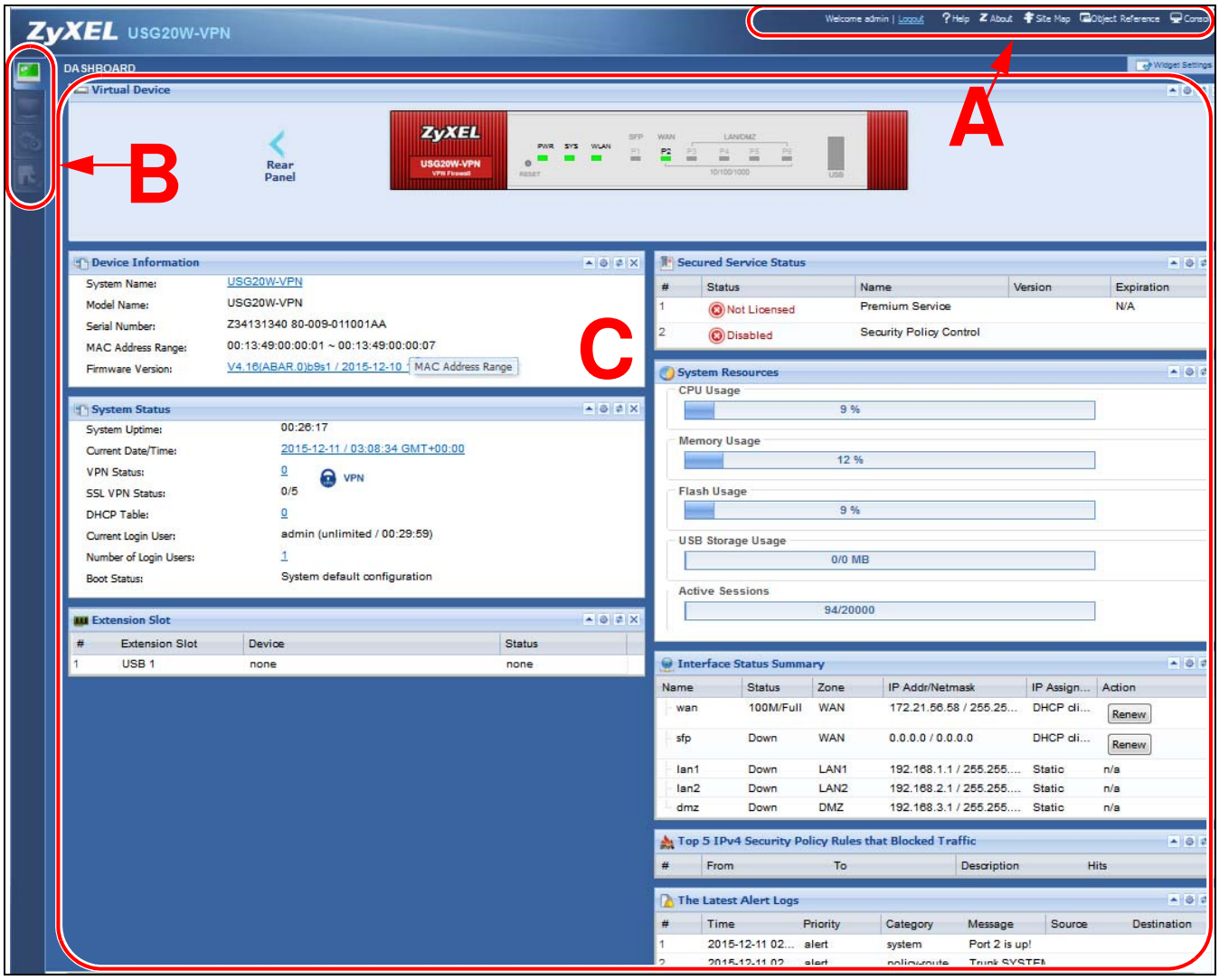


If you select Never and you later want to bring this screen back, use these commands (note the space before the underscore).

```
Router> enable
Router#
Router# configure terminal
Router(config)#
Router(config)# service-register _setremind
after-10-days
after-180-days
after-30-days
every-time
never
Router(config)# service-register _setremind every-time
Router(config)#
```

See the Command Line Interface (CLI) Reference Guide (RG) for details on all supported commands.

6 Follow the directions in the Update Admin Info screen. If you change the default password, the Login screen appears after you click Apply. If you click Ignore, the Installation Setup Wizard opens if the USG is using its default configuration; otherwise the dashboard appears.



1.3.2 Web Configurator Screens Overview

The Web Configurator screen is divided into these parts (as illustrated on page 25):

- A - title bar
- B - navigation panel
- C - main window

Title Bar

Figure 8 Title Bar



The title bar icons in the upper right corner provide the following functions.

Table 3 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Logout	Click this to log out of the Web Configurator.
Help	Click this to open the help page for the current screen.
About	Click this to display basic information about the USG.
Site Map	Click this to see an overview of links to the Web Configurator screens.
Object Reference	Click this to check which configuration items reference an object.
Console	Click this to open a Java-based console window from which you can run command line interface (CLI) commands. You will be prompted to enter your user name and password. See the Command Reference Guide for information about the commands.
CLI	Click this to open a popup window that displays the CLI commands sent by the Web Configurator to the USG.

About

Click About to display basic information about the USG.

Figure 9 About



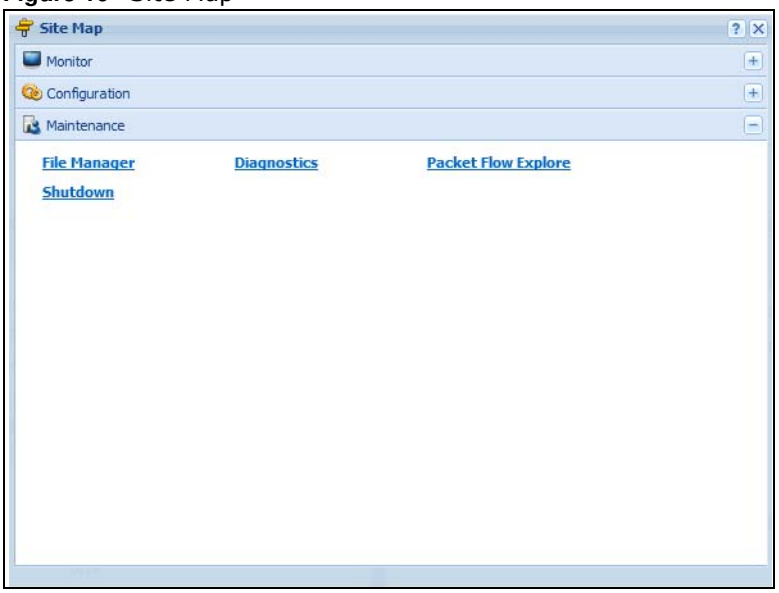
Table 4 About

LABEL	DESCRIPTION
Current Version	This shows the firmware version of the USG.
Released Date	This shows the date (yyyy-mm-dd) and time (hh:mm:ss) when the firmware is released.
OK	Click this to close the screen.

Site Map

Click Site MAP to see an overview of links to the Web Configurator screens. Click a screen's link to go to that screen.

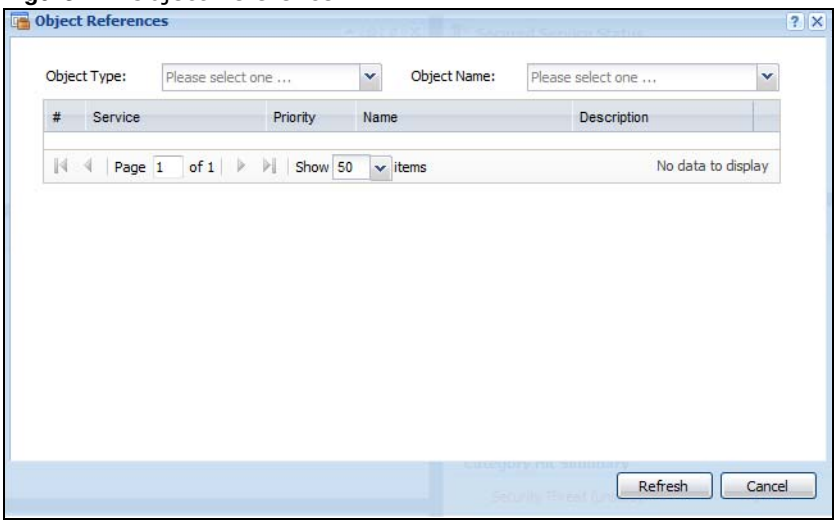
Figure 10 Site Map



Object Reference

Click Object Reference to open the Object Reference screen. Select the type of object and the individual object and click Refresh to show which configuration settings reference the object.

Figure 11 Object Reference



The fields vary with the type of object. This table describes labels that can appear in this screen.

Table 5 Object References

LABEL	DESCRIPTION
Object Name	This identifies the object for which the configuration settings that use it are displayed. Click the object's name to display the object's configuration screen in the main window.
#	This field is a sequential value, and it is not associated with any entry.
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.

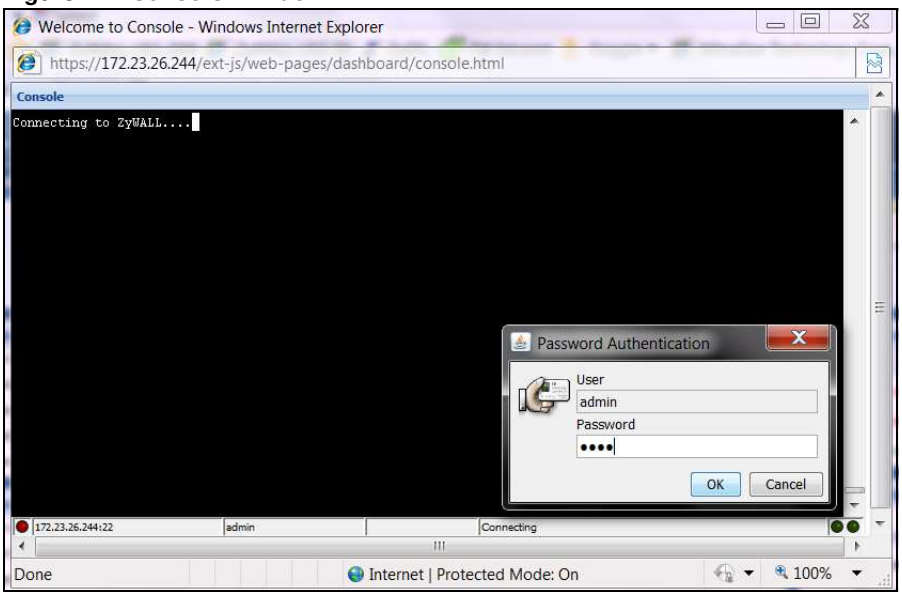
Table 5 Object References (continued)

LABEL	DESCRIPTION
Priority	If it is applicable, this field lists the referencing configuration item's position in its list, otherwise N/ A displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration item has a description configured, it displays here.
Refresh	Click this to update the information in this screen.
Cancel	Click Cancel to close the screen.

Console

Click Console to open a Java-based console window from which you can run CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for information about the commands.

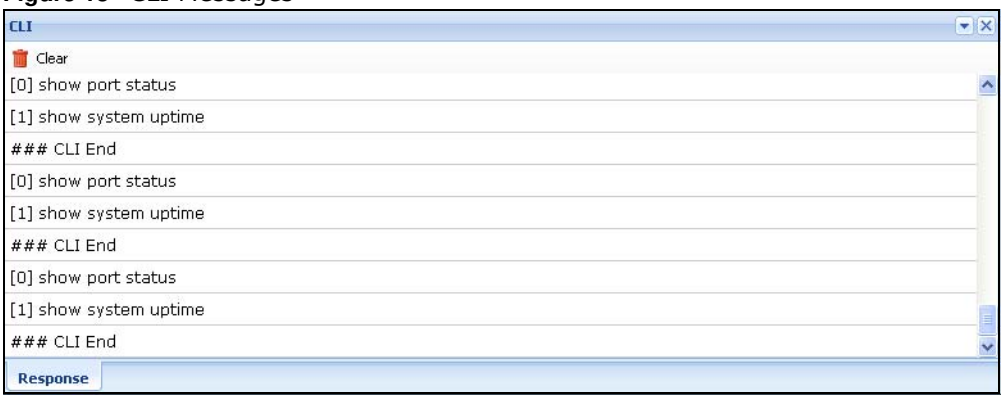
Figure 12 Console Window



CLI Messages

Click CLI to look at the CLI commands sent by the Web Configurator. Open the pop-up window and then click some menus in the web configurator to display the corresponding commands.

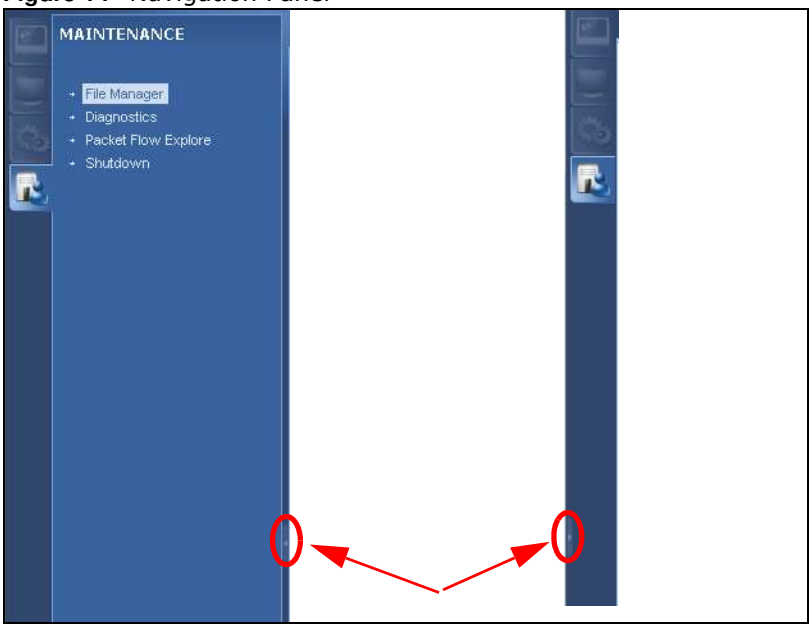
Figure 13 CLI Messages



1.3.3 Navigation Panel

Use the navigation panel menu items to open status and configuration screens. Click the arrow in the middle of the right edge of the navigation panel to hide the panel or drag to resize it. The following sections introduce the USG's navigation panel menus and their screens.

Figure 14 Navigation Panel



Dashboard

The dashboard displays general device information, system status, system resource usage, licensed service status, and interface status in widgets that you can re-arrange to suit your needs. See the Web Help for details on the dashboard.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 6 Monitor Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
System Status		
Port Statistics	Port Statistics	Displays packet statistics for each physical port.
Interface Status	Interface Summary	Displays general interface information and packet statistics.
Traffic Statistics	Traffic Statistics	Collect and display traffic statistics.
Session Monitor	Session Monitor	Displays the status of all current sessions.
IGMP Statistics	IGMP Statistics	Collect and display IGMP statistics.
DDNS Status	DDNS Status	Displays the status of the USG's DDNS domain names.
IP/MAC Binding	IP/MAC Binding	Lists the devices that have received an IP address from USG interfaces using IP/MAC binding.
Login Users	Login Users	Lists the users currently logged into the USG.
Cellular Status	Cellular Status	Displays details about the USG's mobile broadband connection status.
UPnP Port Status	Port Statistics	Displays details about UPnP connections going through the USG.
USB Storage	Storage Information	Displays details about USB device connected to the USG.
Ethernet Neighbor	Ethernet Neighbor	View and manage the USG's neighboring devices via Smart Connect (Layer Link Discovery Protocol (LLDP)). Use the ZyXEL One Network (ZON) utility to view and manage the USG's neighboring devices via the ZyXEL Discovery Protocol (ZDP).
Wireless		
AP Information	WLAN Setting	Edit wireless AP information, remove APs, and reboot them.
DCS		Configure dynamic wireless channel selection.
VPN Monitor		
IPSec	IPSec	Displays and manages the active IPSec SAs.
SSL	SSL	Lists users currently logged into the VPN SSL client portal. You can also log out individual users and delete related session information.
L2TP over IPSec	Session Monitor	Displays details about current L2TP sessions.
UTM Statistics		
Content Filter	Report	Collect and display content filter statistics
Anti-Spam	Report	Collect and display spam statistics.
	Status	Displays how many mail sessions the USG is currently checking and DNSBL (Domain Name Service-based spam Black List) statistics.
Log	View Log	Lists log entries.
	View AP Log	Lists AP log entries.

Configuration Menu

Use the configuration menu screens to configure the USG's features.

Table 7 Configuration Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Quick Setup		Quickly configure WAN interfaces or VPN connections.
Licensing		
Registration	Registration	Register the device and activate trial services.
	Service	View the licensed service status and upgrade licensed services.
Wireless		
AP Management	WLAN Setting	Configuration the USG's general wireless settings.
DCS		Configure dynamic wireless channel selection.
Network		
Interface	Port Role	Use this screen to set the USG's flexible ports such as LAN, OPT, WLAN, or DMZ.
	Ethernet	Manage Ethernet interfaces and virtual Ethernet interfaces.
	PPP	Create and manage PPPoE and PPTP interfaces.
	Cellular	Configure a cellular Internet connection for an installed mobile broadband card.
	Tunnel	Configure tunneling between IPv4 and IPv6 networks.
	VLAN	Create and manage VLAN interfaces and virtual VLAN interfaces.
	Bridge	Create and manage bridges and virtual bridge interfaces.
	Trunk	Create and manage trunks (groups of interfaces) for load balancing.
Routing	Policy Route	Create and manage routing policies.
	Static Route	Create and manage IP static routing information.
	RIP	Configure device-level RIP settings.
	OSPF	Configure device-level OSPF settings, including areas and virtual links.
DDNS	DDNS	Define and manage the USG's DDNS domain names.
NAT	NAT	Set up and manage port forwarding rules.
HTTP Redirect	HTTP Redirect	Set up and manage HTTP redirection rules.
ALG	ALG	Configure SIP, H.323, and FTP pass-through settings.
UPnP	UPnP	Configure interfaces that allow UPnP and NAT-PMP connections.
IP/MAC Binding	Summary	Configure IP to MAC address bindings for devices connected to each supported interface.
	Exempt List	Configure ranges of IP addresses to which the USG does not apply IP/MAC binding.
Layer 2 Isolation	General	Enable layer-2 isolation on the USG and the internal interface(s).
	White List	Enable and configure the white list.
DNS Inbound LB	DNS Load Balancing	Configure DNS Load Balancing.
Web Authentication	Web Authentication	Define a web portal and exempt services from authentication.
	SSO	Configure the USG to work with a Single Sign On agent.
Security Policy		

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Policy Control	Policy	Create and manage level-3 traffic rules and apply UTM profiles.
Session Control	Session Control	Limit the number of concurrent client NAT/security policy sessions.
VPN		
IPSec VPN	VPN Connection	Configure IPSec tunnels.
	VPN Gateway	Configure IKE tunnels.
	Concentrator	Combine IPSec VPN connections into a single secure network
	Configuration Provisioning	Set who can retrieve VPN rule settings from the USG using the USG IPSec VPN Client.
SSL VPN	Access Privilege	Configure SSL VPN access rights for users and groups.
	Global Setting	Configure the USG's SSL VPN settings that apply to all connections.
	SecuExtender	Check for the latest version of the SecuExtender VPN client.
L2TP VPN	L2TP VPN	Configure L2TP over IPSec tunnels.
BWM	BWM	Enable and configure bandwidth management rules.
UTM Profile		
Content Filter	Profile	Create and manage the detailed filtering rules for content filtering profiles and then apply to a traffic flow using a security policy.
	Trusted Web Sites	Create a list of allowed web sites that bypass content filtering policies.
	Forbidden Web Sites	Create a list of web sites to block regardless of content filtering policies.
Anti-Spam	Profile	Turn anti-spam on or off and manage anti-spam policies. Create anti-spam template(s) of settings to apply to a traffic flow using a security policy.
	Mail Scan	Configure e-mail scanning details.
	Black/White List	Set up a black list to identify spam and a white list to identify legitimate e-mail.
	DNSBL	Have the USG check e-mail against DNS Black Lists.
Object		
Zone	Zone	Configure zone template(s) used to define various policies.
User/Group	User	Create and manage users.
	Group	Create and manage groups of users.
	Setting	Manage default settings for all users, general settings for user sessions, and rules to force user authentication.
	MAC Address	Configure the MAC addresses or OUI (Organizationally Unique Identifier) of wireless clients for MAC authentication using the local user database.
AP Profile	Radio	Create template(s) of radio settings to apply to policies as an object.
	SSID	Create template(s) of wireless settings to apply to radio profiles or policies as an object.
MON Profile	MON Profile	Create and manage rogue AP monitoring files that can be associated with different APs.
Address	Address	Create and manage host, range, and network (subnet) addresses.
	Address Group	Create and manage groups of addresseto apply to policies as a single objects.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Service	Service	Create and manage TCP and UDP services.
	Service Group	Create and manage groups of services to apply to policies as a single object.
Schedule	Schedule	Create one-time and recurring schedules.
	Schedule Group	Create and manage groups of schedules to apply to policies as a single object.
AAA Server	Active Directory	Configure the Active Directory settings.
	LDAP	Configure the LDAP settings.
	RADIUS	Configure the RADIUS settings.
Auth. Method	Authentication Method	Create and manage ways of authenticating users.
Certificate	My Certificates	Create and manage the USG's certificates.
	Trusted Certificates	Import and manage certificates from trusted sources.
ISP Account	ISP Account	Create and manage ISP account information for PPPoE/PPTP interfaces.
SSL Application	SSL Application	Create SSL web application or file sharing objects to apply to policies.
DHCPv6	Request	Configure IPv6 DHCP request type and interface information.
	Lease	Configure IPv6 DHCP lease type and interface information.
System		
Host Name	Host Name	Configure the system and domain name for the USG.
USB Storage	Settings	Configure the settings for the connected USB devices.
Date/Time	Date/Time	Configure the current date, time, and time zone in the USG.
Console Speed	Console Speed	Set the console speed.
DNS	DNS	Configure the DNS server and address records for the USG.
WWW	Service Control	Configure HTTP, HTTPS, and general authentication.
	Login Page	Configure how the login and access user screens look.
SSH	SSH	Configure SSH server and SSH service settings.
TELNET	TELNET	Configure telnet server settings for the USG.
FTP	FTP	Configure FTP server settings.
SNMP	SNMP	Configure SNMP communities and services.
Auth. Server	Auth. Server	Configure the USG to act as a RADIUS server.
CloudCNM	CloudCNM	Enable and configure management of the USG by a Central Network Management system.
Language	Language	Select the Web Configurator language.
IPv6	IPv6	Enable IPv6 globally on the USG here.
ZON	ZON	Use the ZyXEL One Network (ZON) utility to view and manage the USG's neighboring devices via the ZyXEL Discovery Protocol (ZDP).
Log & Report		
Email Daily Report	Email Daily Report	Configure where and how to send daily reports and what reports to send.
Log Settings	Log Settings	Configure the system log, e-mail logs, and remote syslog servers.

Maintenance Menu

Use the maintenance menu screens to manage configuration and firmware files, run diagnostics, and reboot or shut down the USG.

Table 8 Maintenance Menu Screens Summary

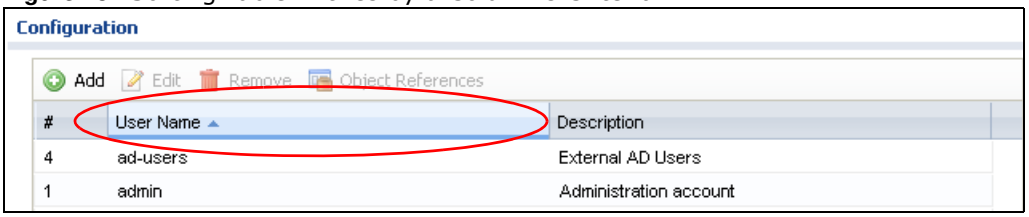
FOLDER OR LINK	TAB	FUNCTION
File Manager	Configuration File	Manage and upload configuration files for the USG.
	Firmware Package	View the current firmware version and upload firmware. Reboot with your choice of firmware.
	Shell Script	Manage and run shell script files for the USG.
Diagnostics	Diagnostic	Collect diagnostic information.
	Packet Capture	Capture packets for analysis.
	Core Dump	Connect a USB device to the USG and save the USG operating system kernel to it here.
	System Log	Connect a USB device to the USG and archive the USG system logs to it here.
	Network Tool	Identify problems with the connections. You can use Ping or TraceRoute to help you identify problems.
	Wireless Frame Capture	Capture wireless frames from APs for analysis.
Packet Flow Explore	Routing Status	Check how the USG determines where to route a packet.
	SNAT Status	View a clear picture on how the USG converts a packet's source IP address and check the related settings.
Shutdown	Shutdown	Turn off the USG.

1.3.4 Tables and Lists

Web Configurator tables and lists are flexible with several options for how to display their entries.

Click a column heading to sort the table's entries according to that column's criteria.

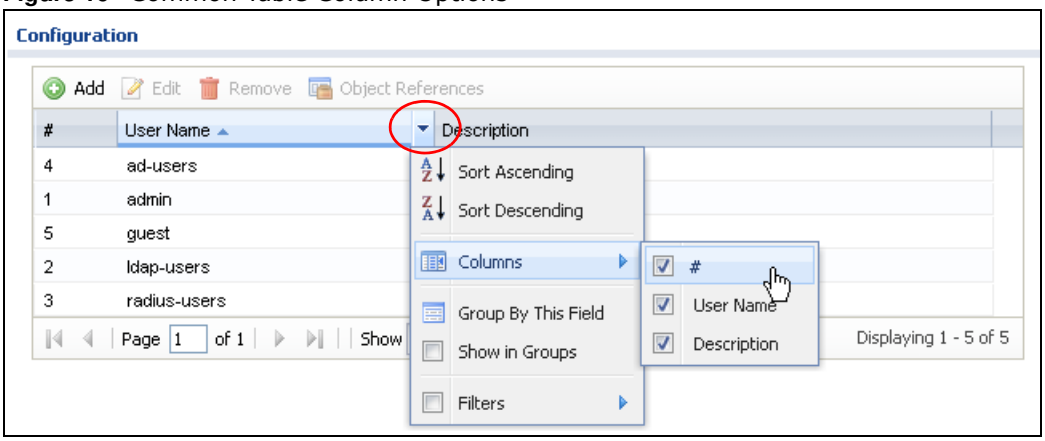
Figure 15 Sorting Table Entries by a Column's Criteria



Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

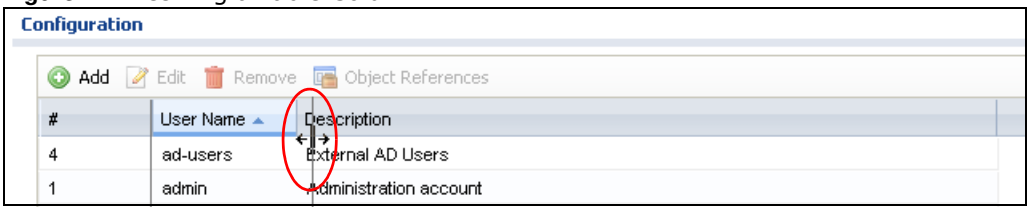
- Sort in ascending or descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups
- Filter by mathematical operators (<, >, or =) or searching for text

Figure 16 Common Table Column Options



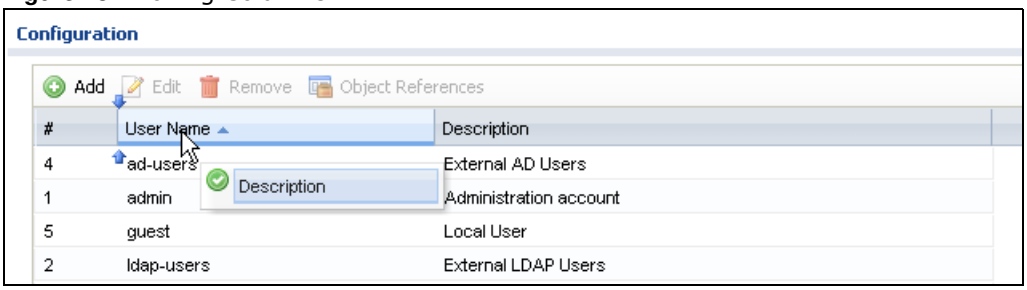
Select a column heading cell's right border and drag to re-size the column.

Figure 17 Resizing a Table Column



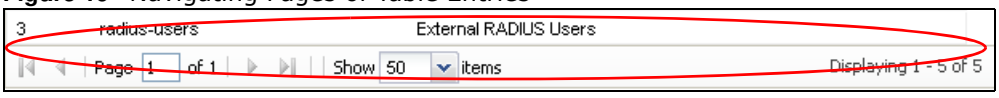
Select a column heading and drag and drop it to change the column order. A green check mark displays next to the column's title when you drag the column to a valid new location.

Figure 18 Moving Columns



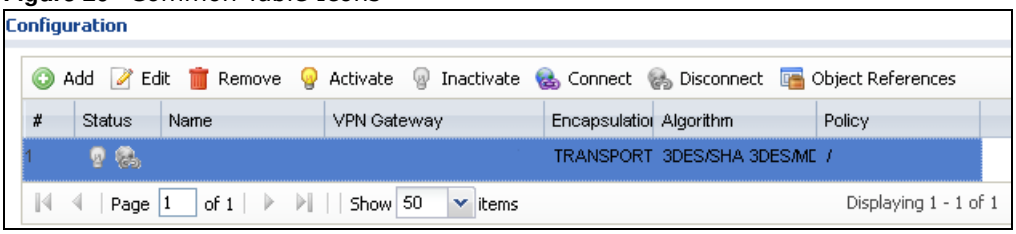
Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.

Figure 19 Navigating Pages of Table Entries



The tables have icons for working with table entries. You can often use the [Shift] or [Ctrl] key to select multiple entries to remove, activate, or deactivate.

Figure 20 Common Table Icons



Here are descriptions for the most common table icons.

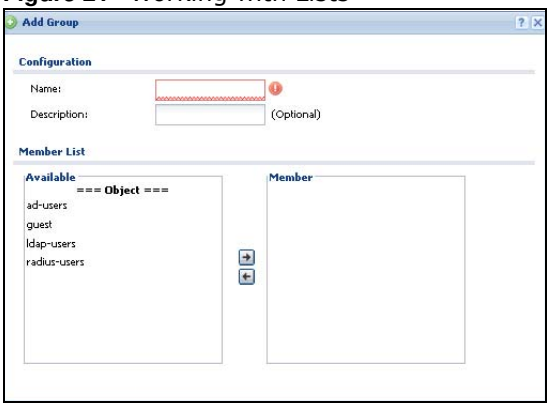
Table 9 Common Table Icons

LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the USG applies the table's entries in order like the security policy for example), you can select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Connect	To connect an entry, select it and click Connect.
Disconnect	To disconnect an entry, select it and click Disconnect.
Object References	Select an entry and click Object References to check which settings use the entry.
Move	To change an entry's position in a numbered list, select it and click Move to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the entry you are moving becomes number 6 and the previous entry 6 (if there is one) gets pushed up (or down) one.

Working with Lists

When a list of available entries displays next to a list of selected entries, you can often just double-click an entry to move it from one list to the other. In some lists you can also use the [Shift] or [Ctrl] key to select multiple entries, and then use the arrow button to move them to the other list.

Figure 21 Working with Lists



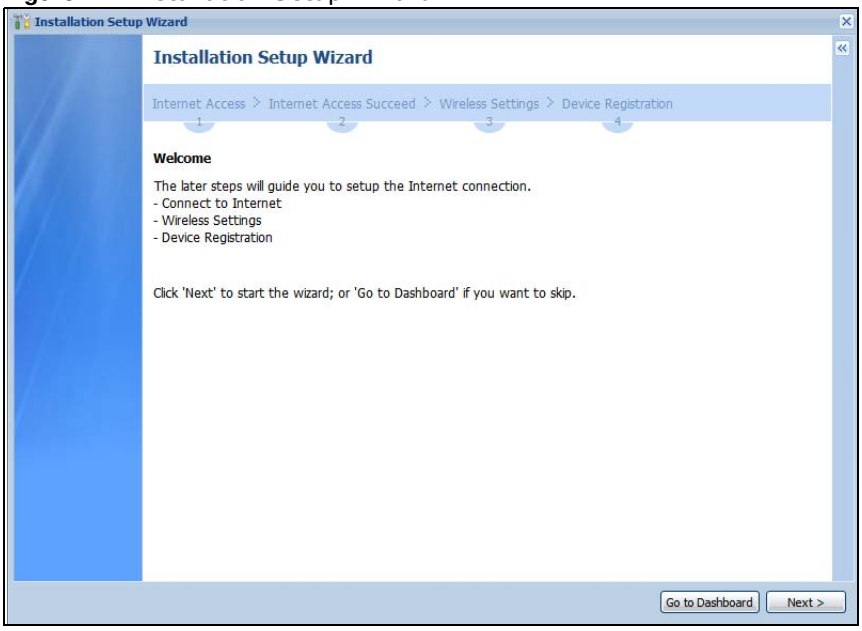
2

Installation Setup Wizard

2.1 Installation Setup Wizard Screens

When you log into the Web Configurator for the first time or when you reset the USG to its default configuration, the Installation Setup Wizard screen displays. This wizard helps you configure Internet connection settings and activate subscription services. This chapter provides information on configuring the Web Configurator's installation setup wizard. See the feature-specific chapters in this User's Guide for background information.

Figure 22 Installation Setup Wizard



- Click the double arrow in the upper right corner to display or hide the help.
- Click Go to Dashboard to skip the installation setup wizard or click Next to start configuring for Internet access.

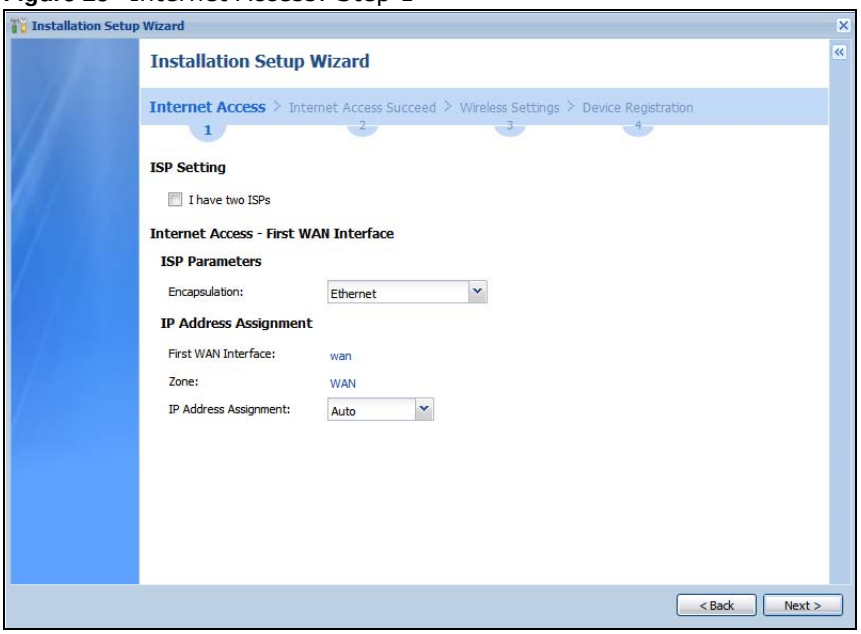
2.1.1 Internet Access Setup - WAN Interface

Use this screen to set how many WAN interfaces to configure and the first WAN interface's type of encapsulation and method of IP address assignment.

The screens vary depending on the encapsulation type. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

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

Figure 23 Internet Access: Step 1



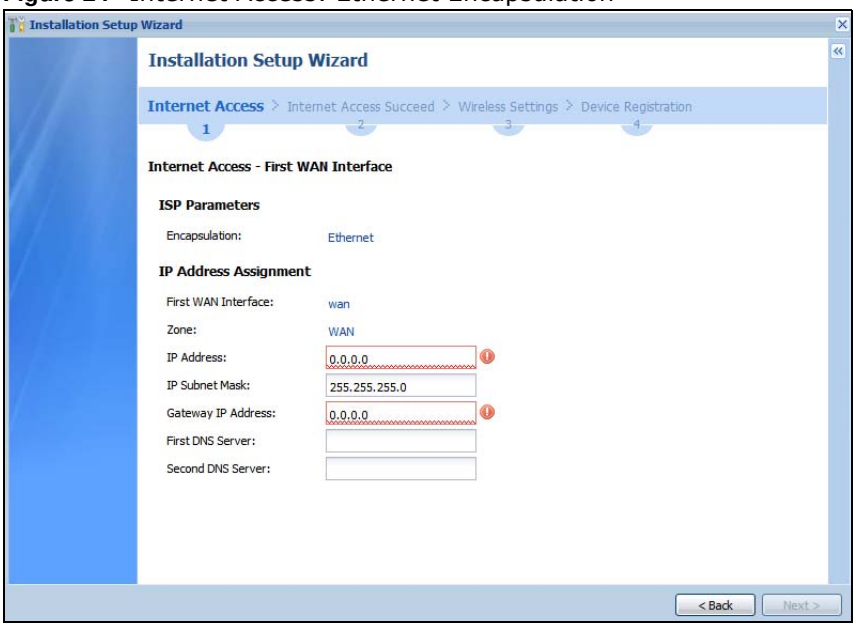
- I have two ISPs: Select this option to configure two Internet connections. Leave it cleared to configure just one. This option appears when you are configuring the first WAN interface.
- Encapsulation: Choose the Ethernet option when the WAN port is used as a regular Ethernet. Otherwise, choose PPPoE or PPTP for a dial-up connection according to the information from your ISP.
- WAN Interface: This is the interface you are configuring for Internet access.
- Zone: This is the security zone to which this interface and Internet connection belong.
- IP Address Assignment: Select Auto if your ISP did not assign you a fixed IP address. Select Static if the ISP assigned a fixed IP address.

2.1.2 Internet Access: Ethernet

This screen is read-only if you set the previous screen's IP Address Assignment field to Auto. If you set the previous screen's IP Address Assignment field to Static, use this screen to configure your IP address settings.

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

Figure 24 Internet Access: Ethernet Encapsulation



- Encapsulation: This displays the type of Internet connection you are configuring.
- First WAN Interface: This is the number of the interface that will connect with your ISP.
- Zone: This is the security zone to which this interface and Internet connection will belong.
- IP Address: Enter your (static) public IP address. Auto displays if you selected Auto as the IP Address Assignment in the previous screen.

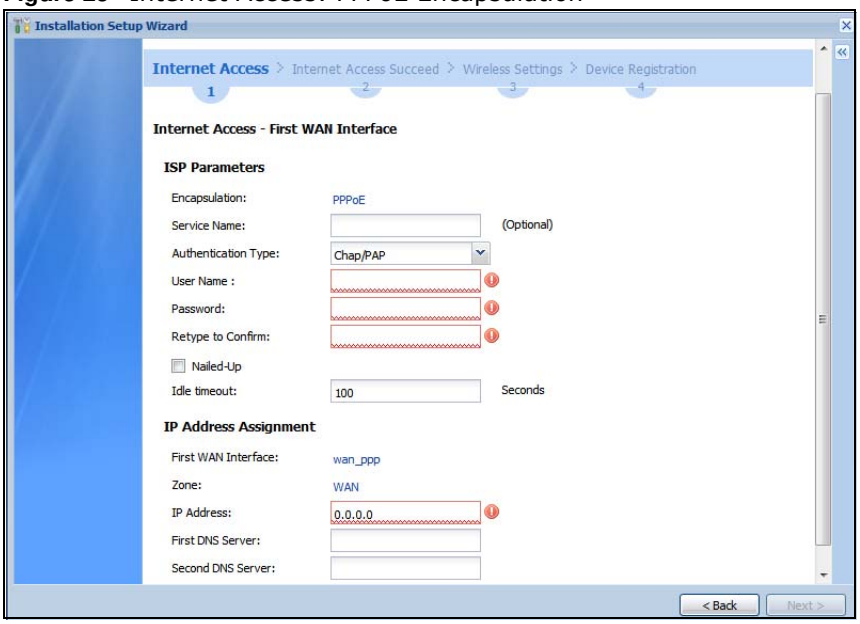
The following fields display if you selected static IP address assignment.

- IP Subnet Mask: Enter the subnet mask for this WAN connection's IP address.
- Gateway IP Address: Enter the IP address of the router through which this WAN connection will send traffic (the default gateway).
- First / Second DNS Server: These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The USG uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

2.1.3 Internet Access: PPPoE

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

Figure 25 Internet Access: PPPoE Encapsulation



2.1.3.1 ISP Parameters

- Type the PPPoE Service Name from your service provider. PPPoE uses a service name to identify and reach the PPPoE server. You can use alphanumeric and -_@$./ characters, and it can be up to 64 characters long.
- Authentication Type - Select an authentication protocol for outgoing connection requests. Options are:
  - CHAP/PAP - Your USG accepts either CHAP or PAP when requested by the remote node.
  - CHAP - Your USG accepts CHAP only.
  - PAP - Your USG accepts PAP only.
  - MSCHAP - Your USG accepts MSCHAP only.
  - MSCHAP-V2 - Your USG accepts MSCHAP-V2 only.
- Type the User Name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
- Type the Password associated with the user name. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
- Select Nailed-Up if you do not want the connection to time out. Otherwise, type the Idle Timeout in seconds that elapses before the router automatically disconnects from the PPPoE server.

2.1.3.2 WAN IP Address Assignments

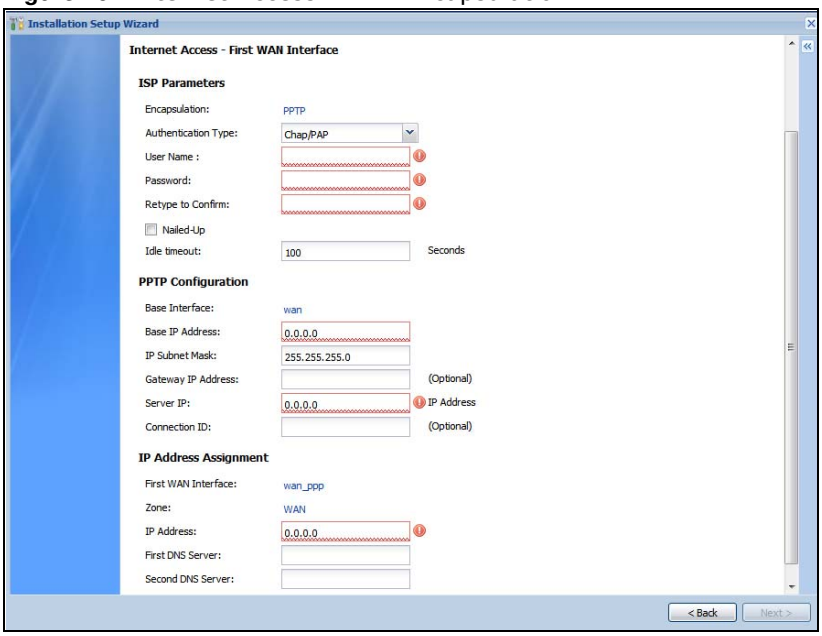
- WAN Interface: This is the name of the interface that will connect with your ISP.
- Zone: This is the security zone to which this interface and Internet connection will belong.
- IP Address: Enter your (static) public IP address. Auto displays if you selected Auto as the IP Address Assignment in the previous screen.

- First / Second DNS Server: These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The USG uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.

2.1.4 Internet Access: PPTP

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

Figure 26 Internet Access: PPTP Encapsulation



2.1.4.1 ISP Parameters

- Authentication Type - Select an authentication protocol for outgoing calls. Options are:
  - CHAP/ PAP - Your USG accepts either CHAP or PAP when requested by the remote node.
  - CHAP - Your USG accepts CHAP only.
  - PAP - Your USG accepts PAP only.
  - MSCHAP - Your USG accepts MSCHAP only.
  - MSCHAP-V2 - Your USG accepts MSCHAP-V2 only.
- Type the User Name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
- Type the Password associated with the user name. Use up to 64 ASCII characters except the [] and ?. This field can be blank. Re-type your password in the next field to confirm it.
- Select Nailed-Up if you do not want the connection to time out. Otherwise, type the Idle Timeout in seconds that elapses before the router automatically disconnects from the PPTP server.

2.1.4.2 PPTP Configuration

- Base Interface: This identifies the Ethernet interface you configure to connect with a modem or router.
- Type a Base IP Address (static) assigned to you by your ISP.
- Type the IP Subnet Mask assigned to you by your ISP (if given).
- Server IP: Type the IP address of the PPTP server.
- Type a Connection ID or connection name. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your broadband modem or router. You can use alphanumeric and -_: characters, and it can be up to 31 characters long.

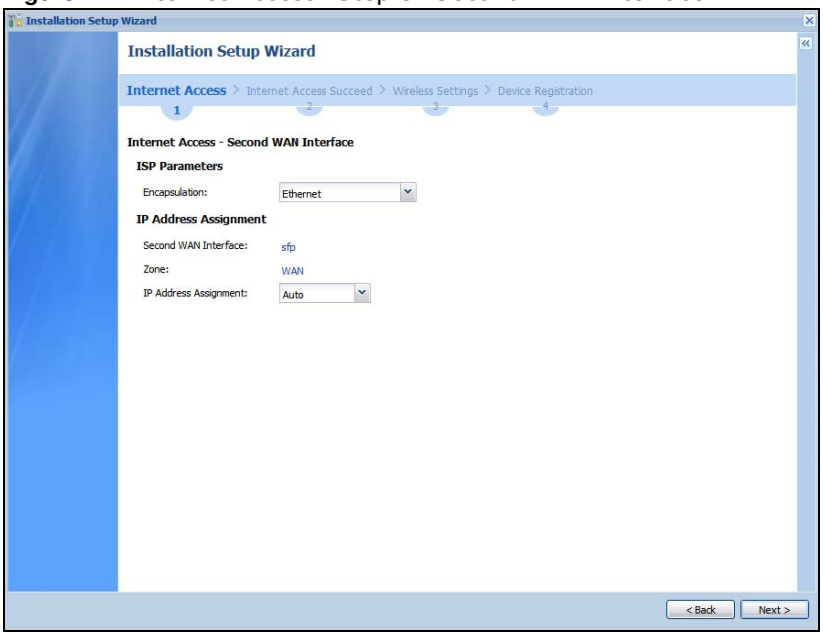
2.1.4.3 WAN IP Address Assignments

- First WAN Interface: This is the connection type on the interface you are configuring to connect with your ISP.
- Zone This is the security zone to which this interface and Internet connection will belong.
- IP Address: Enter your (static) public IP address. Auto displays if you selected Auto as the IP Address Assignment in the previous screen.
- First / Second DNS Server: These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The USG uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

2.1.5 Internet Access Setup - Second WAN Interface

If you selected I have two ISPs, after you configure the First WAN Interface, you can configure the Second WAN Interface. The screens for configuring the second WAN interface are similar to the first (see Section 2.1.1 on page 37).

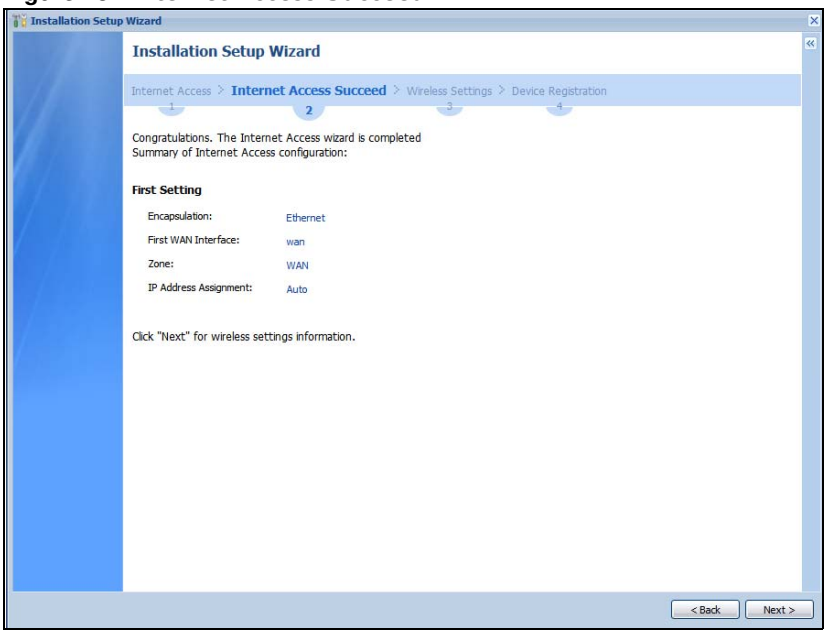
Figure 27 Internet Access: Step 3: Second WAN Interface



2.1.6 Internet Access Succeed

This screen shows your Internet access settings that have been applied successfully.

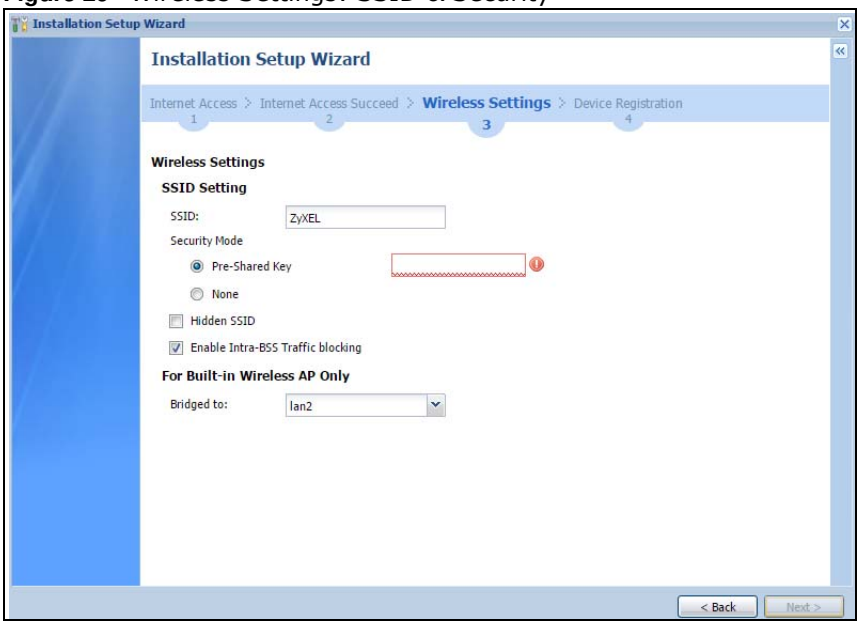
Figure 28 Internet Access Succeed



2.1.7 Wireless Settings: SSID & Security

Configure SSID and wireless security in this screen.

Figure 29 Wireless Settings: SSID & Security



SSID Setting

- SSID - Enter a descriptive name of up to 32 printable characters for the wireless LAN.
- Security Mode - Select Pre-Shared Key to add security on this wireless network. Otherwise, select None to allow any wireless client to associate this network without authentication.
- Pre-Shared Key - Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
- Hidden SSID - Select this option if you want to hide the SSID in the outgoing beacon frame. A wireless client then cannot obtain the SSID through scanning using a site survey tool.
- Enable Intra-BSS Traffic Blocking - Select this option if you want to prevent crossover traffic from within the same SSID. Wireless clients can still access the wired network but cannot communicate with each other.

For Built-in Wireless AP Only

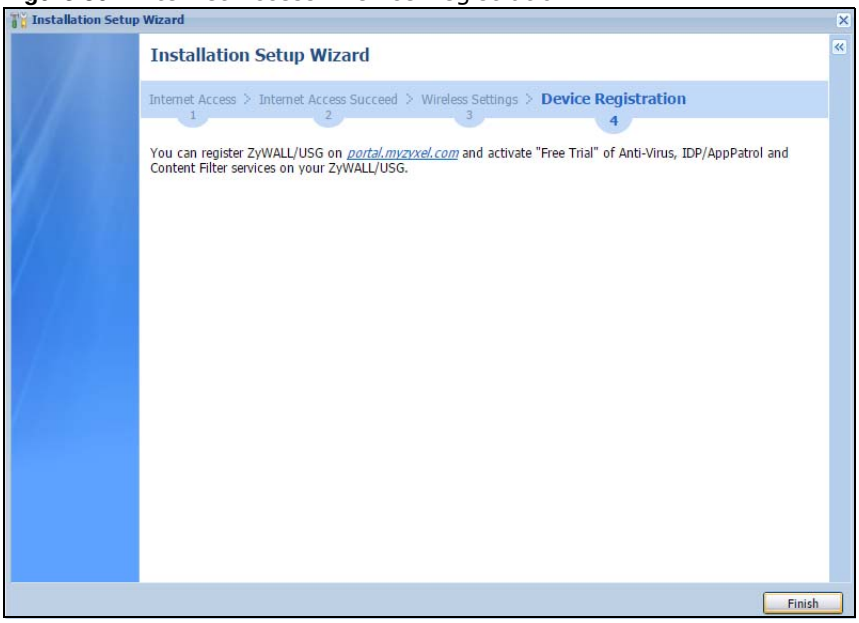
- Bridged to: USGs with W in the model name have a built-in AP. Select an interface to bridge with the built-in AP wireless network. Devices connected to this interface will then be in the same broadcast domain as devices in the AP wireless network.

2.1.8 Internet Access - Device Registration

Click the link in this screen to register your device at portal.myzyxel.com.

Note: The USG must be connected to the Internet in order to register.

Figure 30 Internet Access: Device Registration



You will need the USG's serial number and LAN MAC address to register it if you have not already done so. Use the Configuration > Licensing > Registration > Service screen to update your service subscription status.

3

Hardware, Interfaces and Zones

3.1 Hardware Overview

USG20-VPN and USG20W-VPN have different housings.

3.1.1 Front Panels

The LED indicators are located on the front panel.

Figure 31 USG20-VPN Front Panel

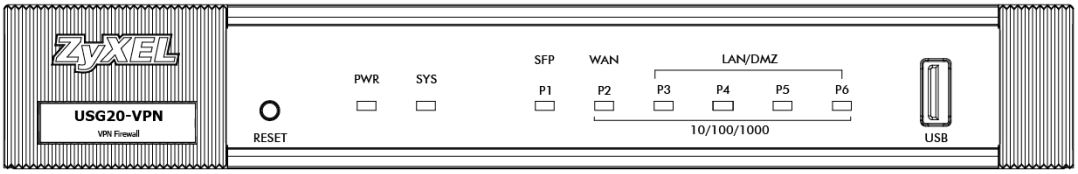
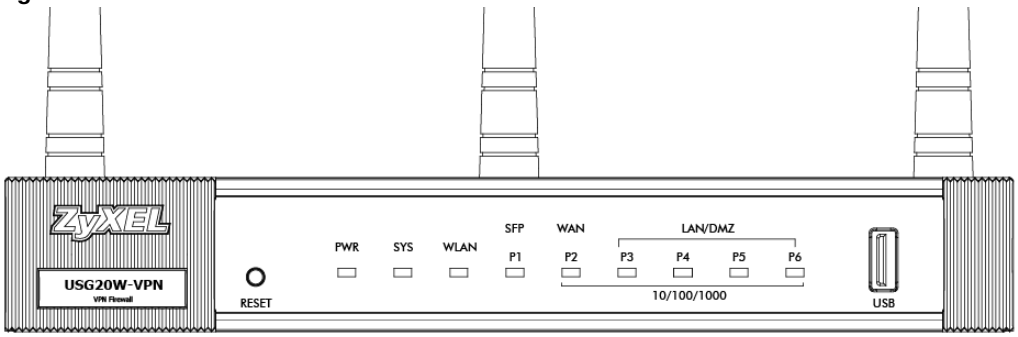


Figure 32 USG20W-VPN Front Panel



The following table describes the LEDs.

Table 10 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The USG is turned off.
	Green	On	The USG is turned on.
	Red	On	There is a hardware component failure. Shut down the device, wait for a few minutes and then restart the device (see Section 3.1.3 on page 47). If the LED turns red again, then please contact your vendor.
SYS	Green	Off	The USG is not ready or has failed.
		On	The USG is ready and running.
		Blinking	The USG is booting.
	Red	On	The USG had an error or has failed.

Table 10 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
WLAN	Green	Off	The built-in wireless LAN card is not ready or has failed.
		On	The built-in wireless LAN card is ready.
		Blinking	The built-in wireless LAN card is sending or receiving packets.
P1, P2...	Green	Off	There is no traffic on this port.
		On	This port has a successful 10/100 Mbps connection.
		Blinking	The USG is sending or receiving packets on this port with a 10/100 Mbps connection.
	Yellow	Off	There is no connection on this port.
		On	This port has a successful 1000 Mbps connection.
		Blinking	The device is sending or receiving packets on this port with a 1000 Mbps connection.

3.1.2 Rear Panels

The connection ports are located on the rear panel.

Figure 33 USG20-VPN Rear Panel

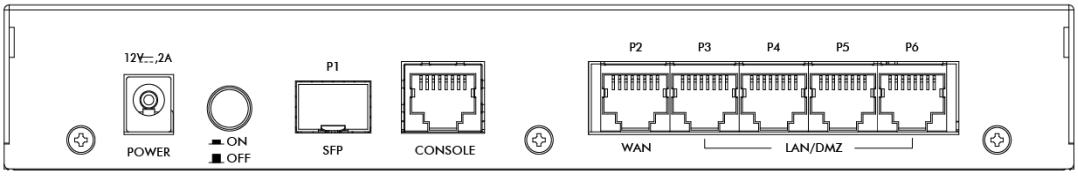
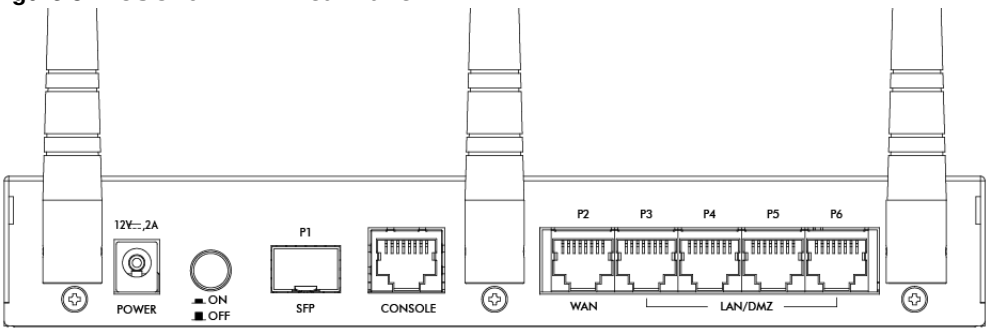


Figure 34 USG20W-VPN Rear Panel



The following table describes the items on the rear panel

Table 11 Rear Panel Items

LABEL	DESCRIPTION
Power	Use the included power cord to connect the power socket to a power outlet. Turn the power switch on if your USG has a power switch.

Table 11 Rear Panel Items (continued)

LABEL	DESCRIPTION
WAN/LAN/DMZ/ (Gigabit SFP/ Ethernet Port)	P1- You have to install an SFP (Small Form-factor Pluggable) transceiver and connect fiber optic cables to it for using a 1Gbps/100Mbps WAN connection. P2~P6 - Connect an Ethernet cable to the port for using a 1Gbps WAN/LAN/DMZ connection.
Console	You can use the console port to manage the USG using CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for more information about the CLI. When configuring using the console port, you need a computer equipped with communications software configured to the following parameters: • Speed 115200 bps • Data Bits 8 • Parity None • Stop Bit 1 • Flow Control Off

Note: Use an 8-wire Ethernet cable to run your Gigabit Ethernet connection at 1000 Mbps. Using a 4-wire Ethernet cable limits your connection to 100 Mbps. Note that the connection speed also depends on what the Ethernet device at the other end can support.

3.1.3 Wall-mounting

Both USG20-VPN and USG20W-VPN can be mounted on a wall.

1 Drill two holes 3 mm ~ 4 mm (0.12" ~ 0.16") wide, 20 mm ~ 30 mm (0.79” ~ 1.18”) deep and 150 mm apart, into a wall. Place two screw anchors in the holes.

2 Screw two screws with 6 mm ~ 8 mm (0.24" ~ 0.31") wide heads into the screw anchors. Do not screw the screws all the way in to the wall; leave a small gap between the head of the screw and the wall.

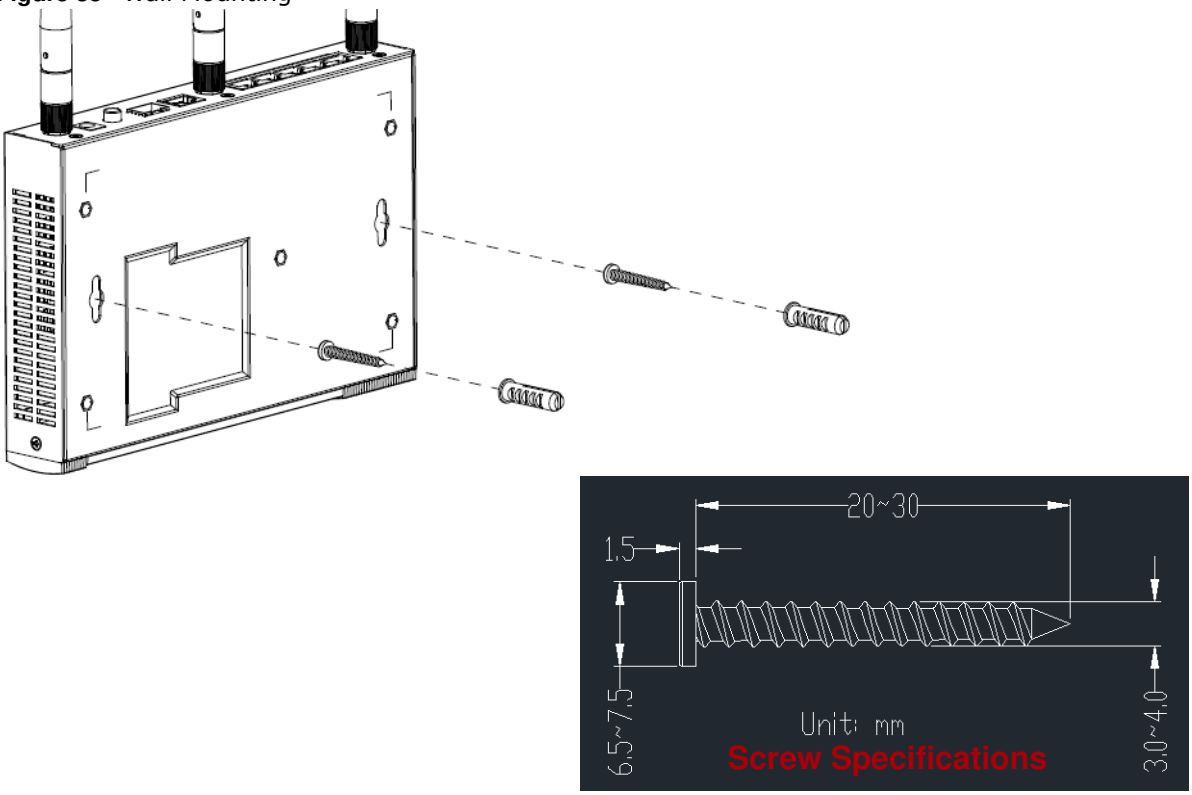
The gap must be big enough for the screw heads to slide into the screw slots and the connection cables to run down the back of the USG.

Note: Make sure the screws are securely fixed to the wall and strong enough to hold the weight of the USG with the connection cables.

3 Use the holes on the bottom of the USG to hang the USG on the screws.

Wall-mount the USG horizontally. The USG's side panels with ventilation slots should not be facing up or down as this position is less safe.

Figure 35 Wall Mounting



3.2 Default Zones, Interfaces, and Ports

The default configurations for zones, interfaces, and ports are as follows. References to interfaces may be generic rather than the specific name used in your model. For example, this guide may use "the WAN interface" rather than "wan1" or "wan2".

The following table shows the default physical port and interface mapping for each model at the time of writing.

Table 12 Default Physical Port - Interface Mapping

PORT / INTERFACE	P1	P2	P3	P4	P5	P6
• USG20-VPN	sfp	wan	lan1	lan1	lan1	lan1
• USG20W-VPN	sfp	wan	lan1	lan1	lan1	lan1

The following table shows the default interface and zone mapping for each model at the time of writing.

Table 13 Default Zone - Interface Mapping

ZONE / INTERFACE	WAN	LAN1	LAN2	DMZ
• USG20-VPN	WAN WAN_PPP SFP SFP_PPP	LAN1	LAN2	DMZ
• USG20W-VPN	WAN WAN_PPP SFP SFP_PPP	LAN1	LAN2	DMZ

3.3 Stopping the USG

Always use Maintenance > Shutdown > Shutdown or the `shutdown` command before you turn off the USG or remove the power. Not doing so can cause the firmware to become corrupt.

4

Quick Setup Wizards

4.1 Quick Setup Overview

The Web Configurator's quick setup wizards help you configure Internet and VPN connection settings. This chapter provides information on configuring the quick setup screens in the Web Configurator. See the feature-specific chapters in this User's Guide for background information.

In the Web Configurator, click Configuration > Quick Setup to open the first Quick Setup screen.

Figure 36 Quick Setup



- WAN Interface

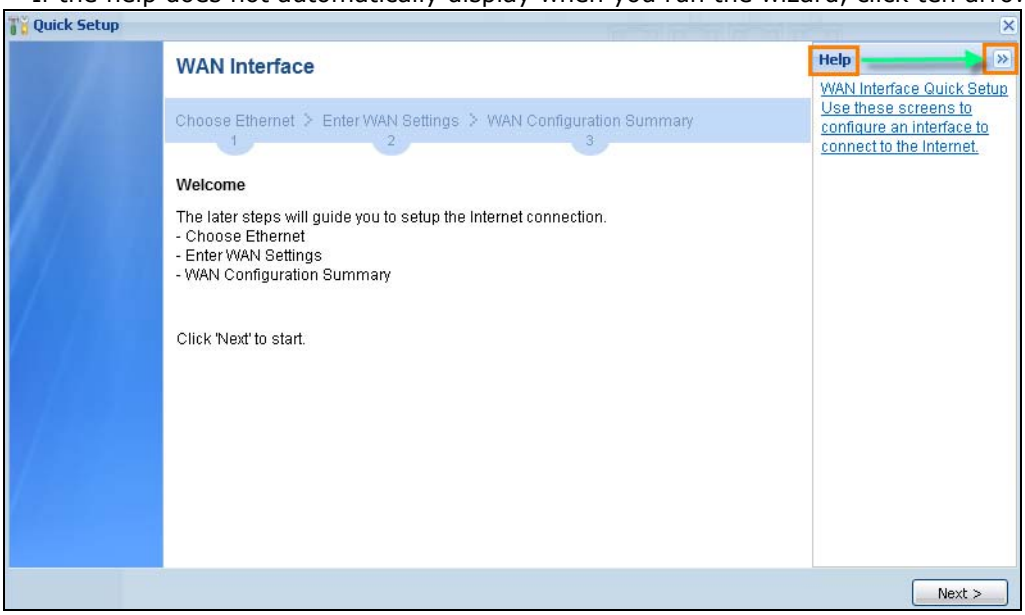
  Click this link to open a wizard to set up a WAN (Internet) connection. This wizard creates matching ISP account settings in the USG if you use PPPoE or PPTP. See Section 4.2 on page 51.

- VPN SETUP

  Use VPN Setup to configure a VPN (Virtual Private Network) rule for a secure connection to another computer or network. Use VPN Settings for Configuration Provisioning to set up a VPN rule that can be retrieved with the USG IPSec VPN Client. You only need to enter a user name, password and the IP address of the USG in the IPSec VPN Client to get all VPN settings automatically from the USG. See Section 4.3 on page 56.Use VPN Settings for L2TP VPN Settings to configure the L2TP VPN for clients.

- Wizard Help

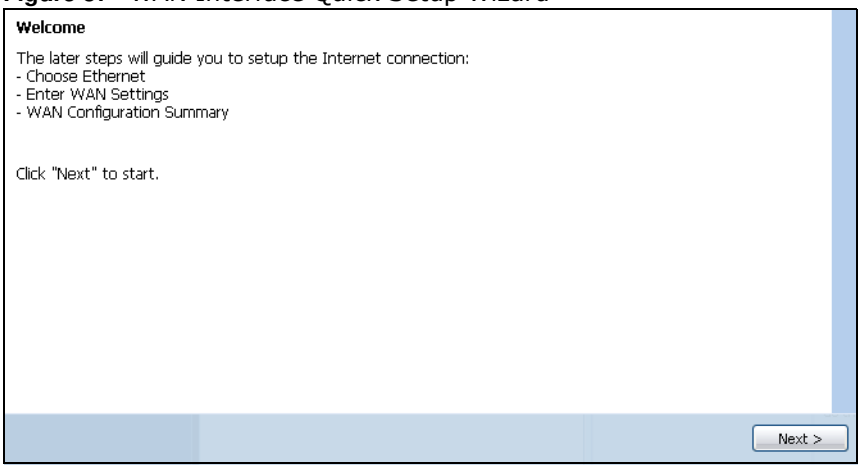
  If the help does not automatically display when you run the wizard, click teh arrow to display it.



4.2 WAN Interface Quick Setup

Click WAN Interface in the main Quick Setup screen to open the WAN Interface Quick Setup Wizard Welcome screen. Use these screens to configure an interface to connect to the Internet. Click Next.

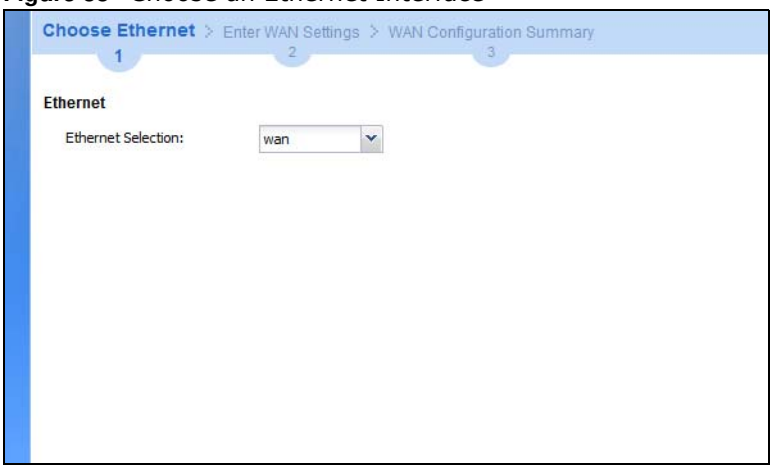
Figure 37 WAN Interface Quick Setup Wizard



4.2.1 Choose an Ethernet Interface

Select the Ethernet interface (names vary by model) that you want to configure for a WAN connection and click Next.

Figure 38 Choose an Ethernet Interface

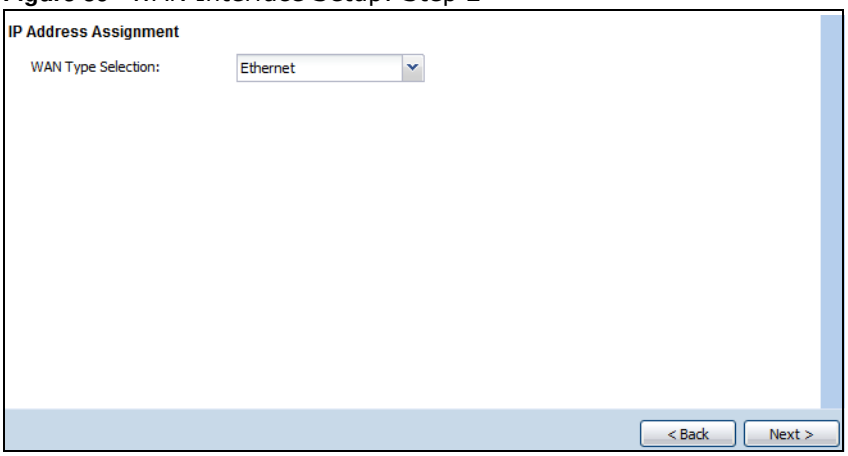


4.2.2 Select WAN Type

WAN Type Selection: Select the type of encapsulation this connection is to use. Choose Ethernet when the WAN port is used as a regular Ethernet.

Otherwise, choose PPPoE or PPTP for a dial-up connection according to the information from your ISP.

Figure 39 WAN Interface Setup: Step 2



The screens vary depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

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

4.2.3 Configure WAN IP Settings

Use this screen to select whether the interface should use a fixed or dynamic IP address.

Figure 40 WAN Interface Setup: Step 2 Dynamic IP

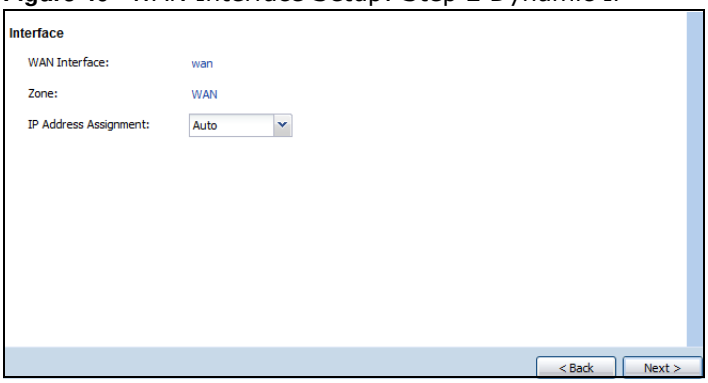
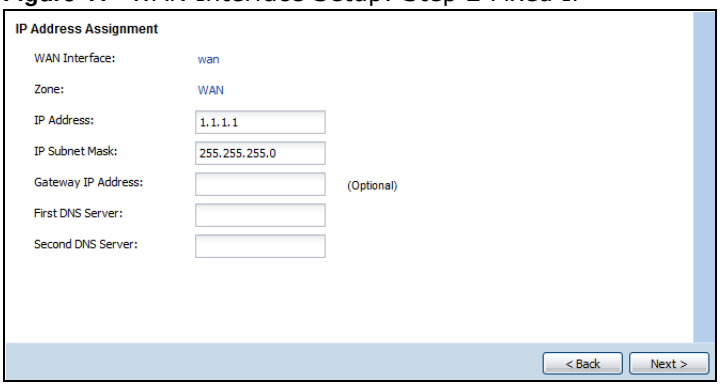


Figure 41 WAN Interface Setup: Step 2 Fixed IP



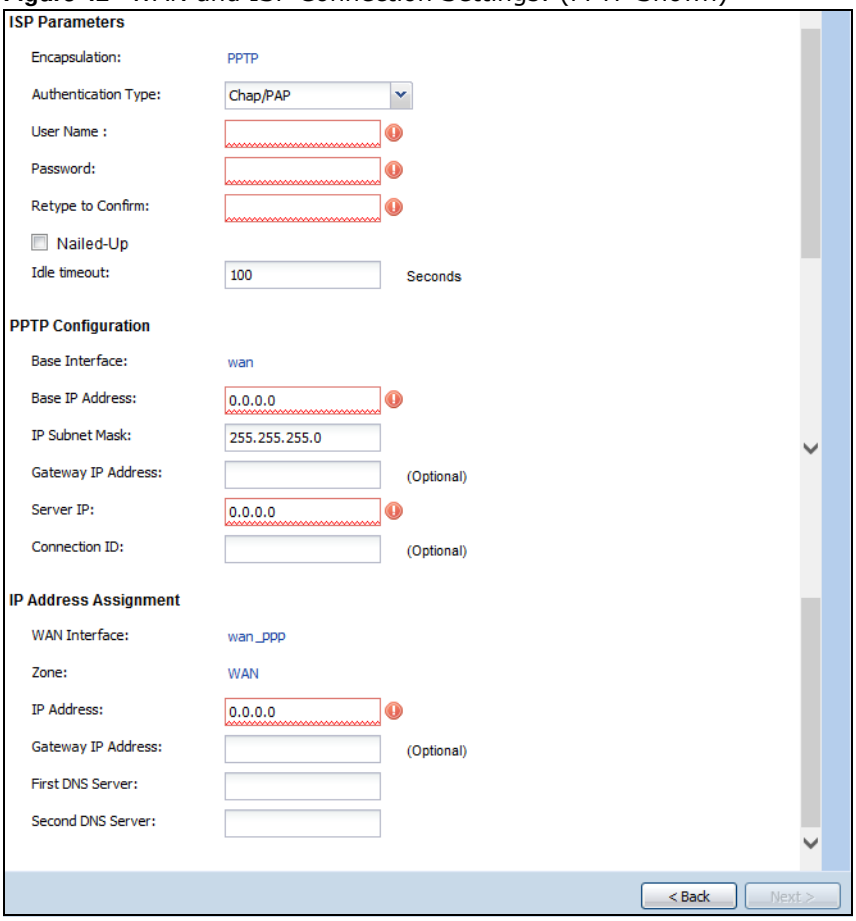
- WAN Interface: This is the interface you are configuring for Internet access.
- Zone: This is the security zone to which this interface and Internet connection belong.
- IP Address Assignment: Select Auto If your ISP did not assign you a fixed IP address. Select Static if you have a fixed IP address and enter the IP address, subnet mask, gateway IP address (optional) and DNS server IP address(es).

4.2.4 ISP and WAN and ISP Connection Settings

Use this screen to configure the ISP and WAN interface settings. This screen is read-only if you select Ethernet and set t the IP Address Assignment to AutoStatic. If you set the IP Address Assignment to static and/or select PPTP or PPPoE, enter the Internet access information exactly as your ISP gave it to you.

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

Figure 42 WAN and ISP Connection Settings: (PPTP Shown)



The following table describes the labels in this screen.

Table 14 WAN and ISP Connection Settings

LABEL	DESCRIPTION
ISP Parameter	This section appears if the interface uses a PPPoE or PPTP Internet connection.
Encapsulation	This displays the type of Internet connection you are configuring.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: CHAP/ PAP - Your USG accepts either CHAP or PAP when requested by this remote node. CHAP - Your USG accepts CHAP only. PAP - Your USG accepts PAP only. MSCHAP - Your USG accepts MSCHAP only. MSCHAP-V2 - Your USG accepts MSCHAP-V2 only.
User Name	Type the user name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select Nailed-Up if you do not want the connection to time out.

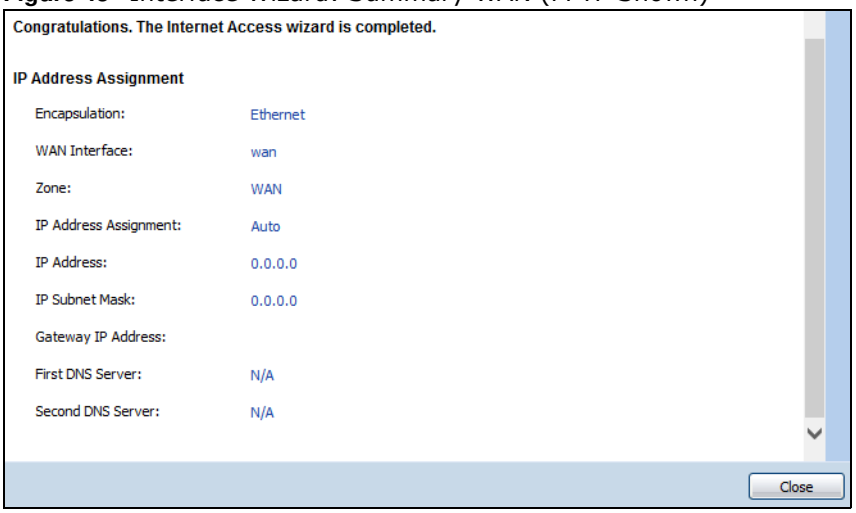
Table 14 WAN and ISP Connection Settings (continued)

LABEL	DESCRIPTION
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. 0 means no timeout.
PPTP Configuration	This section only appears if the interface uses a PPPoE or PPTP Internet connection.
Base Interface	This displays the identity of the Ethernet interface you configure to connect with a modem or router.
Base IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP	Type the IP address of the PPTP server.
Connection ID	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem. You can use alphanumeric and -_: characters, and it can be up to 31 characters long.
WAN Interface Setup	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	This field is read-only when the WAN interface uses a dynamic IP address. If your WAN interface uses a static IP address, enter it in this field.
First DNS Server Second DNS Server	These fields only display for an interface with a static IP address. Enter the DNS server IP address(es) in the field(s) to the right. Leave the field as 0.0.0.0 if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The USG uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.

4.2.5 Quick Setup Interface Wizard: Summary

This screen displays the WAN interface's settings.

Figure 43 Interface Wizard: Summary WAN (PPTP Shown)



The following table describes the labels in this screen.

Table 15 Interface Wizard: Summary WAN

LABEL	DESCRIPTION
Encapsulation	This displays what encapsulation this interface uses to connect to the Internet.
Service Name	This field only appears for a PPPoE interface. It displays the PPPoE service name specified in the ISP account.
Server IP	This field only appears for a PPTP interface. It displays the IP address of the PPTP server.
User Name	This is the user name given to you by your ISP.
Nailed-Up	If No displays the connection will not time out. Yes means the USG uses the idle timeout.
Idle Timeout	This is how many seconds the connection can be idle before the router automatically disconnects from the PPPoE server. 0 means no timeout.
Connection ID	If you specified a connection ID, it displays here.
WAN Interface	This identifies the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address Assignment	This field displays whether the WAN IP address is static or dynamic (Auto).
First DNS Server Second DNS Server	If the IP Address Assignment is Static, these fields display the DNS server IP address(es).
Close	Click Close to exit the wizard.

4.3 VPN Setup Wizard

Click VPN Setup in the main Quick Setup screen to open the VPN Setup Wizard Welcome screen.

Figure 44 VPN Setup Wizard

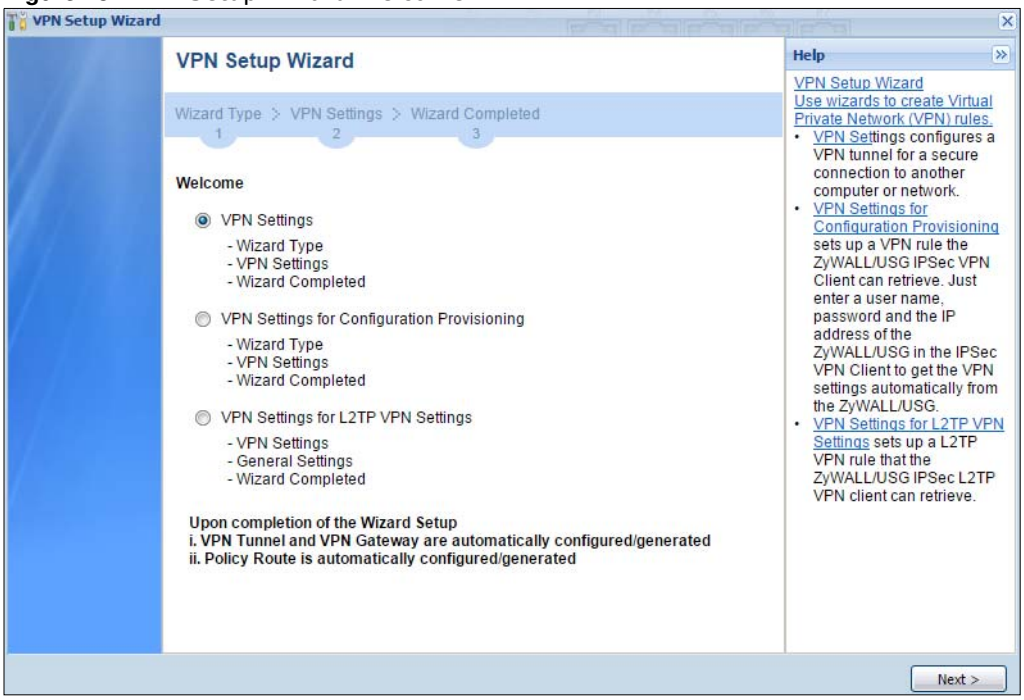


4.3.1 Welcome

Use wizards to create Virtual Private Network (VPN) rules. After you complete the wizard, the Phase 1 rule settings appear in the VPN > IPSec VPN > VPN Gateway screen and the Phase 2 rule settings appear in the VPN > IPSec VPN > VPN Connection screen.

- VPN Settings configures a VPN tunnel for a secure connection to another computer or network.
- VPN Settings for Configuration Provisioning sets up a VPN rule the USG IPSec VPN Client can retrieve. Just enter a user name, password and the IP address of the USG in the IPSec VPN Client to get the VPN settings automatically from the USG.
- VPN Settings for L2TP VPN Settings sets up a L2TP VPN rule that the USG IPSec L2TP VPN client can retrieve.

Figure 45 VPN Setup Wizard Welcome

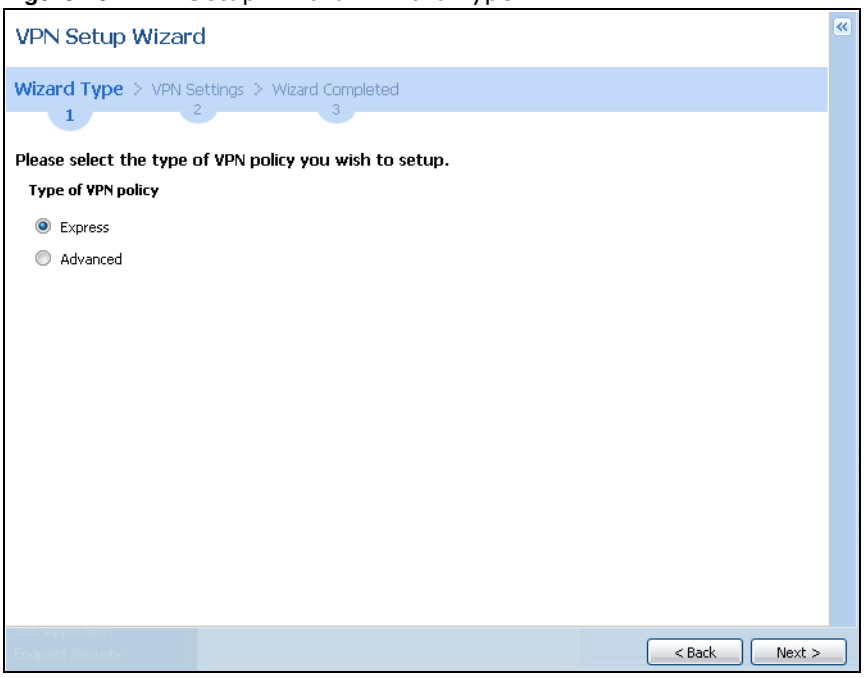


4.3.2 VPN Setup Wizard: Wizard Type

Choose Express to create a VPN rule with the default phase 1 and phase 2 settings to connect to another ZLD-based USG using a pre-shared key.

Choose Advanced to change the default settings and/or use certificates instead of a pre-shared key to create a VPN rule to connect to another IPSec device.

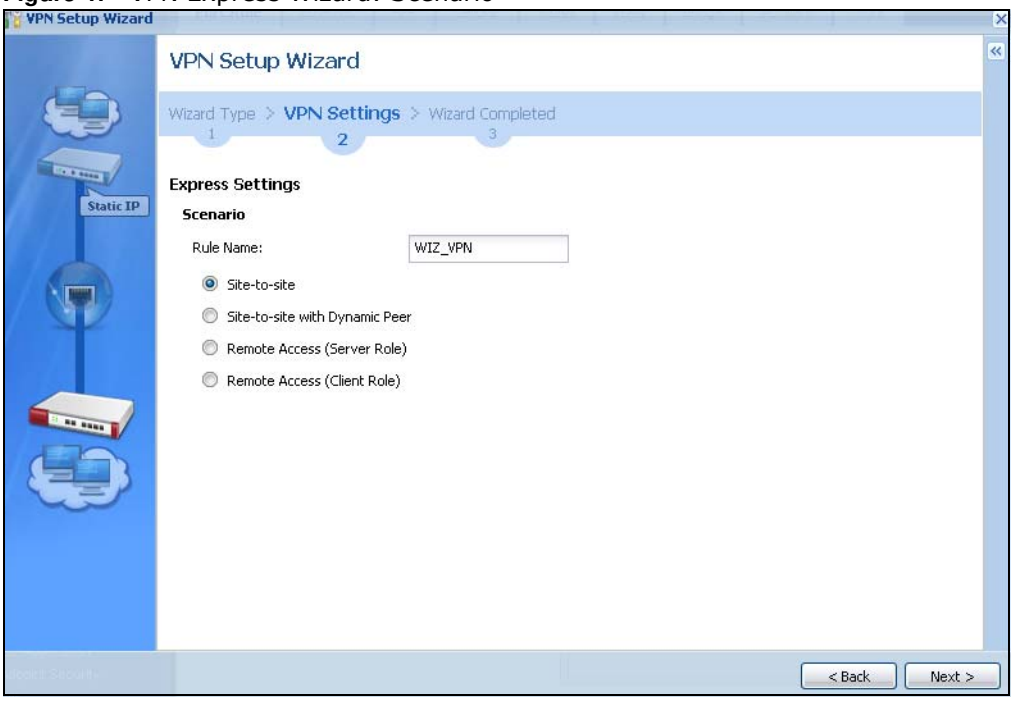
Figure 46 VPN Setup Wizard: Wizard Type



4.3.3 VPN Express Wizard - Scenario

Click the Express radio button as shown in Figure 46 on page 58 to display the following screen.

Figure 47 VPN Express Wizard: Scenario



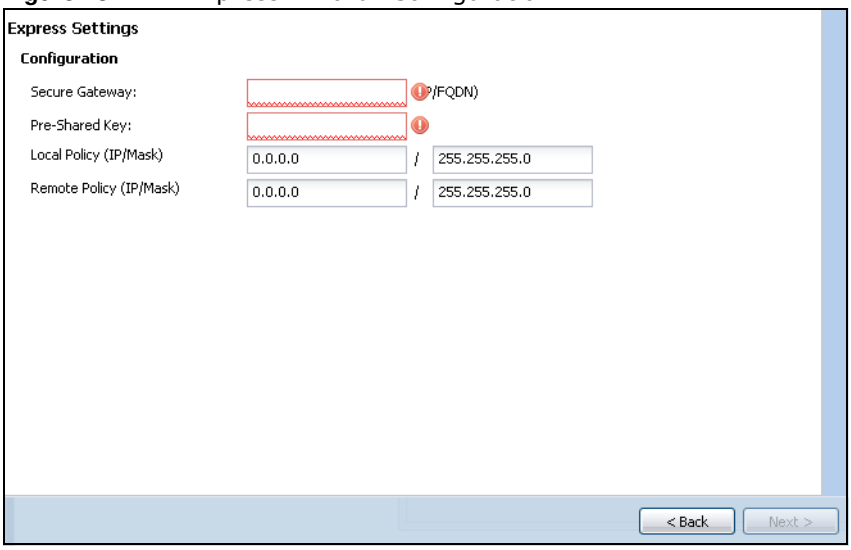
Rule Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- Site-to-site - The remote IPSec device has a static IP address or a domain name. This USG can initiate the VPN tunnel.
- Site-to-site with Dynamic Peer - The remote IPSec device has a dynamic IP address. Only the remote IPSec device can initiate the VPN tunnel.
- Remote Access (Server Role) - Allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
- Remote Access (Client Role) - Connect to an IPSec server. This USG is the client (dial-in user) and can initiate the VPN tunnel.

4.3.4 VPN Express Wizard - Configuration

Figure 48 VPN Express Wizard: Configuration

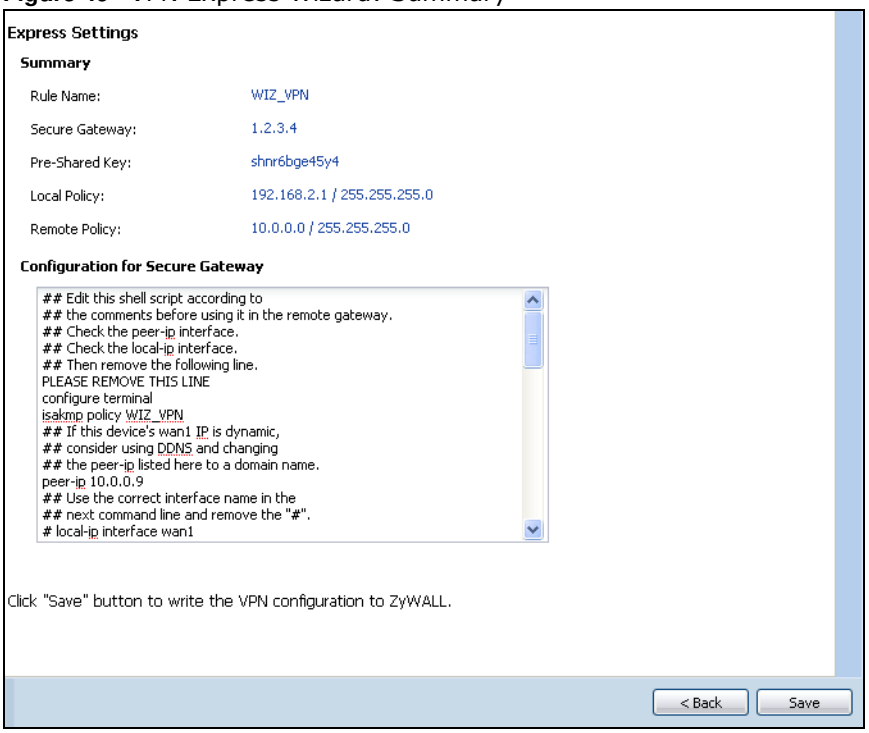


- Secure Gateway: Any displays in this field if it is not configurable for the chosen scenario. Otherwise, enter the WAN IP address or domain name of the remote IPSec device (secure gateway) to identify the remote IPSec router by its IP address or a domain name. Use 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address.
- Pre-Shared Key: Type the password. Both ends of the VPN tunnel must use the same password. Use 8 to 31 case-sensitive ASCII characters or 8 to 31 pairs of hexadecimal ("0-9", "A-F") characters. Proceed a hexadecimal key with "0x". You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
- Local Policy (IP/Mask): Type the IP address of a computer on your network that can use the tunnel. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
- Remote Policy (IP/Mask): Any displays in this field if it is not configurable for the chosen scenario. Otherwise, type the IP address of a computer behind the remote IPSec device. You can also specify a subnet. This must match the local IP address configured on the remote IPSec device.

4.3.5 VPN Express Wizard - Summary

This screen provides a read-only summary of the VPN tunnel's configuration and commands that you can copy and paste into another ZLD-based USG's command line interface to configure it.

Figure 49 VPN Express Wizard: Summary

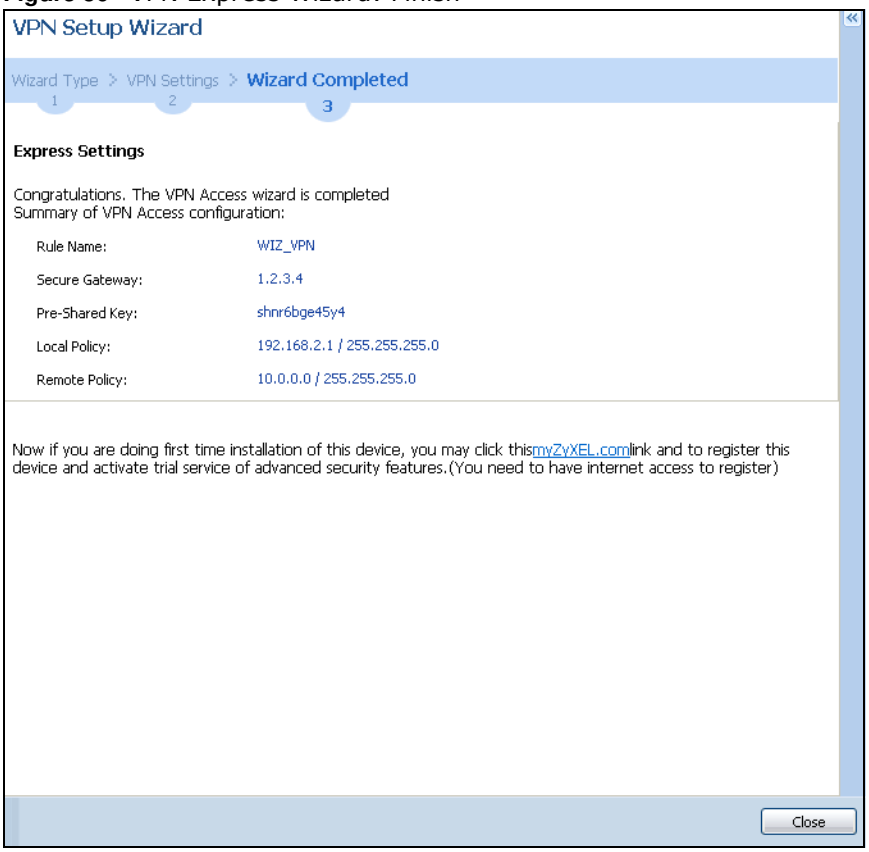


- Rule Name: Identifies the VPN gateway policy.
- Secure Gateway: IP address or domain name of the remote IPSec device. If this field displays Any, only the remote IPSec device can initiate the VPN connection.
- Pre-Shared Key: VPN tunnel password. It identifies a communicating party during a phase 1 IKE negotiation.
- Local Policy: IP address and subnet mask of the computers on the network behind your USG that can use the tunnel.
- Remote Policy: IP address and subnet mask of the computers on the network behind the remote IPSec device that can use the tunnel. If this field displays Any, only the remote IPSec device can initiate the VPN connection.
- Copy and paste the Configuration for Secure Gateway commands into another ZLD-based USG's command line interface to configure it to serve as the other end of this VPN tunnel. You can also use a text editor to save these commands as a shell script file with a ".zysh" filename extension. Use the file manager to run the script in order to configure the VPN connection. See the commands reference guide for details on the commands displayed in this list.

4.3.6 VPN Express Wizard - Finish

Now the rule is configured on the USG. The Phase 1 rule settings appear in the VPN > IPSec VPN > VPN Gateway screen and the Phase 2 rule settings appear in the VPN > IPSec VPN > VPN Connection screen.

Figure 50 VPN Express Wizard: Finish

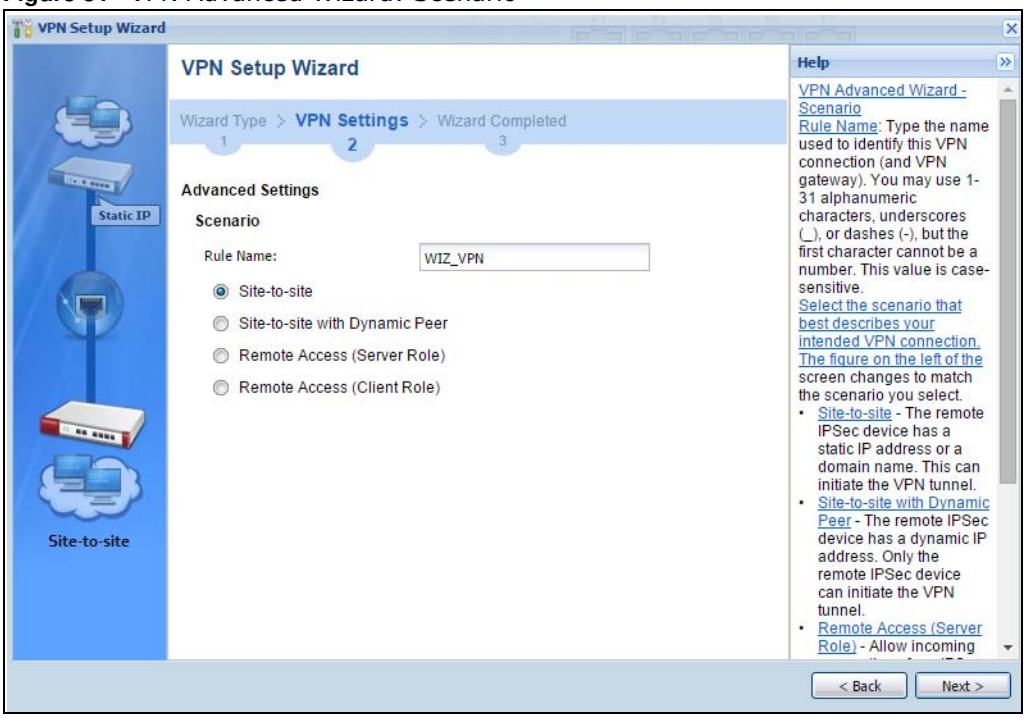


Click Close to exit the wizard.

4.3.7 VPN Advanced Wizard - Scenario

Click the Advanced radio button as shown in Figure 46 on page 58 to display the following screen.

Figure 51 VPN Advanced Wizard: Scenario



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

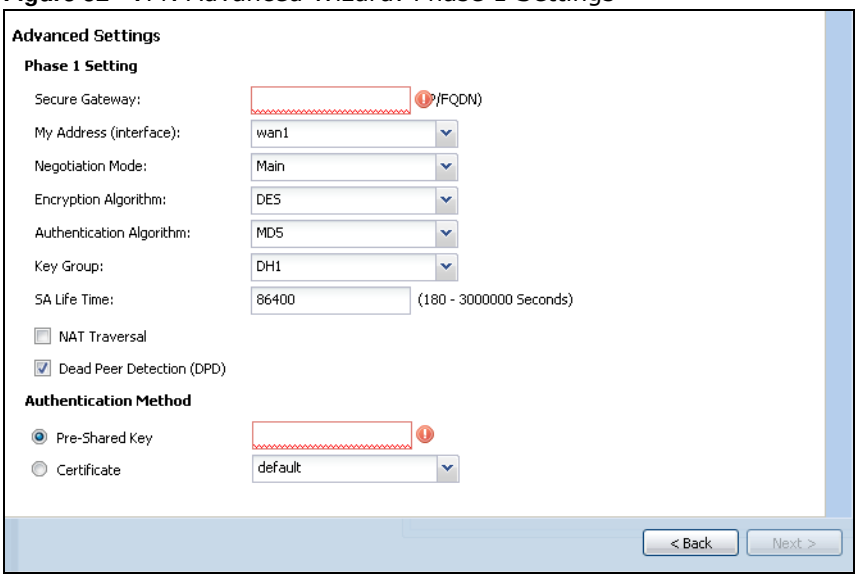
Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- Site-to-site - The remote IPSec device has a static IP address or a domain name. This USG can initiate the VPN tunnel.
- Site-to-site with Dynamic Peer - The remote IPSec device has a dynamic IP address. Only the remote IPSec device can initiate the VPN tunnel.
- Remote Access (Server Role) - Allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
- Remote Access (Client Role) - Connect to an IPSec server. This USG is the client (dial-in user) and can initiate the VPN tunnel.

4.3.8 VPN Advanced Wizard - Phase 1 Settings

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

Figure 52 VPN Advanced Wizard: Phase 1 Settings



- Secure Gateway: Any displays in this field if it is not configurable for the chosen scenario. Otherwise, enter the WAN IP address or domain name of the remote IPSec device (secure gateway) to identify the remote IPSec device by its IP address or a domain name. Use 0.0.0.0 if the remote IPSec device has a dynamic WAN IP address.
- My Address (interface): Select an interface from the drop-down list box to use on your USG.
- Negotiation Mode: This displays Main or Aggressive:
  - Main encrypts the USG's and remote IPSec router's identities but takes more time to establish the IKE SA
  - Aggressive is faster but does not encrypt the identities.

The USG and the remote IPSec router must use the same negotiation mode. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

- Encryption Algorithm: 3DES and AES use encryption. The longer the key, the higher the security (this may affect throughput). Both sender and receiver must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. AES128 uses a 128-bit key and is faster than 3DES. AES192 uses a 192-bit key, and AES256 uses a 256-bit key.
- Authentication Algorithm: MD5 gives minimal security and SHA512 gives the highest security. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The stronger the algorithm the slower it is.
- Key Group: DH5 is more secure than DH1 or DH2 (although it may affect throughput). DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number.
- SA Life Time: Set how often the USG renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- NAT Traversal: Select this if the VPN tunnel must pass through NAT (there is a NAT router between the IPSec devices).

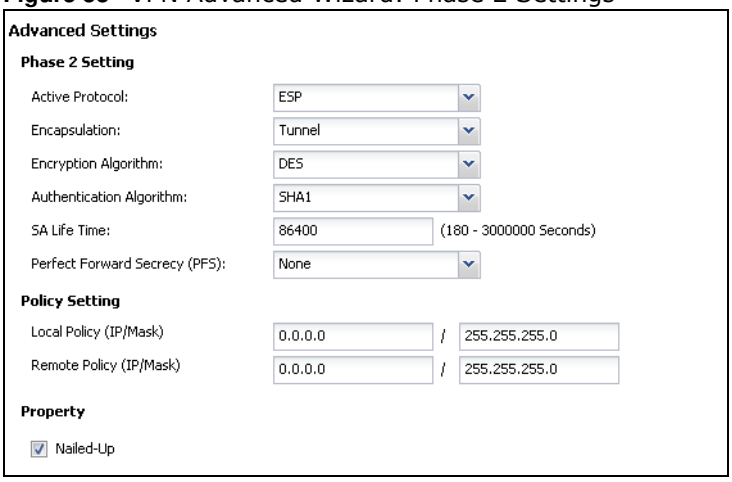
Note: The remote IPSec device must also have NAT traversal enabled. See the help in the main IPSec VPN screens for more information.

- Dead Peer Detection (DPD) has the USG make sure the remote IPSec device is there before transmitting data through the IKE SA. If there has been no traffic for at least 15 seconds, the USG sends a message to the remote IPSec device. If it responds, the USG transmits the data. If it does not respond, the USG shuts down the IKE SA.
- Authentication Method: Select Pre-Shared Key to use a password or Certificate to use one of the USG's certificates.

4.3.9 VPN Advanced Wizard - Phase 2

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

Figure 53 VPN Advanced Wizard: Phase 2 Settings

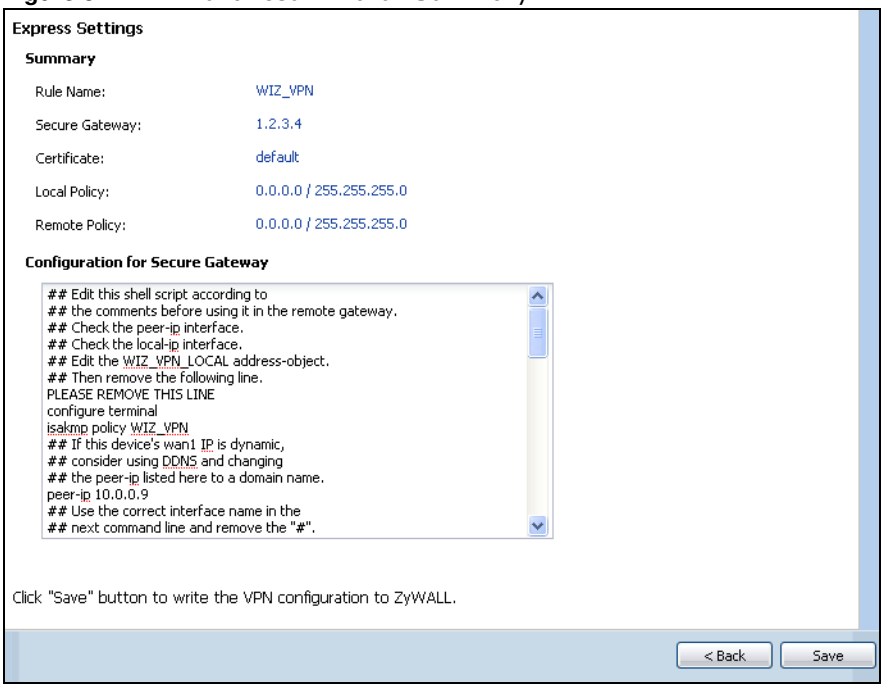


- Active Protocol: ESP is compatible with NAT, AH is not.
- Encapsulation: Tunnel is compatible with NAT, Transport is not.
- Encryption Algorithm: 3DES and AES use encryption. The longer the AES key, the higher the security (this may affect throughput). Null uses no encryption.
- Authentication Algorithm: MD5 gives minimal security and SHA512 gives the highest security. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The stronger the algorithm the slower it is.
- SA Life Time: Set how often the USG renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- Perfect Forward Secrecy (PFS): Disabling PFS allows faster IPSec setup, but is less secure. Select DH1, DH2 or DH5 to enable PFS. DH5 is more secure than DH1 or DH2 (although it may affect throughput). DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number (more secure, yet slower).
- Local Policy (IP/Mask): Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
- Remote Policy (IP/Mask): Type the IP address of a computer behind the remote IPSec device. You can also specify a subnet. This must match the local IP address configured on the remote IPSec device.
- Nailed-Up: This displays for the site-to-site and remote access client role scenarios. Select this to have the USG automatically renegotiate the IPSec SA when the SA life time expires.

4.3.10 VPN Advanced Wizard - Summary

This is a read-only summary of the VPN tunnel settings.

Figure 54 VPN Advanced Wizard: Summary

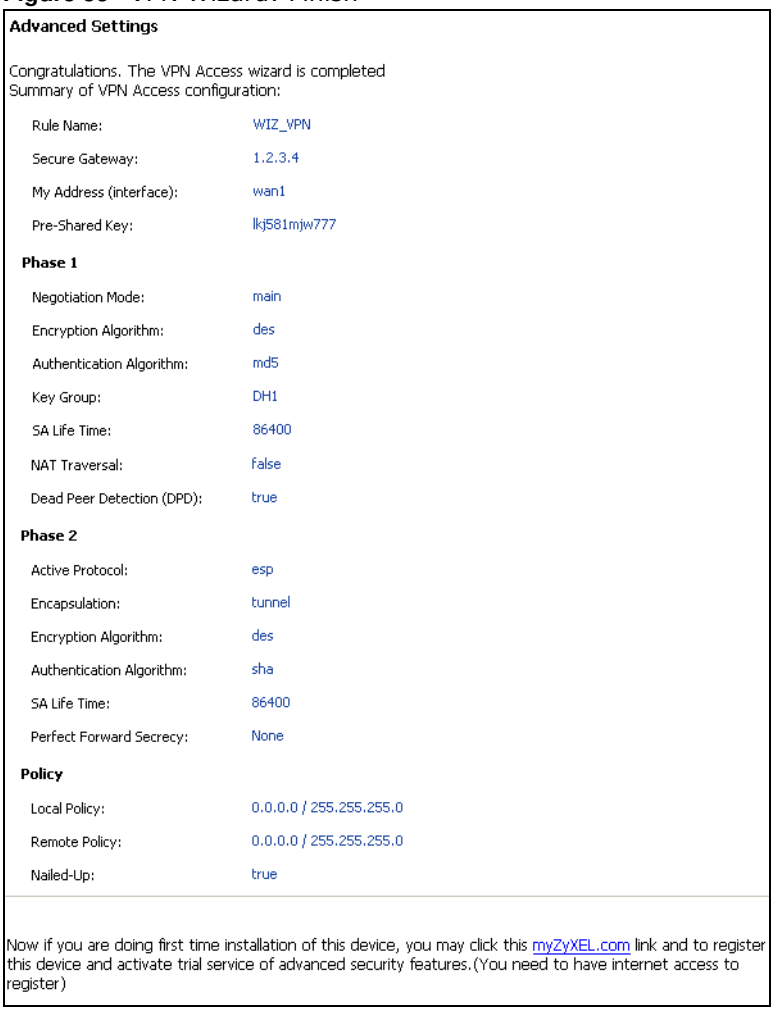


- Rule Name: Identifies the VPN connection (and the VPN gateway).
- Secure Gateway: IP address or domain name of the remote IPSec device.
- Pre-Shared Key: VPN tunnel password.
- Certificate: The certificate the USG uses to identify itself when setting up the VPN tunnel.
- Local Policy: IP address and subnet mask of the computers on the network behind your USG that can use the tunnel.
- Remote Policy: IP address and subnet mask of the computers on the network behind the remote IPSec device that can use the tunnel.
- Copy and paste the Configuration for Remote Gateway commands into another ZLD-based USG's command line interface.
- Click Save to save the VPN rule.

4.3.11 VPN Advanced Wizard - Finish

Now the rule is configured on the USG. The Phase 1 rule settings appear in the VPN > IPSec VPN > VPN Gateway screen and the Phase 2 rule settings appear in the VPN > IPSec VPN > VPN Connection screen.

Figure 55 VPN Wizard: Finish



Click Close to exit the wizard.

4.4 VPN Settings for Configuration Provisioning Wizard: Wizard Type

Use VPN Settings for Configuration Provisioning to set up a VPN rule that can be retrieved with the USG IPSec VPN Client.

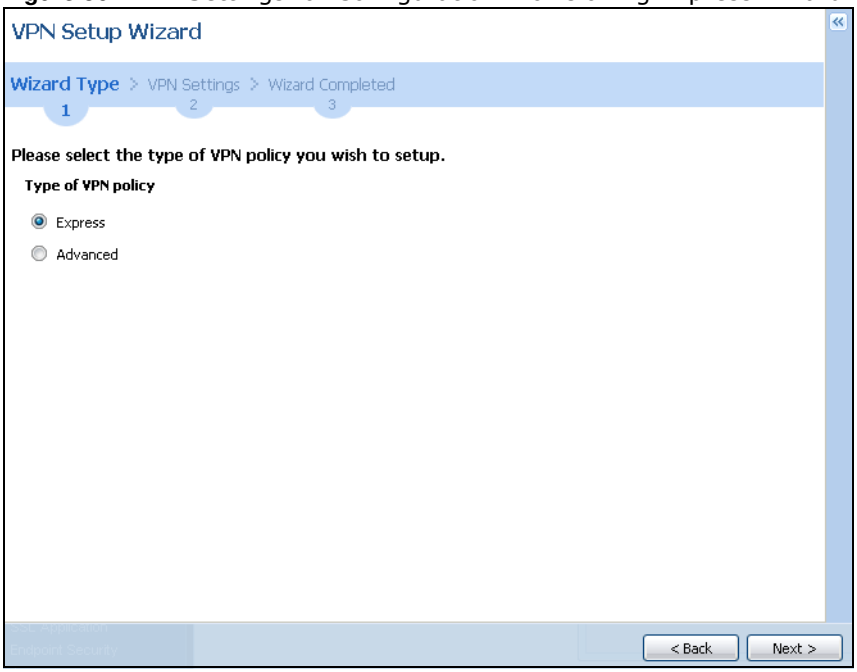
VPN rules for the USG IPSec VPN Client have certain restrictions. They must *not* contain the following settings:

- AH active protocol
- NULL encryption
- SHA512 authentication
- A subnet or range remote policy

Choose Express to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key.

Choose Advanced to change the default settings and/or use certificates instead of a pre-shared key in the VPN rule.

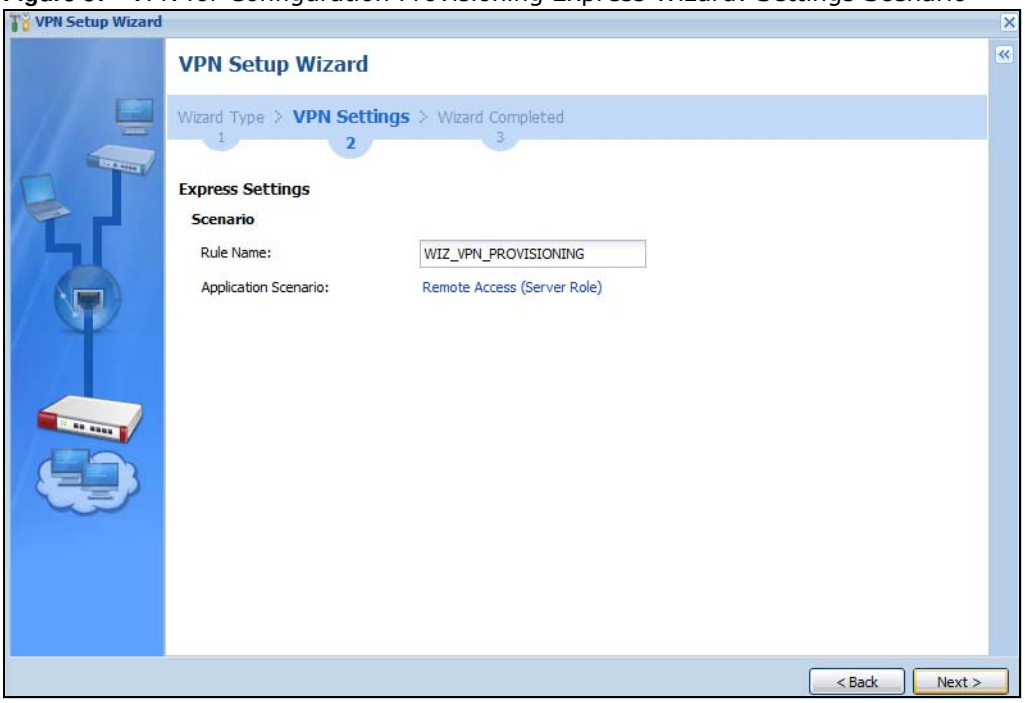
Figure 56 VPN Settings for Configuration Provisioning Express Wizard: Wizard Type



4.4.1 Configuration Provisioning Express Wizard - VPN Settings

Click the Express radio button as shown in the previous screen to display the following screen.

Figure 57 VPN for Configuration Provisioning Express Wizard: Settings Scenario



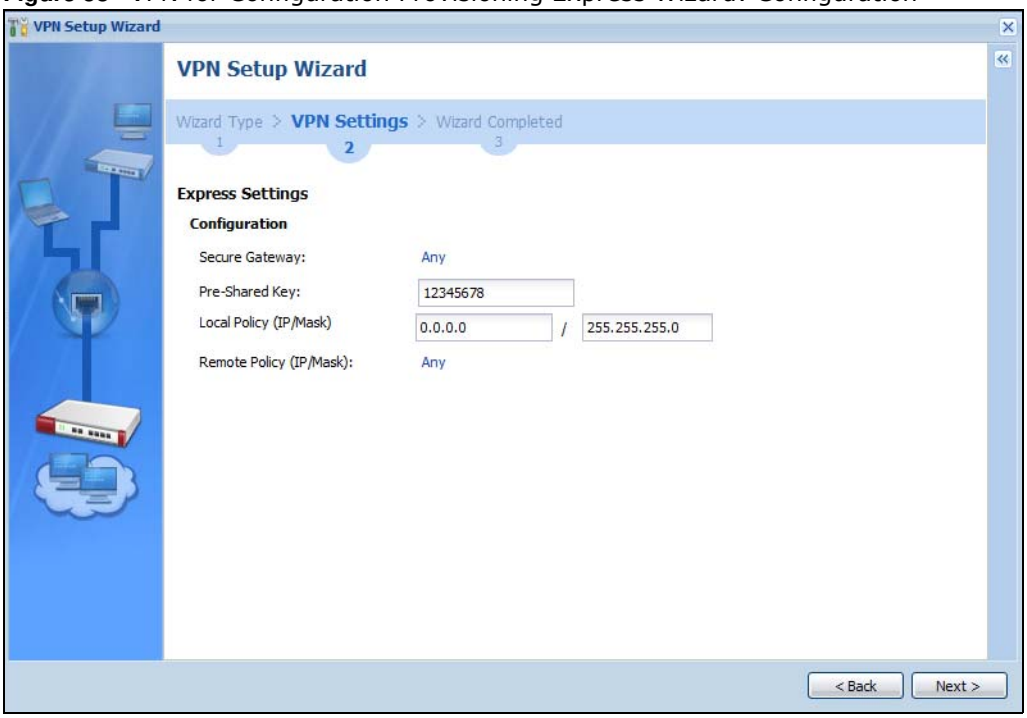
Rule Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Application Scenario: Only the Remote Access (Server Role) is allowed in this wizard. It allows incoming connections from the USG IPSec VPN Client.

4.4.2 Configuration Provisioning VPN Express Wizard - Configuration

Click Next to continue the wizard.

Figure 58 VPN for Configuration Provisioning Express Wizard: Configuration

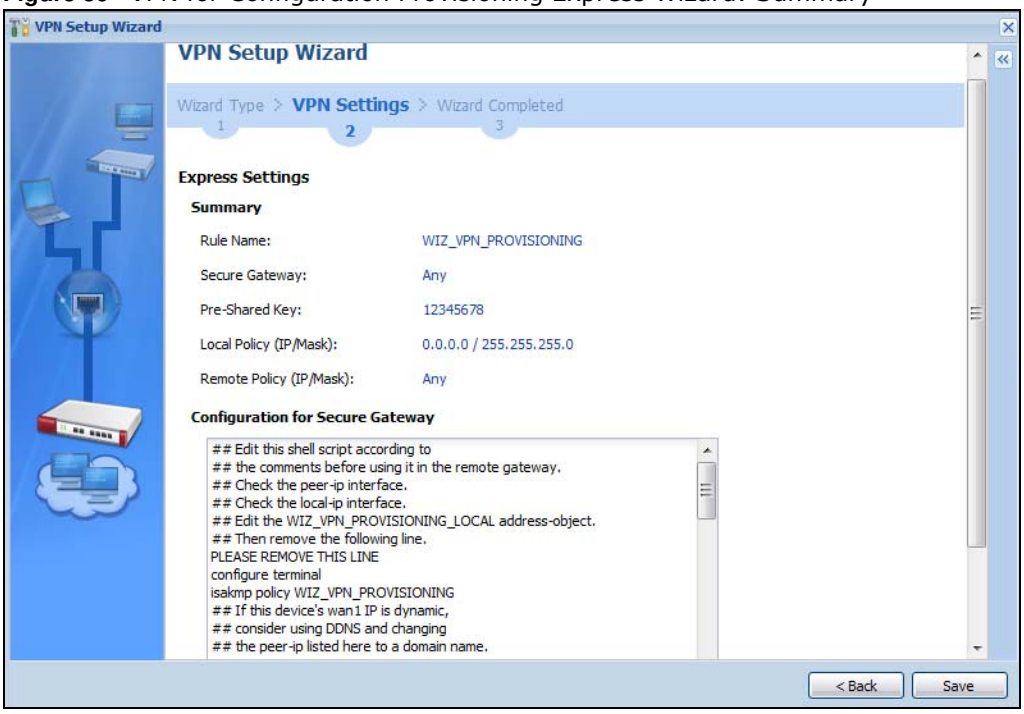


- Secure Gateway: Any displays in this field because it is not configurable in this wizard. It allows incoming connections from the USG IPSec VPN Client.
- Pre-Shared Key: Type the password. Both ends of the VPN tunnel must use the same password. Use 8 to 31 case-sensitive ASCII characters or 8 to 31 pairs of hexadecimal ("0-9", "A-F") characters. Proceed a hexadecimal key with "0x". You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
- Local Policy (IP/Mask): Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
- Remote Policy (IP/Mask): Any displays in this field because it is not configurable in this wizard.

4.4.3 VPN Settings for Configuration Provisioning Express Wizard - Summary

This screen has a read-only summary of the VPN tunnel's configuration and commands you can copy and paste into another ZLD-based USG's command line interface to configure it.

Figure 59 VPN for Configuration Provisioning Express Wizard: Summary

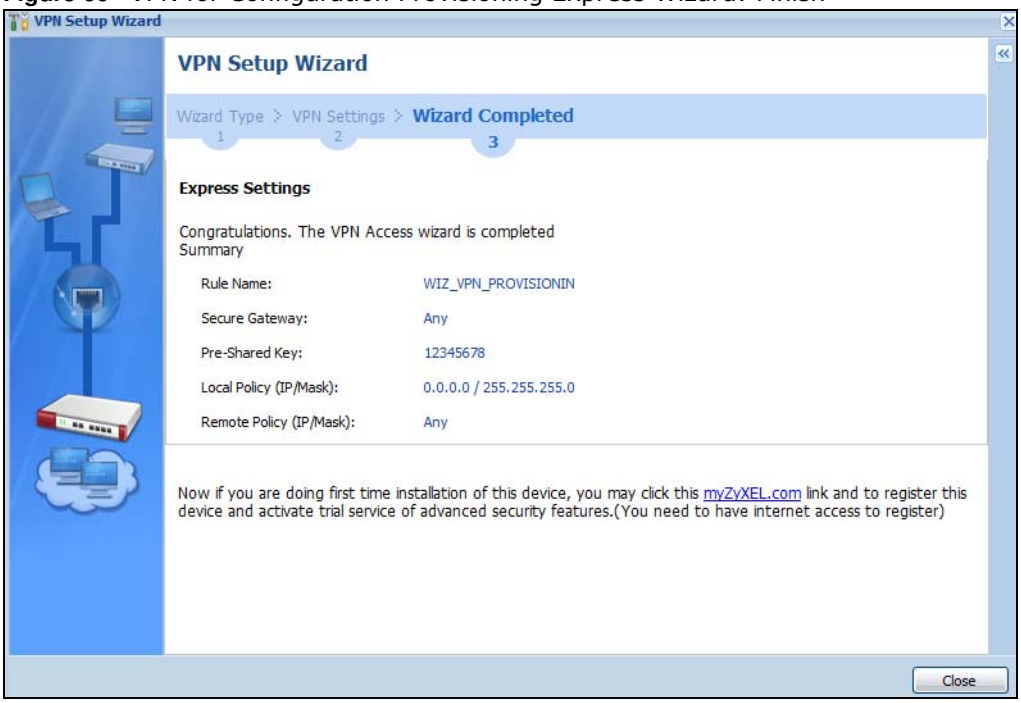


- Rule Name: Identifies the VPN gateway policy.
- Secure Gateway: Any displays in this field because it is not configurable in this wizard. It allows incoming connections from the USG IPSec VPN Client.
- Pre-Shared Key: VPN tunnel password. It identifies a communicating party during a phase 1 IKE negotiation.
- Local Policy: (Static) IP address and subnet mask of the computers on the network behind your USG that can be accessed using the tunnel.
- Remote Policy: Any displays in this field because it is not configurable in this wizard.
- The Configuration for Secure Gateway displays the configuration that the USG IPSec VPN Client will get from the USG.
- Click Save to save the VPN rule.

4.4.4 VPN Settings for Configuration Provisioning Express Wizard - Finish

Now the rule is configured on the USG. The Phase 1 rule settings appear in the VPN > IPSec VPN > VPN Gateway screen and the Phase 2 rule settings appear in the VPN > IPSec VPN > VPN Connection screen. Enter the IP address of the USG in the USG IPSec VPN Client to get all these VPN settings automatically from the USG.

Figure 60 VPN for Configuration Provisioning Express Wizard: Finish

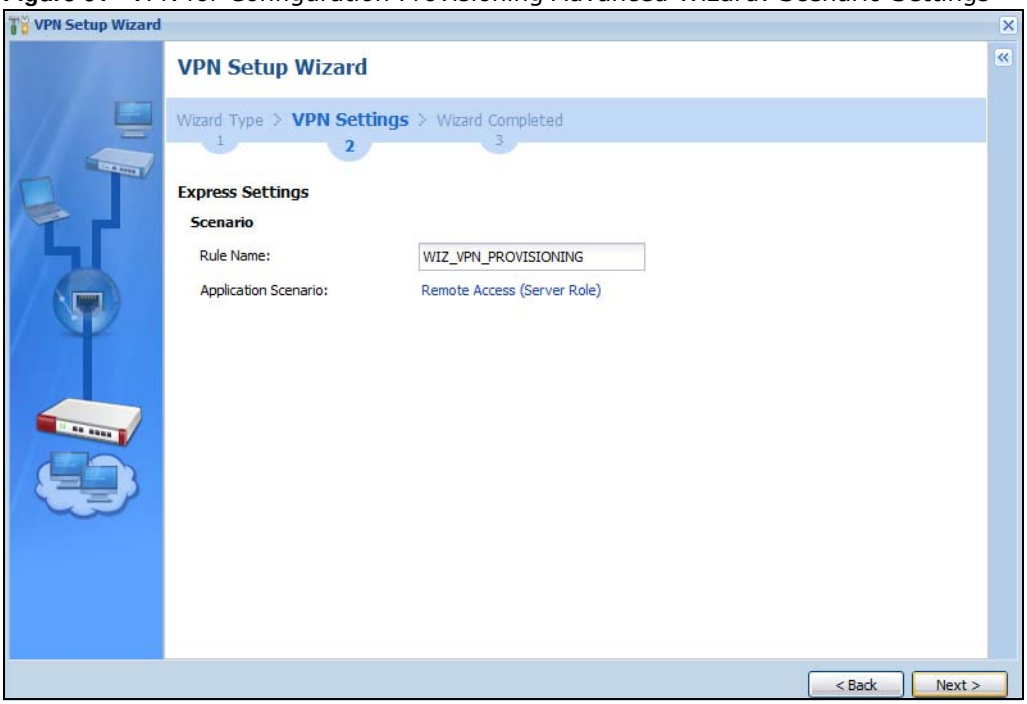


Click Close to exit the wizard.

4.4.5 VPN Settings for Configuration Provisioning Advanced Wizard - Scenario

Click the Advanced radio button as shown in the screen shown in Figure 56 on page 68 to display the following screen.

Figure 61 VPN for Configuration Provisioning Advanced Wizard: Scenario Settings



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

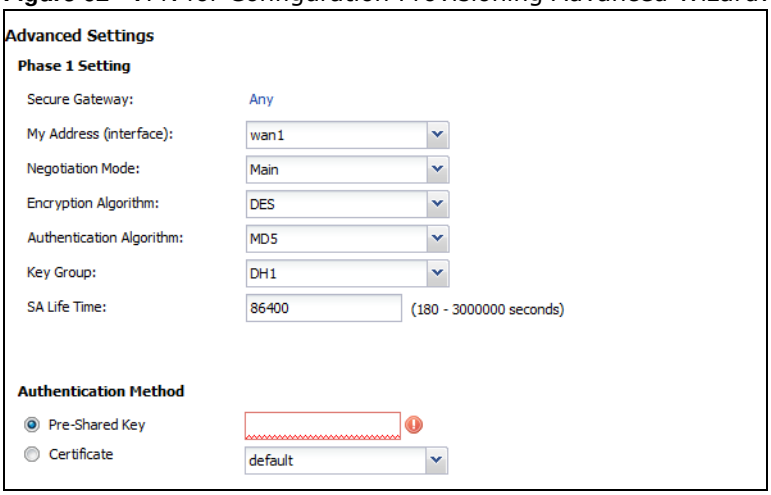
Application Scenario: Only the Remote Access (Server Role) is allowed in this wizard. It allows incoming connections from the USG IPSec VPN Client.

Click Next to continue the wizard.

4.4.6 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 1 Settings

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

Figure 62 VPN for Configuration Provisioning Advanced Wizard: Phase 1 Settings



- Secure Gateway: Any displays in this field because it is not configurable in this wizard. It allows incoming connections from the USG IPSec VPN Client.
- My Address (interface): Select an interface from the drop-down list box to use on your USG.
- Negotiation Mode:This displays Main or Aggressive:
  - Main encrypts the USG's and remote IPSec router's identities but takes more time to establish the IKE SA
  - Aggressive is faster but does not encrypt the identities.

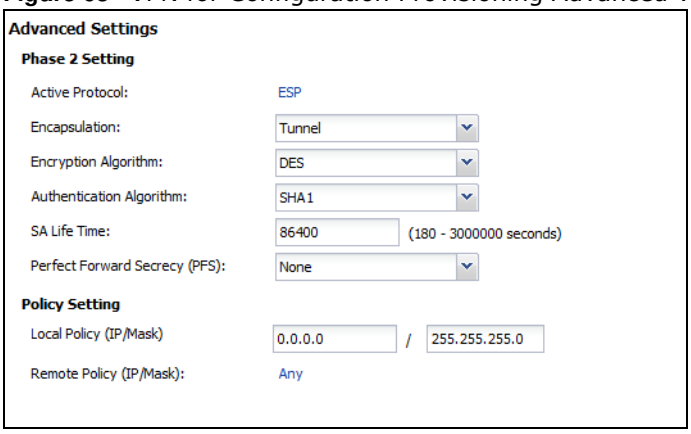
The USG and the remote IPSec router must use the same negotiation mode. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

- Encryption Algorithm: 3DES and AES use encryption. The longer the key, the higher the security (this may affect throughput). Both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. AES128 uses a 128-bit key and is faster than 3DES. AES192 uses a 192-bit key and AES256 uses a 256-bit key.
- Authentication Algorithm: MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. MD5 gives minimal security. SHA1 gives higher security and SHA256 gives the highest security. The stronger the algorithm, the slower it is.
- Key Group: DH5 is more secure than DH1 or DH2 (although it may affect throughput). DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number.
- SA Life Time: Set how often the USG renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- Authentication Method: Select Pre-Shared Key to use a password or Certificate to use one of the USG's certificates.

4.4.7 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 2

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

Figure 63 VPN for Configuration Provisioning Advanced Wizard: Phase 2 Settings

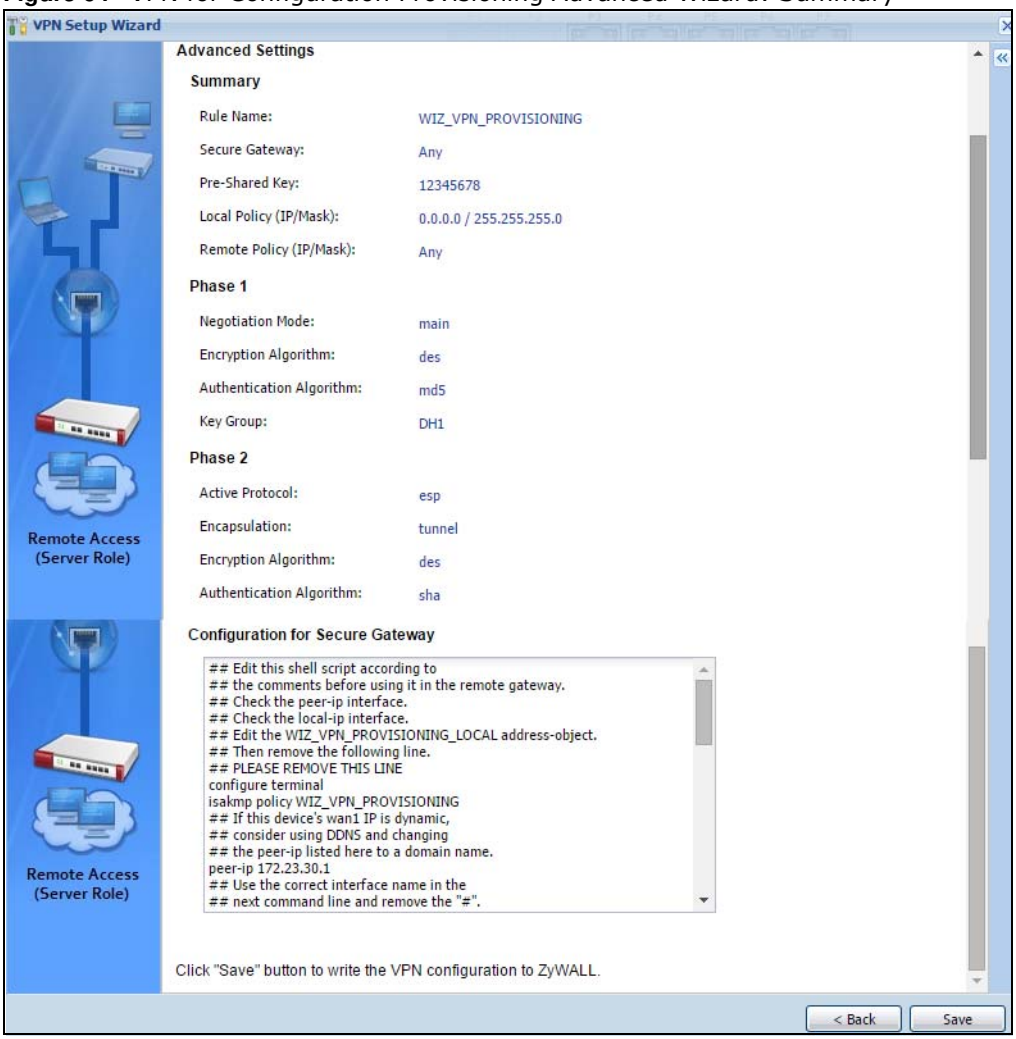


- Active Protocol: ESP is compatible with NAT. AH is not available in this wizard.
- Encapsulation: Tunnel is compatible with NAT, Transport is not.
- Encryption Algorithm: 3DES and AES use encryption. The longer the AES key, the higher the security (this may affect throughput). Null uses no encryption.
- Authentication Algorithm: MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. MD5 gives minimal security. SHA1 gives higher security and SHA256 gives the highest security. The stronger the algorithm, the slower it is.
- SA Life Time: Set how often the USG renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- Perfect Forward Secrecy (PFS): Disabling PFS allows faster IPSec setup, but is less secure. Select DH1, DH2 or DH5 to enable PFS. DH5 is more secure than DH1 or DH2 (although it may affect throughput). DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number (more secure, yet slower).
- Local Policy (IP/Mask): Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
- Remote Policy (IP/Mask): Any displays in this field because it is not configurable in this wizard.
- Nailed-Up: This displays for the site-to-site and remote access client role scenarios. Select this to have the USG automatically renegotiate the IPSec SA when the SA life time expires.

4.4.8 VPN Settings for Configuration Provisioning Advanced Wizard - Summary

This is a read-only summary of the VPN tunnel settings.

Figure 64 VPN for Configuration Provisioning Advanced Wizard: Summary



Summary

- Rule Name: Identifies the VPN connection (and the VPN gateway).
- Secure Gateway: Any displays in this field because it is not configurable in this wizard. It allows incoming connections from the USG IPSec VPN Client.
- Pre-Shared Key: VPN tunnel password.
- Local Policy: IP address and subnet mask of the computers on the network behind your USG that can use the tunnel.
- Remote Policy: Any displays in this field because it is not configurable in this wizard.

Phase 1

- Negotiation Mode: This displays Main or Aggressive:
  - Main encrypts the USG's and remote IPSec router's identities but takes more time to establish the IKE SA
  - Aggressive is faster but does not encrypt the identities.

The USG and the remote IPSec router must use the same negotiation mode. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

- Encryption Algorithm: This displays the encryption method used. The longer the key, the higher the security, the lower the throughput (possibly).
  - DES uses a 56-bit key.
  - 3DES uses a 168-bit key.
  - AES128 uses a 128-bit key
  - AES192 uses a 192-bit key
  - AES256 uses a 256-bit key.
- Authentication Algorithm: This displays the authentication algorithm used. The stronger the algorithm, the slower it is.
  - MD5 gives minimal security.
  - SHA1 gives higher security
  - SHA256 gives the highest security.
- Key Group: This displays the Diffie-Hellman (DH) key group used. DH5 is more secure than DH1 or DH2 (although it may affect throughput).
  - DH1 uses a 768 bit random number.
  - DH2 uses a 1024 bit (1Kb) random number.
  - DH5 uses a 1536 bit random number.

Phase 2

- Active Protocol: This displays ESP (compatible with NAT) or AH.
- Encapsulation: This displays Tunnel (compatible with NAT) or Transport.
- Encryption Algorithm: This displays the encryption method used. The longer the key, the higher the security, the lower the throughput (possibly).
  - DES uses a 56-bit key.
  - 3DES uses a 168-bit key.
  - AES128 uses a 128-bit key
  - AES192 uses a 192-bit key
  - AES256 uses a 256-bit key.
  - Null uses no encryption.
- Authentication Algorithm: This displays the authentication algorithm used. The stronger the algorithm, the slower it is.
  - MD5 gives minimal security.
  - SHA1 gives higher security
  - SHA256 gives the highest security..

The Configuration for Secure Gateway displays the configuration that the USG IPSec VPN Client will get from the USG.

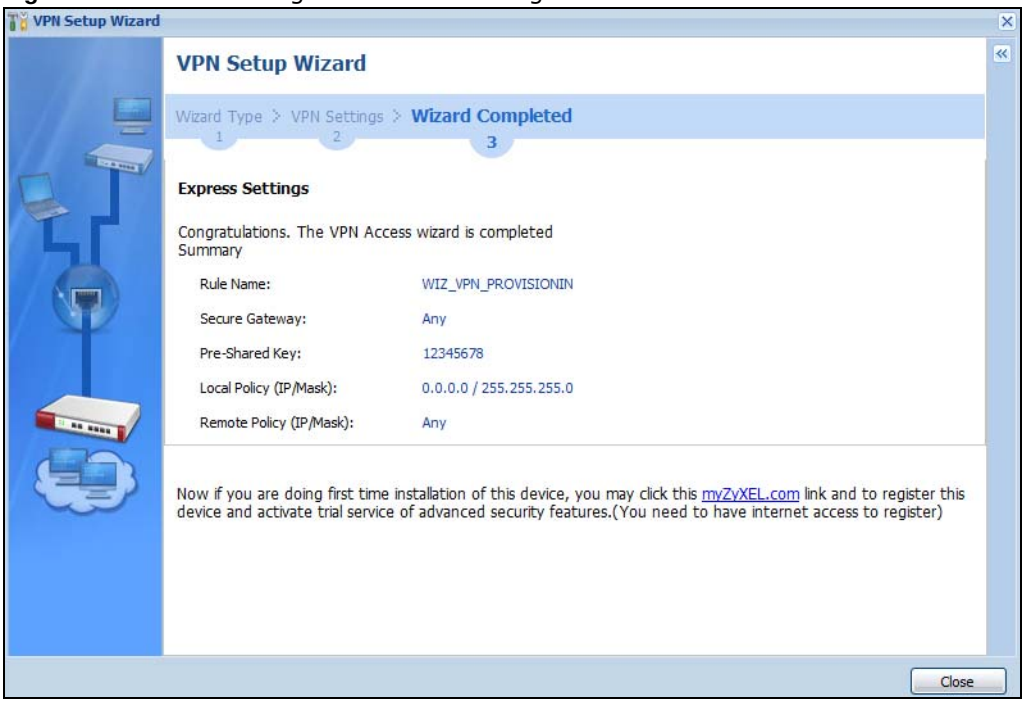
Click Save to save the VPN rule.

4.4.9 VPN Settings for Configuration Provisioning Advanced Wizard- Finish

Now the rule is configured on the USG. The Phase 1 rule settings appear in the VPN > IPSec VPN > VPN Gateway screen and the Phase 2 rule settings appear in the VPN > IPSec VPN > VPN

Connection screen. Enter the IP address of the USG in the USG IPSec VPN Client to get all these VPN settings automatically from the USG.

Figure 65 VPN for Configuration Provisioning Advanced Wizard: Finish

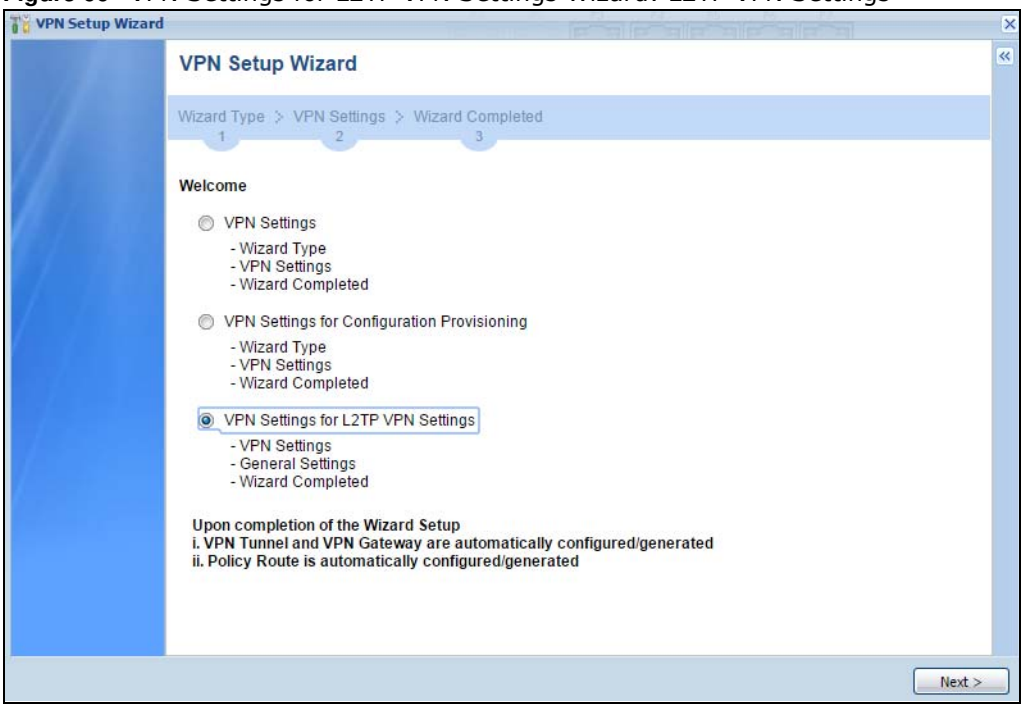


Click Close to exit the wizard.

4.5 VPN Settings for L2TP VPN Settings Wizard

Use VPN Settings for L2TP VPN Settings to set up an L2TP VPN rule. Click Configuration > Quick Setup > VPN Settings and select VPN Settings for L2TP VPN Settings to see the following screen.

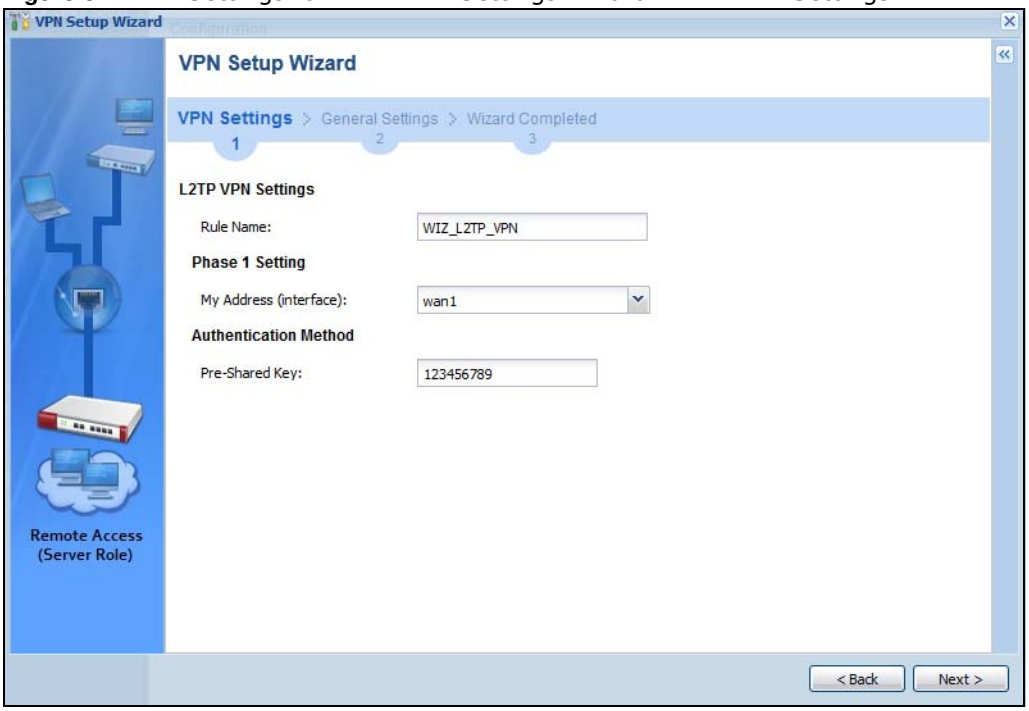
Figure 66 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings



Click Next to continue the wizard.

4.5.1 L2TP VPN Settings

Figure 67 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings



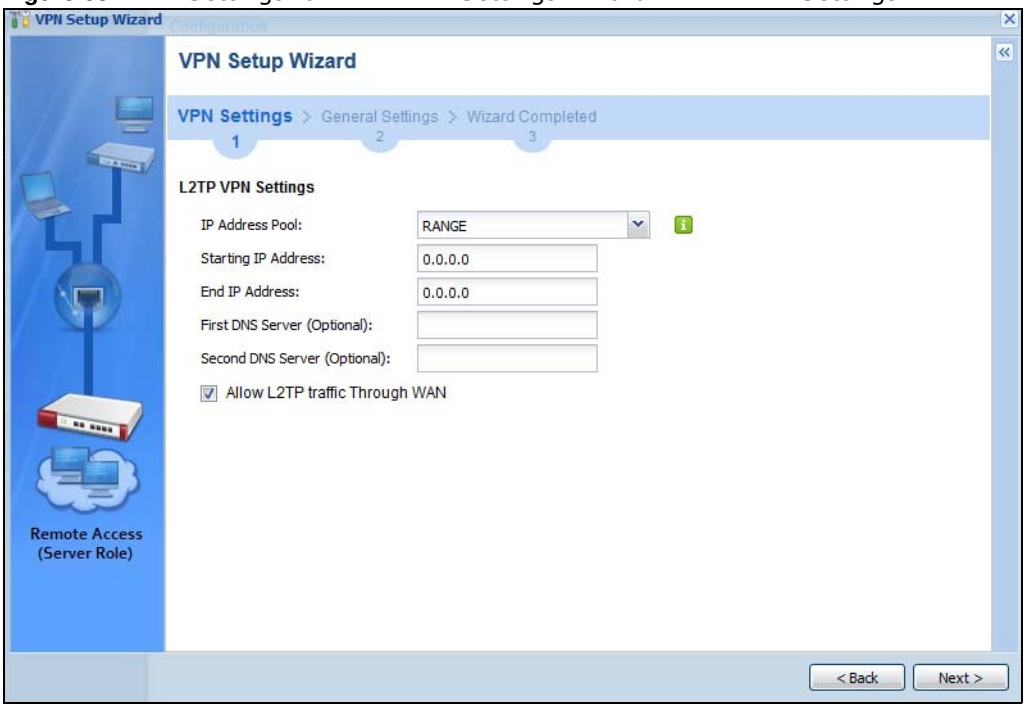
- Rule Name: Type the name used to identify this L2TP VPN connection (and L2TP VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

- My Address (interface): Select one of the interfaces from the pull down menu to apply the L2TP VPN rule.
- Pre-Shared Key: Type the password. Both ends of the VPN tunnel must use the same password. Use 8 to 31 case-sensitive ASCII characters or 8 to 31 pairs of hexadecimal ("0-9", "A-F") characters. Proceed a hexadecimal key with "0x". You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.

Click Next to continue the wizard.

4.5.2 L2TP VPN Settings

Figure 68 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings



- IP Address Pool: Select Range or Subnet from the pull down menu. This IP address pool is used to assign to the L2TP VPN clients.
- Starting IP Address: Enter the starting IP address in the field.
- End IP Address: Enter the ending IP address in the field.
- First DNS Server (Optional): Enter the first DNS server IP address in the field. Leave the filed as 0.0.0.0 if you do not want to configure DNS servers. If you do not configure a DNS server you must know the IP address of a machine in order to access it.
- Second DNS Server (Optional):Enter the second DNS server IP address in the field. Leave the filed as 0.0.0.0 if you do not want to configure DNS servers. If you do not configure a DNS server you must know the IP address of a machine in order to access it.
- Allow L2TP traffic Through WAN: Select this check box to allow traffic from L2TP clients to go to the Internet.

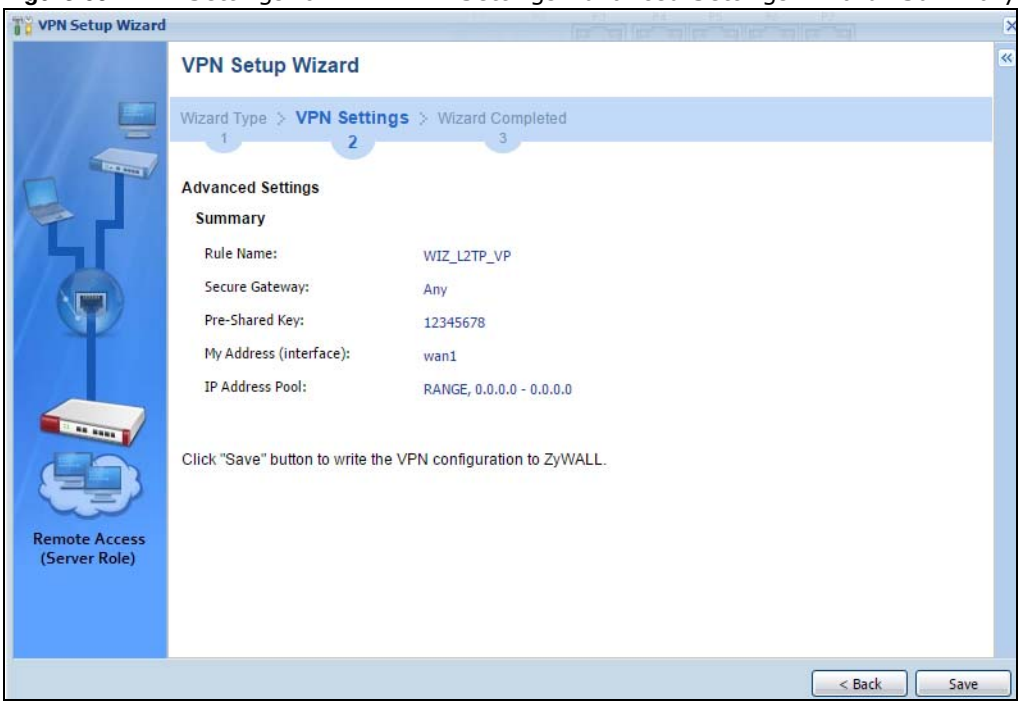
Click Next to continue the wizard.

Note: DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The USG uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.

4.5.3 VPN Settings for L2TP VPN Setting Wizard - Summary

This is a read-only summary of the L2TP VPN settings.

Figure 69 VPN Settings for L2TP VPN Settings Advanced Settings Wizard: Summary



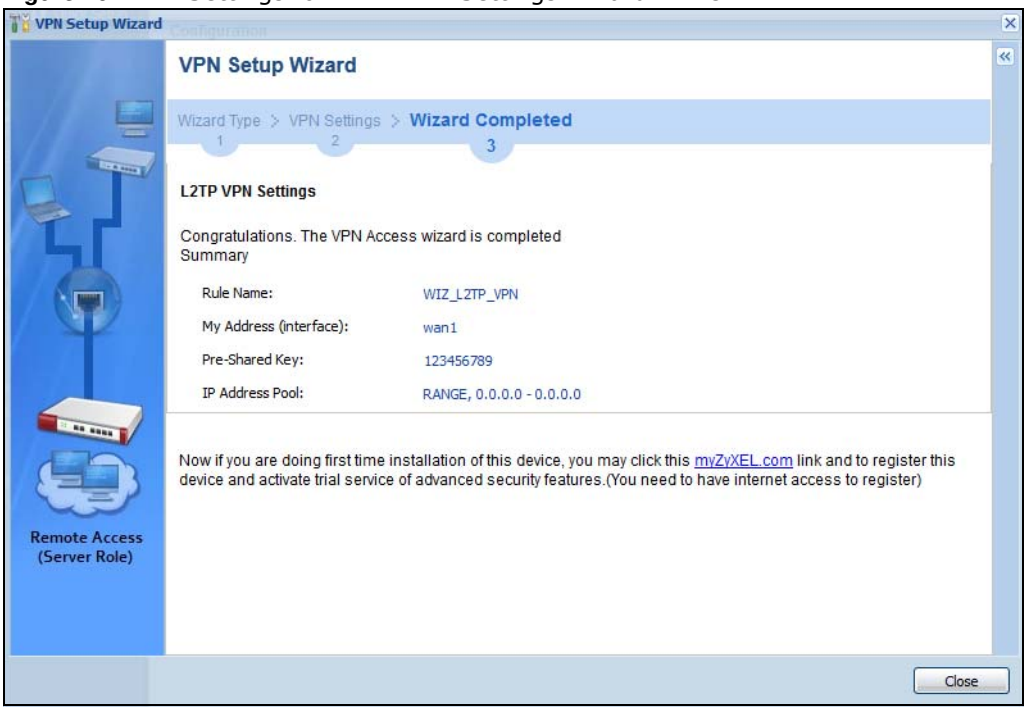
Summary

- Rule Name: Identifies the L2TP VPN connection (and the L2TP VPN gateway).
- Secure Gateway: "Any" displays in this field because it is not configurable in this wizard. It allows incoming connections from the L2TP VPN Client.
- Pre-Shared Key: L2TP VPN tunnel password.
- My Address (Interface): This displays the interface to use on your USG for the L2TP tunnel.
- IP Address Pool: This displays the IP address pool used to assign to the L2TP VPN clients.

Click Save to complete the L2TP VPN Setting and the following screen will show.

4.5.4 VPN Settings for L2TP VPN Setting Wizard Completed

Figure 70 VPN Settings for L2TP VPN Settings Wizard: Finish



Now the rule is configured on the USG. The L2TP VPN rule settings appear in the VPN > L2TP VPN screen and also in the VPN > IPSec VPN > VPN Connection and VPN Gateway screen.

5

Dashboard

5.1 Overview

Use the Dashboard screens to check status information about the USG.

5.1.1 What You Can Do in this Chapter

Use the main Dashboard screen to see the USG's general device information, system status, system resource usage, licensed service status, and interface status. You can also display other status screens for more information.

Use the Dashboard screens to view the following.

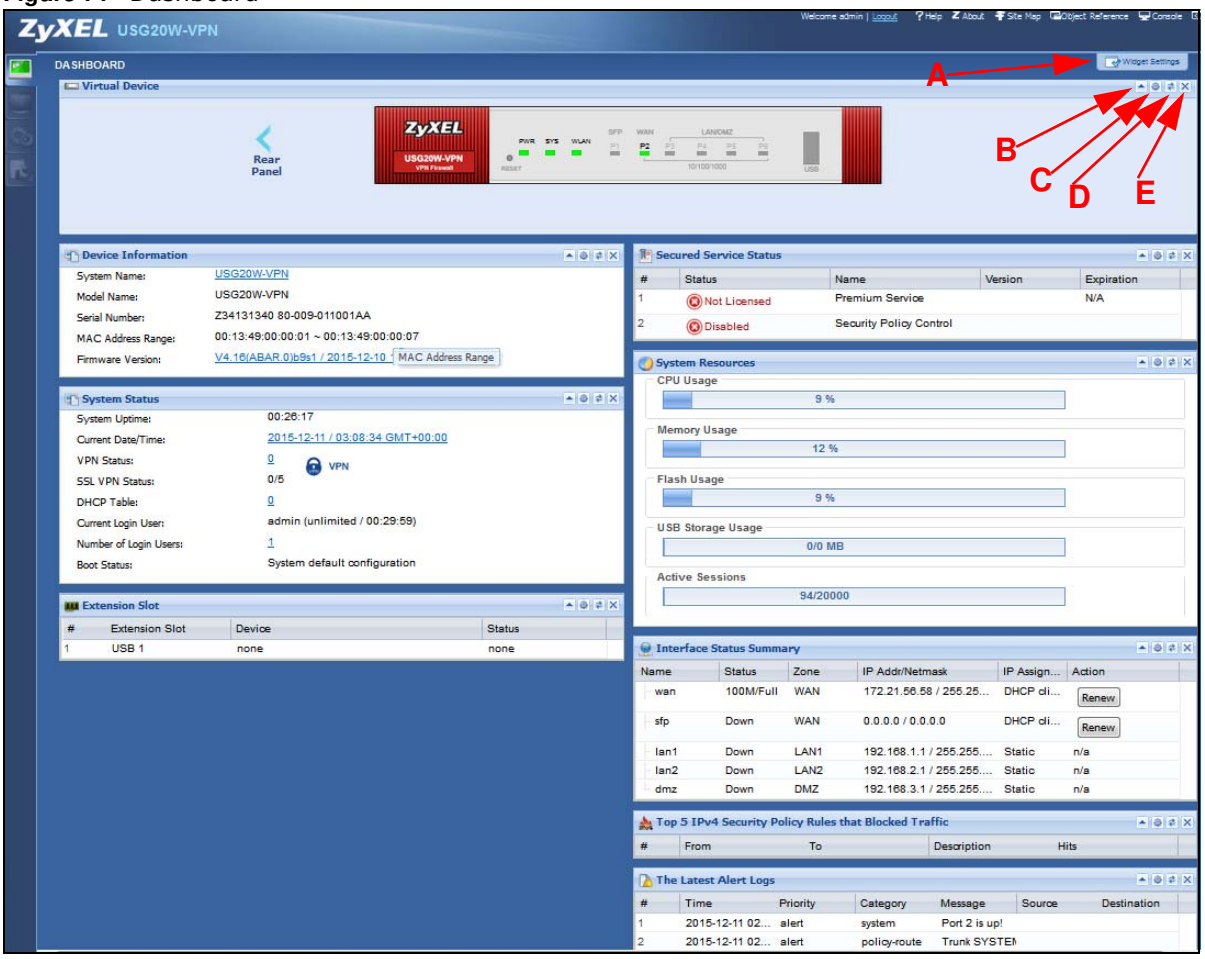
- Device Information Screen on page 85
- System Status Screen on page 86
- VPN Status Screen on page 87
- DHCP Table Screen on page 88
- Number of Login Users Screen on page 89
- System Resources Screen on page 90
- CPU Usage Screen on page 91
- Memory Usage Screen on page 92
- Active Session Screen on page 93
- Extension Slot Screen on page 94
- Interface Status Summary Screen on page 94
- Secured Service Status Screen on page 95
- Content Filter Statistics Screen on page 96
- Top 5 IPv4/IPv6 Security Policy Rules that Blocked Traffic Screen on page 97
- Top 5 IPv4/IPv6 Security Policy Rules that Blocked Traffic Screen on page 97
- Top 5 IPv4/IPv6 Security Policy Rules that Blocked Traffic Screen on page 97
- The Latest Alert Logs Screen on page 97

5.2 Main Dashboard Screen

The Dashboard screen displays when you log into the USG or click Dashboard in the navigation panel. The dashboard displays general device information, system status, system resource usage, licensed service status, and interface status in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets.

Click on the icon to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting, and other information.

Figure 71 Dashboard



The following table describes the labels in this screen.

Table 16 Dashboard

LABEL	DESCRIPTION
Widget Settings (A)	Use this link to open or close widgets by selecting/clearing the associated checkbox.
expand / collapse widget (B)	Click this to collapse a widget. It then becomes a down arrow. Click it again to enlarge the widget again.
Refresh time setting (C)	Set the interval for refreshing the information displayed in the widget.
Refresh Now (D)	Click this to update the widget's information immediately.
Close widget (E)	Click this to close the widget. Use Widget Setting to re-open it.
Virtual Device	
Rear Panel	Click this to view details about the USG's rear panel. Hover your cursor over a connected interface or slot to display status details.

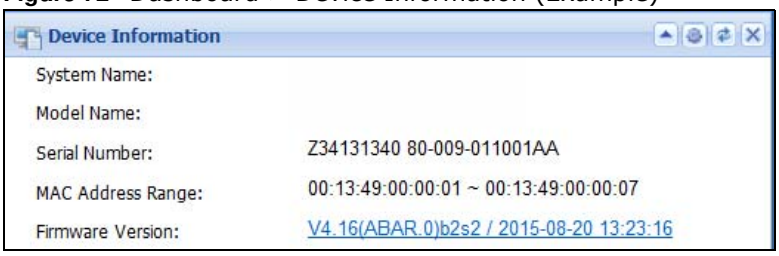
Table 16 Dashboard (continued)

LABEL	DESCRIPTION
Front Panel	Click this to view details about the status of the USG's front panel LEDs and connections. See Section 3.1.1 on page 45 for LED descriptions. An unconnected interface or slot appears grayed out.
	The following front and rear panel labels display when you hover your cursor over a connected interface or slot.
Name	This field displays the name of each interface.
Status	This field displays the current status of each interface or device installed in a slot. The possible values depend on what type of interface it is. Inactive - The Ethernet interface is disabled. Down - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. Speed / Duplex - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (Full or Half). The status for a WLAN card is none. For cellular (mobile broadband) interfaces, see Section 9.5 on page 174 for the status that can appear. For the auxiliary interface: Inactive - The auxiliary interface is disabled. Connected - The auxiliary interface is enabled and connected. Disconnected - The auxiliary interface is not connected.
Zone	This field displays the zone to which the interface is currently assigned.
IP Address/ Mask	This field displays the current IP address and subnet mask assigned to the interface. If the interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).

5.2.1 Device Information Screen

The Device Information screen displays USG's system and model name, serial number, MAC address and firmware version shown in the below screen.

Figure 72 Dashboard > Device Information (Example)



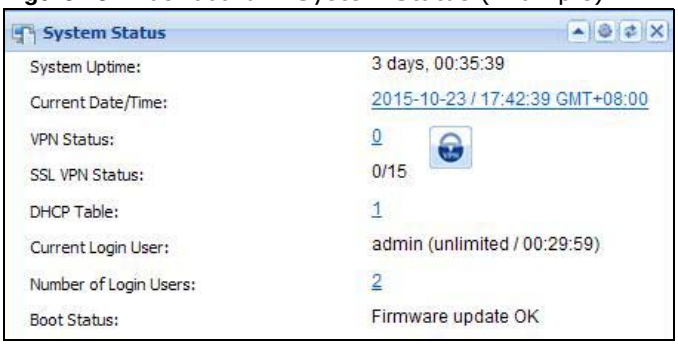
This tabel describes the fields in the above screen.

Table 17 Dashboard > Device Information

LABEL	DESCRIPTION
Device Information	This identifies a device installed in one of the USG's extension slots, the Security Extension Module slot, or USB ports. For an installed SEM (Security Extension Module) card, this field displays what kind of SEM card is installed. SEM-VPN - The VPN accelerator. The SEM-VPN provides 500 Mbps VPN throughput, 2,000 IPSec VPN tunnels, and 750 SSL VPN users. SEM-DUAL - accelerator for both VPN and UTM. The SEM-DUAL provides the benefits of the SEM-VPN.
System Name	This field displays the name used to identify the USG on any network. Click the link and open the Host Name screen where you can edit and make changes to the system and domain name.
Model Name	This field displays the model name of this USG.
Serial Number	This field displays the serial number of this USG. The serial number is used for device tracking and control.
MAC Address Range	This field displays the MAC addresses used by the USG. Each physical port has one MAC address. The first MAC address is assigned to physical port 1, the second MAC address is assigned to physical port 2, and so on.
Firmware Version	This field displays the version number and date of the firmware the USG is currently running. Click the link to open the Firmware Package screen where you can upload firmware.

5.2.2 System Status Screen

Figure 73 Dashboard > System Status (Example)



This table describes the fields in the above screen.

Table 18 Dashboard > System Status

LABEL	DESCRIPTION
System Uptime	This field displays how long the USG has been running since it last restarted or was turned on.
Current Date/Time	This field displays the current date and time in the USG. The format is yyyy-mm-dd hh:mm:ss. Click on the link to see the Date/Time screen where you can make edits and changes to the date, time and time zone information.
VPN Status	Click on the link to look at the VPN tunnels that are currently established. See Section 5.2.3 on page 87. Click on the VPN icon to go to the ZyXEL VPN Client product page at the ZyXEL website.
SSL VPN Status	The first number is the actual number of VPN tunnels up and the second number is the maximum number of SSL VPN tunnels allowed.

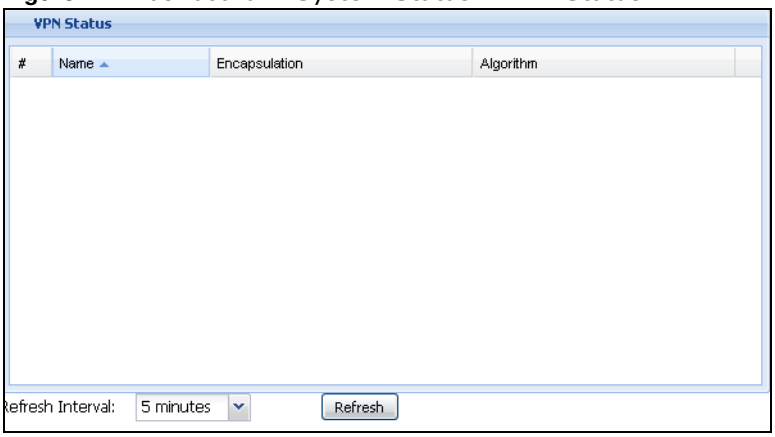
Table 18 Dashboard > System Status

LABEL	DESCRIPTION
DHCP Table	Click this to look at the IP addresses currently assigned to the USG's DHCP clients and the IP addresses reserved for specific MAC addresses. See Section 5.2.4 on page 88.
Current Login User	This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining.
Number of Login Users	This field displays the number of users currently logged in to the USG. Click the icon to pop-open a list of the users who are currently logged in to the USG.
Boot Status	This field displays details about the USG's startup state. OK - The USG started up successfully. Firmware update OK - A firmware update was successful. Problematic configuration after firmware update - The application of the configuration failed after a firmware upgrade. System default configuration - The USG successfully applied the system default configuration. This occurs when the USG starts for the first time or you intentionally reset the USG to the system default settings. Fallback to lastgood configuration - The USG was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file. Fallback to system default configuration - The USG was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf). Booting in progress - The USG is still applying the system configuration.

5.2.3 VPN Status Screen

Click on VPN Status link to look at the VPN tunnels that are currently established. The following screen will show.

Figure 74 Dashboard > System Status > VPN Status



This table describes the fields in the above screen.

Table 19 Dashboard > System Status > VPN Status

LABLE	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPSec SA.
Encapsulation	This field displays how the IPSec SA is encapsulated.
Algorithm	This field displays the encryption and authentication algorithms used in the SA.
Refresh Interval	Select how often you want this window to be updated automatically.
Refresh	Click this to update the information in the window right away.

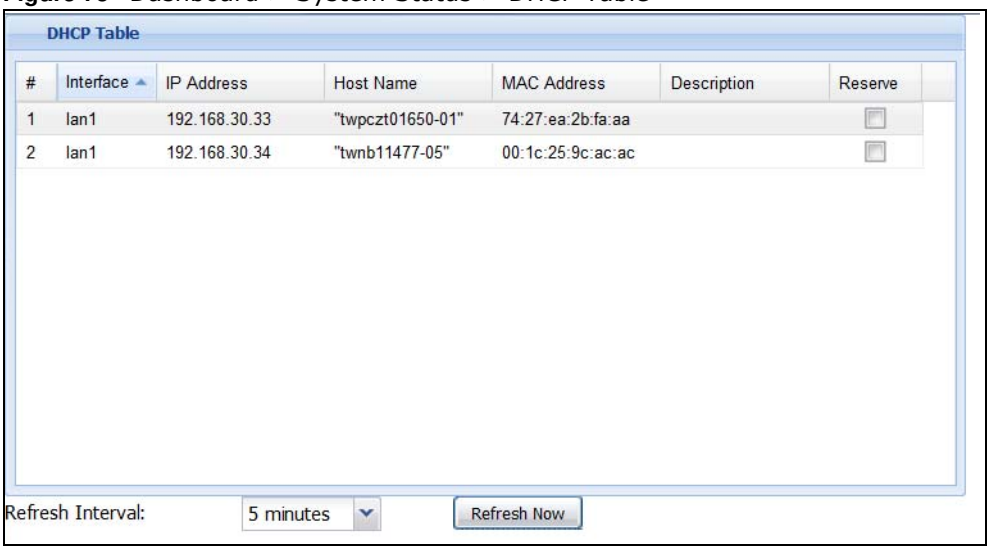
ZyXEL VPN Client Product Page



5.2.4 DHCP Table Screen

Click on the DHCP Table link to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. The following screen will show.

Figure 75 Dashboard > System Status > DHCP Table



This table describes the fields in the above screen.

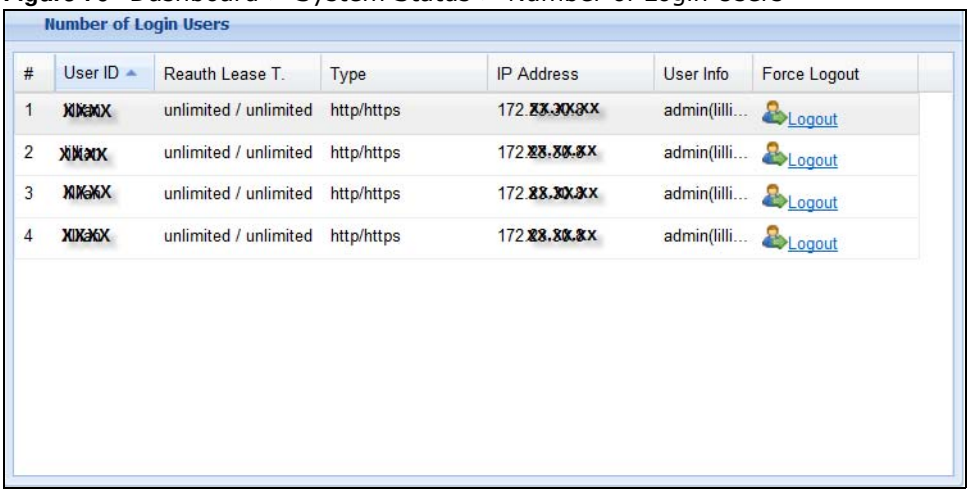
Table 20 Dashboard > System Status > DHCP Table

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
Interface	This field identifies the interface that assigned an IP address to a DHCP client.
IP Address	This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address. Click the column's heading cell to sort the table entries by IP address. Click the heading cell again to reverse the sort order.
Host Name	This field displays the name used to identify this device on the network (the computer name). The USG learns these from the DHCP client requests. "None" shows here for a static DHCP entry.
MAC Address	This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved. Click the column's heading cell to sort the table entries by MAC address. Click the heading cell again to reverse the sort order.
Description	For a static DHCP entry, the host name or the description you configured shows here. This field is blank for dynamic DHCP entries.
Reserve	If this field is selected, this entry is a static DHCP entry. The IP address is reserved for the MAC address. If this field is clear, this entry is a dynamic DHCP entry. The IP address is assigned to a DHCP client. To create a static DHCP entry using an existing dynamic DHCP entry, select this field, and then click Apply. To remove a static DHCP entry, clear this field, and then click Apply.

5.2.5 Number of Login Users Screen

Click the Number of Login Users link to see the following screen.

Figure 76 Dashboard > System Status > Number of Login Users



This table describes the fields in the above screen.

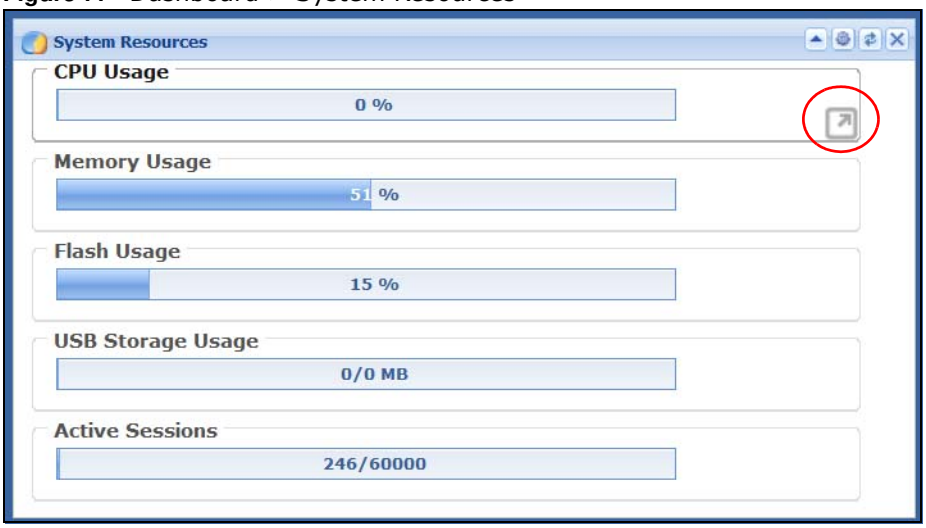
Table 21 Dashboard > System Status > Number of Login Users

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the USG.
Reauth Lease T.	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user.
Type	This field displays the way the user logged in to the USG.
IP address	This field displays the IP address of the computer used to log in to the USG.
User Info	This field displays the types of user accounts the USG uses. If the user type is `ext-user` (external user), this field will show its external-group information when you move your mouse over it. If the external user matches two external-group objects, both external-group object names will be shown.
Force Logout	Click this icon to end a user's session.

5.2.6 System Resources Screen

Hover your mouse over an item and click the arrow on the right to see more details on that resource.

Figure 77 Dashboard > System Resources



This table describes the fields in the above screen.

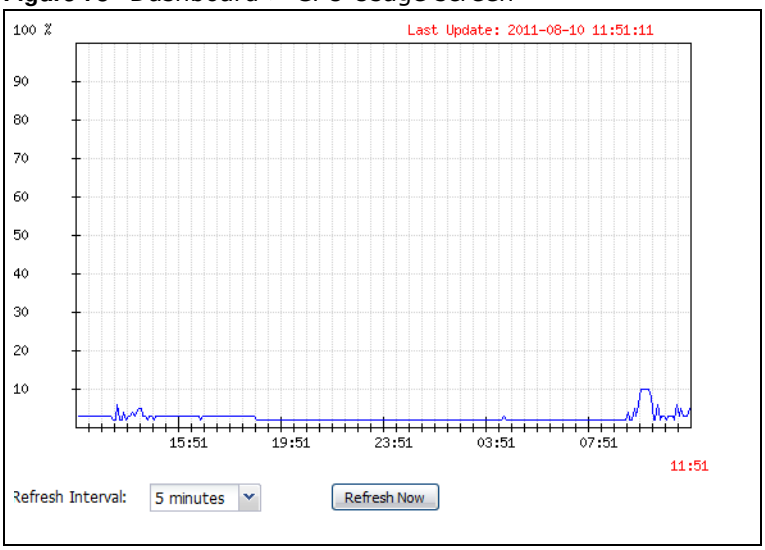
Table 22 .Dashboard > System Resources

LABEL	DESCRIPTION
CPU Usage	This field displays what percentage of the USG's processing capability is currently being used. Hover your cursor over this field to display the Show CPU Usage icon that takes you to a chart of the USG's recent CPU usage.
Memory Usage	This field displays what percentage of the USG's RAM is currently being used. Hover your cursor over this field to display the Show Memory Usage icon that takes you to a chart of the USG's recent memory usage.
Flash Usage	This field displays what percentage of the USG's onboard flash memory is currently being used.
USB Storage Usage	This field shows how much storage in the USB device connected to the USG is in use.
Active Sessions	This field shows how many sessions, established and non-established, that pass through/from/to/within the USG. Hover your cursor over this field to display icons. Click the Detail icon to go to the Session Monitor screen to see details about the active sessions. Click the Show Active Sessions icon to display a chart of USG's recent session usage.

5.2.7 CPU Usage Screen

Use the below screen to look at a chart of the USG's recent CPU usage. To access this screen, click CPU Usage in the dashboard.

Figure 78 Dashboard > CPU Usage screen



This table describes the fields in the above screen.

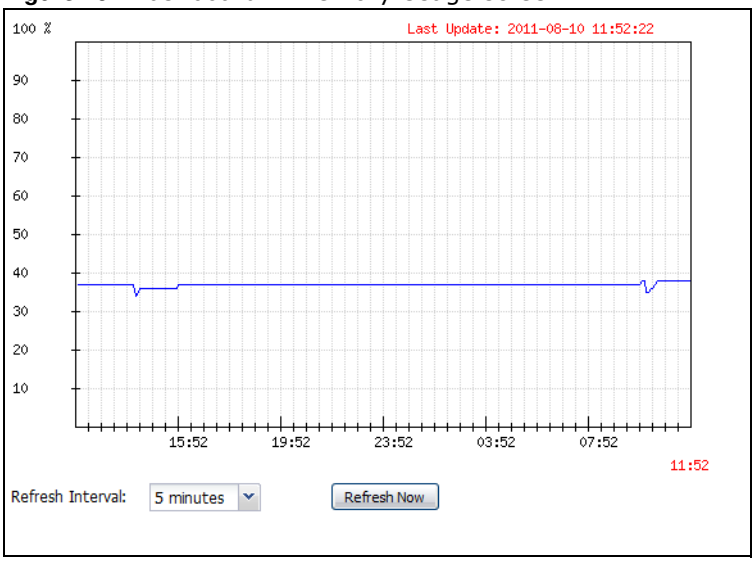
Table 23 Dashboard > CPU Usage

LABEL	DESCRIPTION
	The y-axis represents the percentage of CPU usage.
	The x-axis shows the time period over which the CPU usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

5.2.8 Memory Usage Screen

Use the below screen to look at a chart of the USG's recent memory (RAM) usage. To access this screen, click Memory Usage in the dashboard.

Figure 79 Dashboard > Memory Usage screen



This table describes the fields in the above screen.

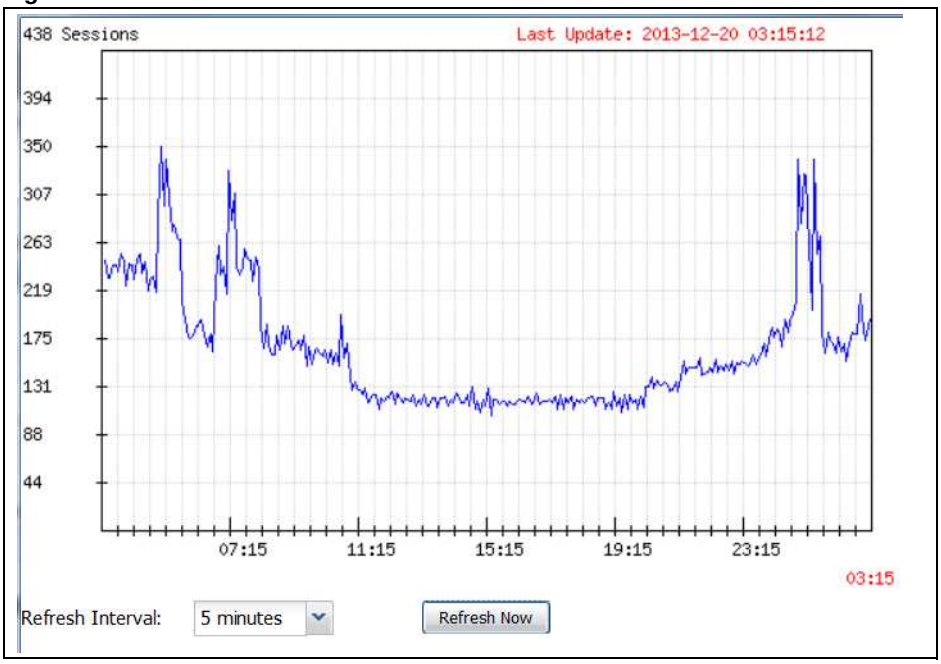
Table 24 Dashboard > Memory Usage screen.

LABEL	DESCRIPTION
	The y-axis represents the percentage of RAM usage.
	The x-axis shows the time period over which the RAM usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

5.2.9 Active Session Screen

To see the details of Active Sessions, move the cursor to the far right of the Active Sessions box and the Detail and the Show Active Session icons appear. Click the Show Active Session icon.

Figure 80 Dashboard > Active Sessions > Show Active Session



This table describes the fields in the above screen.

Table 25 Dashboard > Active Sessions > Show Active Session

Sessions	The y-axis represents the number of session.
	The x-axis shows the time period over which the session usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

5.2.10 Extension Slot Screen

Figure 81 Dashboard > Extension Slot



This table describes the fields in the above screen.

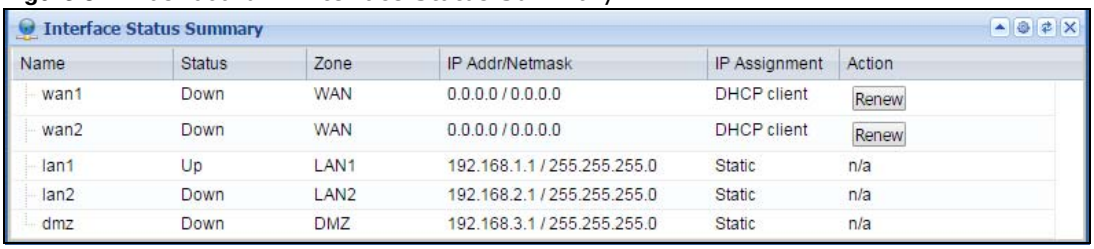
Table 26 Dashboard > Extension Slot

LABEL	DESCRIPTION
#	
Extension Slot	This field displays the name of each extension slot.
Device	This field displays the name of the device connected to the extension slot (or none if no device is detected). For an installed SEM (Security Extension Module) card, this field displays what kind of SEM card is installed. SEM-VPN - The VPN accelerator. The SEM-VPN provides 500 Mbps VPN throughput, 2,000 IPSec VPN tunnels, and 750 SSL VPN users. SEM-DUAL - accelerator for both VPN and UTM. The SEM-DUAL provides the benefits of the SEM-VPN. USB Flash Drive - Indicates a connected USB storage device and the drive's storage capacity.
Status	The status for an installed WLAN card is none. For cellular (mobile broadband) interfaces, see Section 6.10 on page 113 for the status that can appear. For an installed SEM (Security Extension Module) card, this field displays one of the following: Active - The SEM card is working properly. Ready to activate - The SEM was inserted while the USG was operating. Restart the USG to use the SEM. Driver load failed - An error occurred during the USG's attempt to activate the SEM card. Make sure the SEM is installed properly and the thumbscrews are tightened. If this status still displays, contact your vendor. Ready - A USB storage device connected to the USG is ready for the USG to use. Unused - The USG is unable to mount a USB storage device connected to the USG.

5.2.11 Interface Status Summary Screen

Interfaces per USG model vary.

Figure 82 Dashboard > Interface Status Summary



This table describes the fields in the above screen.

Table 27 Dashboard > Interface Status Summary

LABEL	DESCRIPTION
Name	This field displays the name of each interface.
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. For Ethernet interfaces: Inactive - The Ethernet interface is disabled. Down - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. Speed / Duplex - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (Full or Half). For cellular (mobile broadband) interfaces, see Section 6.10 on page 113 for the status that can appear. For the auxiliary interface: Inactive - The auxiliary interface is disabled. Connected - The auxiliary interface is enabled and connected. Disconnected - The auxiliary interface is not connected. For PPP interfaces: Connected - The PPP interface is connected. Disconnected - The PPP interface is not connected. If the PPP interface is disabled, it does not appear in the list. For WLAN interfaces: Up - The WLAN interface is enabled. Down - The WLAN interface is disabled.
Zone	This field displays the zone to which the interface is currently assigned.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address is 0.0.0.0/0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP. If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
IP Assignment	This field displays the interface's IP assignment. It will show DHCP or Static.
Action	Use this field to get or to update the IP address for the interface. Click Renew to send a new DHCP request to a DHCP server. Click the Connect icon to have the USG try to connect a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays n/a. Click the Disconnect icon to stop a PPPoE/PPTP connection.

5.2.12 Secured Service Status Screen

This part shows what security services are available and enabled.

Figure 83 Dashboard > Secured Service Status



This table describes the fields in the above screen.

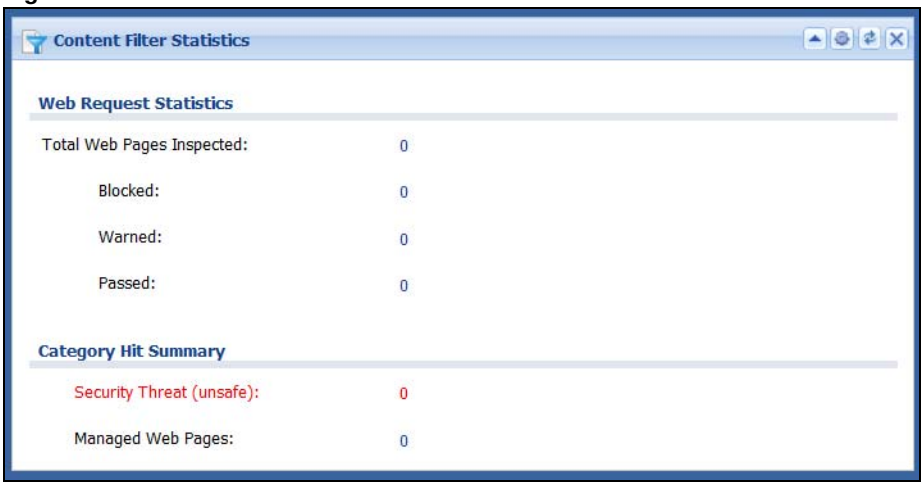
Table 28 Dashboard > Secured Service Status

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific status.
Status	This field displays the status of the USG's security services. It will show these types of status: Licensed, Unlicensed, Disabled or Enabled.
Name	This field displays the name of security services supported by this model. Status will show Licensed for Premium Service after you register the device at myZyXEL.com. You can then activate security service licenses such as Anti-Spam, Content Filter and so on.
Version	This field displays the version number of the services.
Expiration	This field displays the number of days remaining before the license expires.

5.2.13 Content Filter Statistics Screen

Configure Configuration > UTM Profile > Content Filter and then view results here.

Figure 84 Dashboard > Content Filter Statistics



This table describes the fields in the above screen.

Table 29 Dashboard > Content Filter Statistics

LABEL	DESCRIPTION
Web Request Statistics	
Total Web Pages Inspected	This is the number of web pages the USG has checked to see whether they belong to the categories you selected in the content filter screen.

Table 29 Dashboard > Content Filter Statistics

LABEL	DESCRIPTION
Blocked	This is the number of web pages that the USG blocked access.
Warned	This is the number of web pages for which the USG has displayed a warning message to the access requesters.
Passed	This is the number of web pages that the USG allowed access.
Category Hit Summary	
Security Threat (unsafe)	This is the number of requested web pages that belong to the unsafe categories you have selected in the content filter screen.
Managed Web pages	This is the number of requested web pages that belong to the managed categories you have selected in the content filter screen.

5.2.14 Top 5 IPv4/IPv6 Security Policy Rules that Blocked Traffic Screen

Figure 85 Dashboard > Top 5 IPv4/IPv6 Security Policy Rules that Blocked Traffic



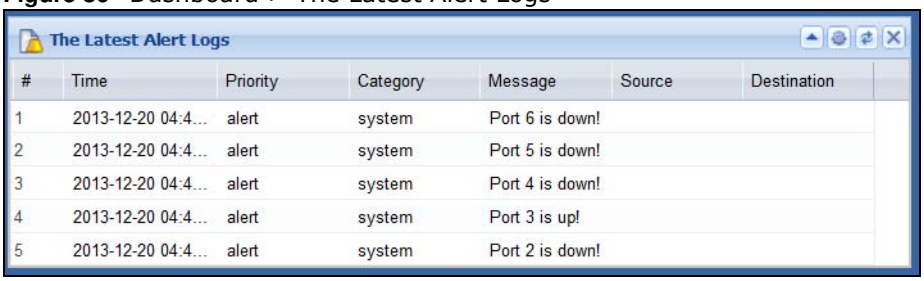
This table describes the fields in the above screen.

Table 30 Dashboard > Top 5 IPv4/IPv6 Security Policy Rules that Blocked Traffic

LABEL	DESCRIPTION
#	This is the entry's rank in the list of the most commonly triggered security policies.
From	This shows the zone packets came from that the triggered security policy.
To	This shows the zone packets went to that the triggered security policy.
Description	This field displays the descriptive name (if any) of the triggered security policy.
Hits	This field displays how many times the security policy was triggered.

5.2.15 The Latest Alert Logs Screen

Figure 86 Dashboard > The Latest Alert Logs



This table describes the fields in the above screen.

Table 31 Dashboard > The Latest Alert Logs

LABEL	DESCRIPTION
#	This is the entry's rank in the list of alert logs.
Time	This field displays the date and time the log was created.
Priority	This field displays the severity of the log.
Category	This field displays the type of log generated.
Message	This field displays the actual log message.
Source	This field displays the source address (if any) in the packet that generated the log.
Destination	This field displays the destination address (if any) in the packet that generated the log.
Source Interface	This field displays the incoming interface of the packet that generated the log.

PART II
Technical Reference

6 Monitor

6.1 Overview

Use the Monitor screens to check status and statistics information.

6.1.1 What You Can Do in this Chapter

Use the Monitor screens for the following.

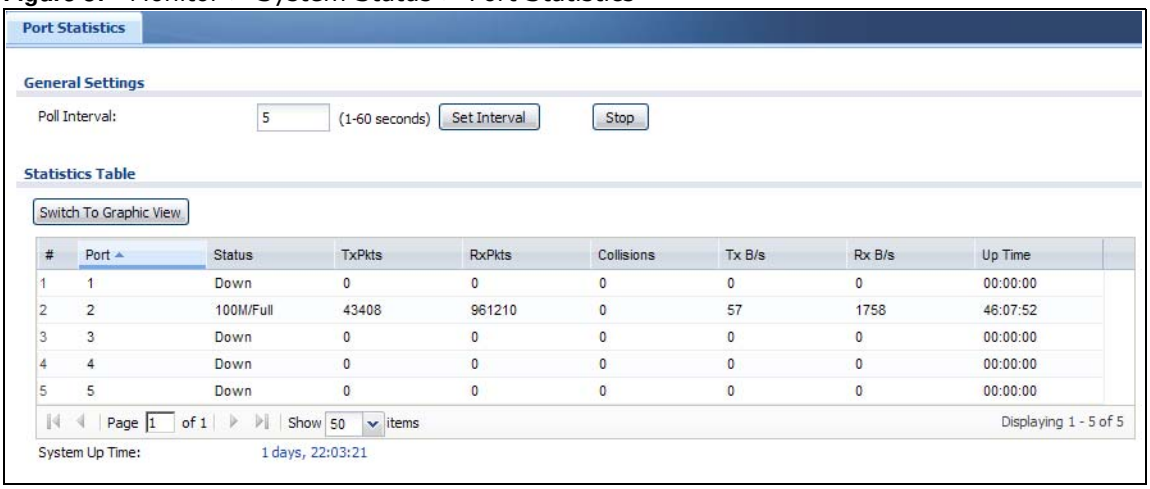
- Use the System Status > Port Statistics screen (see Section 6.2 on page 102) to look at packet statistics for each physical port.
- Use the System Status > Port Statistics > Graph View screen (see Section 6.2 on page 102) to look at a line graph of packet statistics for each physical port.
- Use the System Status > Interface Status screen (Section 6.3 on page 104) to see all of the USG's interfaces and their packet statistics.
- Use the System Status > Traffic Statistics screen (see Section 6.4 on page 106) to start or stop data collection and view statistics.
- Use the System Status > Session Monitor screen (see Section 6.5 on page 109) to view sessions by user or service.
- Use the System Status > IGMP Statistics screen (see Section 6.6 on page 110) to view multicasting details.
- Use the System Status > DDNS Status screen (see Section 6.7 on page 111) to view the status of the USG's DDNS domain names.
- Use the System Status > IP/MAC Binding screen (Section 6.8 on page 112) to view a list of devices that have received an IP address from USG interfaces with IP/MAC binding enabled.
- Use the System Status > Login Users screen (Section 6.9 on page 112) to look at a list of the users currently logged into the USG.
- Use the System Status > Cellular Status screen (Section 6.10 on page 113) to check your mobile broadband connection status.
- Use the System Status > UPnP Port Status screen (see Section 6.11 on page 115) to look at a list of the NAT port mapping rules that UPnP creates on the USG.
- Use the System Status > USB Storage screen (Section 6.12 on page 116) to view information about a connected USB storage device.
- Use the System Status > Ethernet Neighbor screen (Section 6.13 on page 117) to view and manage the USG's neighboring devices via Layer Link Discovery Protocol (LLDP).
- Use the Wireless > AP Information screen (Section 6.14.1 on page 118) to view information on connected APs.
- Use the Wireless > Station Info screen (Section 6.14.3 on page 121) to view information on connected wireless stations.
- Use the Wireless > Detected Device screen (Section 6.14.3 on page 121) to view information about suspected rogue APs.

- Use the VPN Monitor > IPSec screen (Section 6.15 on page 123) to display and manage active IPSec SAs.
- Use the VPN Monitor > SSL screen (see Section 6.16 on page 124) to list the users currently logged into the VPN SSL client portal. You can also log out individual users and delete related session information.
- Use the VPN Monitor > L2TP over IPSec screen (see Section 6.17 on page 125) to display and manage the USG's connected L2TP VPN sessions.
- Use the UTM Statistics > Content Filter screen (Section 6.18 on page 126) to start or stop data collection and view content filter statistics.
- Use the UTM Statistics > Anti-Spam screen (Section 6.19 on page 128) to start or stop data collection and view spam statistics.
- Use the UTM Statistics > Anti-Spam > Status screen (Section 6.19.2 on page 130) to see how many mail sessions the USG is currently checking and DNSBL statistics.
- Use the Log screens (Section 6.20 on page 131) to view the USG's current log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen.

6.2 The Port Statistics Screen

Use this screen to look at packet statistics for each Gigabit Ethernet port. To access this screen, click Monitor > System Status > Port Statistics.

Figure 87 Monitor > System Status > Port Statistics



The following table describes the labels in this screen.

Table 32 Monitor > System Status > Port Statistics

LABEL	DESCRIPTION
Poll Interval	Enter how often you want this window to be updated automatically, and click Set Interval.
Set Interval	Click this to set the Poll Interval the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the Poll Interval and clicking Set Interval.
Switch to Graphic View	Click this to display the port statistics as a line graph.

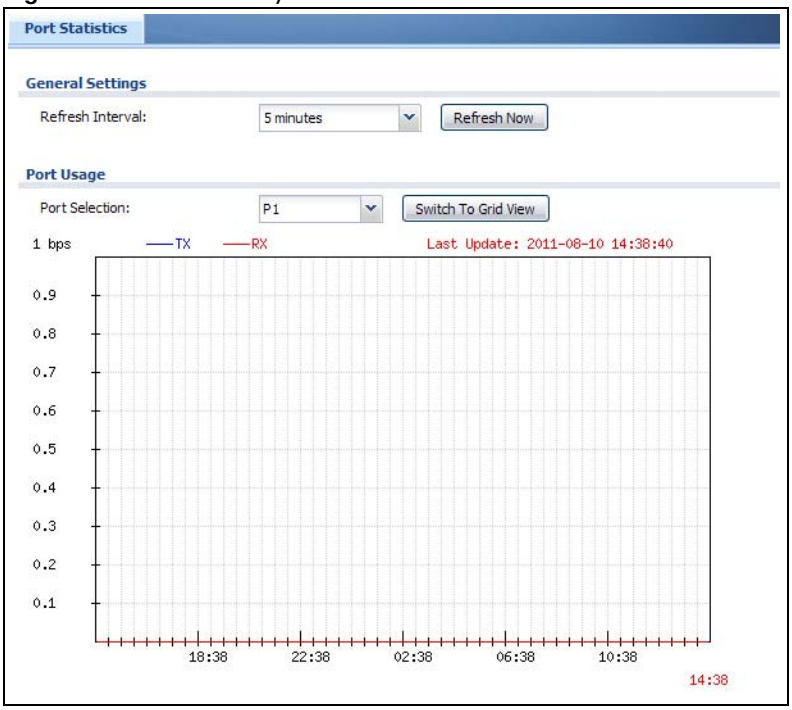
Table 32 Monitor > System Status > Port Statistics (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific port.
Port	This field displays the physical port number.
Status	This field displays the current status of the physical port. Down - The physical port is not connected. Speed / Duplex - The physical port is connected. This field displays the port speed and duplex setting (Full or Half).
TxPkts	This field displays the number of packets transmitted from the USG on the physical port since it was last connected.
RxPkts	This field displays the number of packets received by the USG on the physical port since it was last connected.
Collisions	This field displays the number of collisions on the physical port since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Up Time	This field displays how long the physical port has been connected.
System Up Time	This field displays how long the USG has been running since it last restarted or was turned on.

6.2.1 The Port Statistics Graph Screen

Use this screen to look at a line graph of packet statistics for each physical port. To access this screen, click Port Statistics in the Status screen and then the Switch to Graphic View Button.

Figure 88 Monitor > System Status > Port Statistics > Switch to Graphic View



The following table describes the labels in this screen.

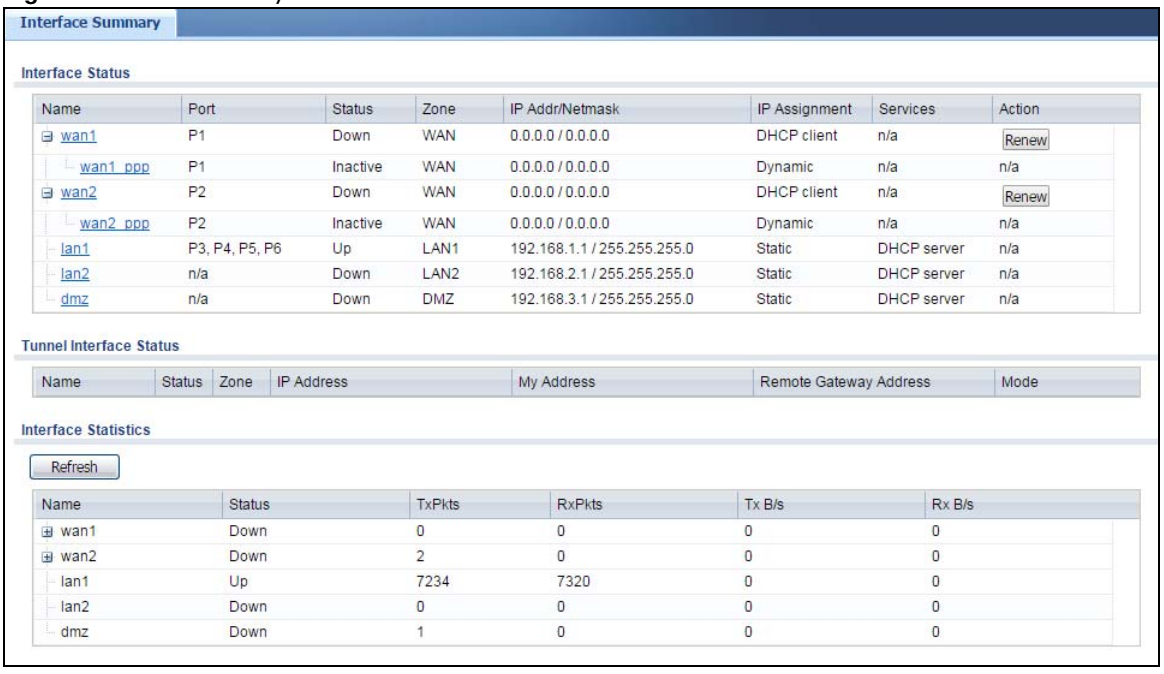
Table 33 Monitor > System Status > Port Statistics > Switch to Graphic View

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.
Port Selection	Select the number of the physical port for which you want to display graphics.
Switch to Grid View	Click this to display the port statistics as a table.
bps	The y-axis represents the speed of transmission or reception.
time	The x-axis shows the time period over which the transmission or reception occurred
TX	This line represents traffic transmitted from the USG on the physical port since it was last connected.
RX	This line represents the traffic received by the USG on the physical port since it was last connected.
Last Update	This field displays the date and time the information in the window was last updated.
System Up Time	This field displays how long the USG has been running since it last restarted or was turned on.

6.3 Interface Status Screen

This screen lists all of the USG's interfaces and gives packet statistics for them. Click Monitor > System Status > Interface Status to access this screen.

Figure 89 Monitor > System Status > Interface Status



Each field is described in the following table.

Table 34 Monitor > System Status > Interface Status

LABEL	DESCRIPTION
Interface Status	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text.
Name	This field displays the name of each interface. If there is an Expand icon (plus-sign) next to the name, click this to look at the status of virtual interfaces on top of this interface.
Port	This field displays the physical port number.
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. For Ethernet interfaces: • Inactive - The Ethernet interface is disabled. • Down - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. • Speed / Duplex - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (Full or Half). For cellular (mobile broadband) interfaces, see Section 6.12 on page 116 the Web Help for the status that can appear. For the auxiliary interface: • Inactive - The auxiliary interface is disabled. • Connected - The auxiliary interface is enabled and connected. • Disconnected - The auxiliary interface is not connected. For virtual interfaces, this field always displays Up. If the virtual interface is disabled, it does not appear in the list. For VLAN and bridge interfaces, this field always displays Up. If the VLAN or bridge interface is disabled, it does not appear in the list. For PPP interfaces: • Connected - The PPP interface is connected. • Disconnected - The PPP interface is not connected. If the PPP interface is disabled, it does not appear in the list. For WLAN interfaces: • Up - The WLAN interface is enabled. • Down - The WLAN interface is disabled.
Zone	This field displays the zone to which the interface is assigned.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address and subnet mask are 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP. If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
IP Assignment	This field displays how the interface gets its IP address. • Static - This interface has a static IP address. • DHCP Client - This interface gets its IP address from a DHCP server.
Services	This field lists which services the interface provides to the network. Examples include DHCP relay, DHCP server, DDNS, RIP, and OSPF. This field displays n/a if the interface does not provide any services to the network.

Table 34 Monitor > System Status > Interface Status (continued)

LABEL	DESCRIPTION
Action	Use this field to get or to update the IP address for the interface. Click Renew to send a new DHCP request to a DHCP server. Click Connect to try to connect a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays n/a.
Tunnel Interface Status	This displays the details of the USG's configured tunnel interfaces.
Name	This field displays the name of the interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Zone	This field displays the zone to which the interface is assigned.
IP Address	This is the IP address of the interface. If the interface is active (and connected), the USG tunnels local traffic sent to this IP address to the Remote Gateway Address.
My Address	This is the interface or IP address uses to identify itself to the remote gateway. The USG uses this as the source for the packets it tunnels to the remote gateway.
Remote Gateway Address	This is the IP address or domain name of the remote gateway to which this interface tunnels traffic.
Mode	This field displays the tunnel mode that you are using.
Interface Statistics	This table provides packet statistics for each interface.
Refresh	Click this button to update the information in the screen.
Name	This field displays the name of each interface. If there is a Expand icon (plus-sign) next to the name, click this to look at the statistics for virtual interfaces on top of this interface.
Status	This field displays the current status of the interface. • Down - The interface is not connected. • Speed / Duplex - The interface is connected. This field displays the port speed and duplex setting (Full or Half). This field displays Connected and the accumulated connection time (hh:mm:ss) when the PPP interface is connected.
TxPkts	This field displays the number of packets transmitted from the USG on the interface since it was last connected.
RxPkts	This field displays the number of packets received by the USG on the interface since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the interface in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the interface in the one-second interval before the screen updated.

6.4 The Traffic Statistics Screen

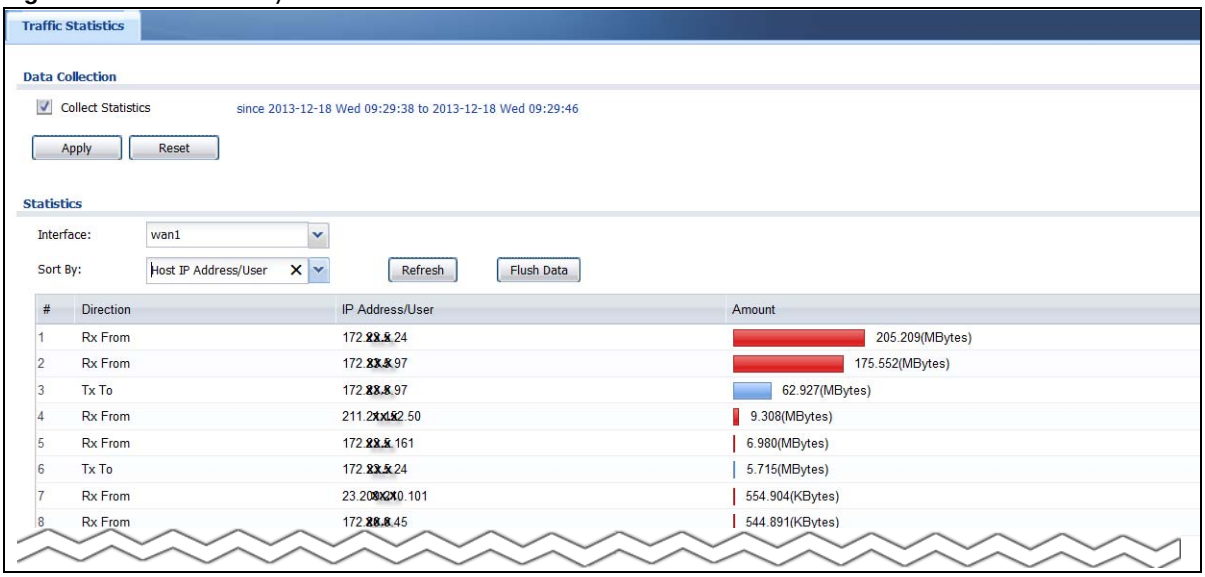
Click Monitor > System Status > Traffic Statistics to display the Traffic Statistics screen. This screen provides basic information about the following for example:

- Most-visited Web sites and the number of times each one was visited. This count may not be accurate in some cases because the USG counts HTTP GET packets. Please see Table 35 on page 107 for more information.
- Most-used protocols or service ports and the amount of traffic on each one

- LAN IP with heaviest traffic and how much traffic has been sent to and from each one

You use the Traffic Statistics screen to tell the USG when to start and when to stop collecting information for these reports. You cannot schedule data collection; you have to start and stop it manually in the Traffic Statistics screen.

Figure 90 Monitor > System Status > Traffic Statistics



There is a limit on the number of records shown in the report. Please see Table 36 on page 108 for more information. The following table describes the labels in this screen.

Table 35 Monitor > System Status > Traffic Statistics

LABEL	DESCRIPTION
Data Collection	
Collect Statistics	Select this to have the USG collect data for the report. If the USG has already been collecting data, the collection period displays to the right. The progress is not tracked here real-time, but you can click the Refresh button to update it.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.
Statistics	
Interface	Select the interface from which to collect information. You can collect information from Ethernet, VLAN, bridge and PPPoE/PPTP interfaces.
Sort By	Select the type of report to display. Choices are: • Host IP Address/ User - displays the IP addresses or users with the most traffic and how much traffic has been sent to and from each one. • Service/ Port - displays the most-used protocols or service ports and the amount of traffic for each one. • Web Site Hits - displays the most-visited Web sites and how many times each one has been visited. Each type of report has different information in the report (below).
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics and update the report display.
	These fields are available when the Traffic Type is Host IP Address/ User.
#	This field is the rank of each record. The IP addresses and users are sorted by the amount of traffic.

Table 35 Monitor > System Status > Traffic Statistics (continued)

LABEL	DESCRIPTION
Direction	This field indicates whether the IP address or user is sending or receiving traffic. • Ingress- traffic is coming from the IP address or user to the USG. • Egress - traffic is going from the USG to the IP address or user.
IP Address/User	This field displays the IP address or user in this record. The maximum number of IP addresses or users in this report is indicated in Table 36 on page 108.
Amount	This field displays how much traffic was sent or received from the indicated IP address or user. If the Direction is Ingress, a red bar is displayed; if the Direction is Egress, a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes or Gbytes, depending on the amount of traffic for the particular IP address or user. The count starts over at zero if the number of bytes passes the byte count limit. See Table 36 on page 108.
	These fields are available when the Traffic Type is Service/ Port.
#	This field is the rank of each record. The protocols and service ports are sorted by the amount of traffic.
Service/Port	This field displays the service and port in this record. The maximum number of services and service ports in this report is indicated in Table 36 on page 108.
Protocol	This field indicates what protocol the service was using.
Direction	This field indicates whether the indicated protocol or service port is sending or receiving traffic. • Ingress - traffic is coming into the router through the interface • Egress - traffic is going out from the router through the interface
Amount	This field displays how much traffic was sent or received from the indicated service / port. If the Direction is Ingress, a red bar is displayed; if the Direction is Egress, a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes, Gbytes, or Tbytes, depending on the amount of traffic for the particular protocol or service port. The count starts over at zero if the number of bytes passes the byte count limit. See Table 36 on page 108.
	These fields are available when the Traffic Type is Web Site Hits.
#	This field is the rank of each record. The domain names are sorted by the number of hits.
Web Site	This field displays the domain names most often visited. The USG counts each page viewed on a Web site as another hit. The maximum number of domain names in this report is indicated in Table 36 on page 108.
Hits	This field displays how many hits the Web site received. The USG counts hits by counting HTTP GET packets. Many Web sites have HTTP GET references to other Web sites, and the USG counts these as hits too. The count starts over at zero if the number of hits passes the hit count limit. See Table 36 on page 108.

The following table displays the maximum number of records shown in the report, the byte count limit, and the hit count limit.

Table 36 Maximum Values for Reports

LABEL	DESCRIPTION
Maximum Number of Records	20
Byte Count Limit	2^{64} bytes; this is just less than 17 million terabytes.
Hit Count Limit	2^{64} hits; this is over 1.8×10^{19} hits.

6.5 The Session Monitor Screen

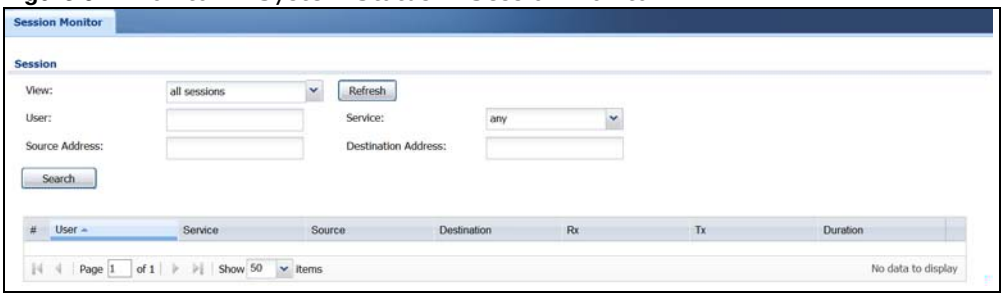
The Session Monitor screen displays all established sessions that pass through the USG for debugging or statistical analysis. It is not possible to manage sessions in this screen. The following information is displayed.

- User who started the session
- Protocol or service port used
- Source address
- Destination address
- Number of bytes received (so far)
- Number of bytes transmitted (so far)
- Duration (so far)

You can look at all established sessions that passed through the USG by user, service, source IP address, or destination IP address. You can also filter the information by user, protocol / service or service group, source address, and/or destination address and view it by user.

Click Monitor > System Status > Session Monitor to display the following screen.

Figure 91 Monitor > System Status > Session Monitor



The following table describes the labels in this screen.

Table 37 Monitor > System Status > Session Monitor

LABEL	DESCRIPTION
View	Select how you want the established sessions that passed through the USG to be displayed. Choices are: • sessions by users - display all active sessions grouped by user • sessions by services - display all active sessions grouped by service or protocol • sessions by source IP - display all active sessions grouped by source IP address • sessions by destination IP - display all active sessions grouped by destination IP address • all sessions - filter the active sessions by the User, Service, Source Address, and Destination Address, and display each session individually (sorted by user).
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open and close the screen.
	The User, Service, Source Address, and Destination Address fields display if you view all sessions. Select your desired filter criteria and click the Refresh button to filter the list of sessions.
User	This field displays when View is set to all sessions. Type the user whose sessions you want to view. It is not possible to type part of the user name or use wildcards in this field; you must enter the whole user name.

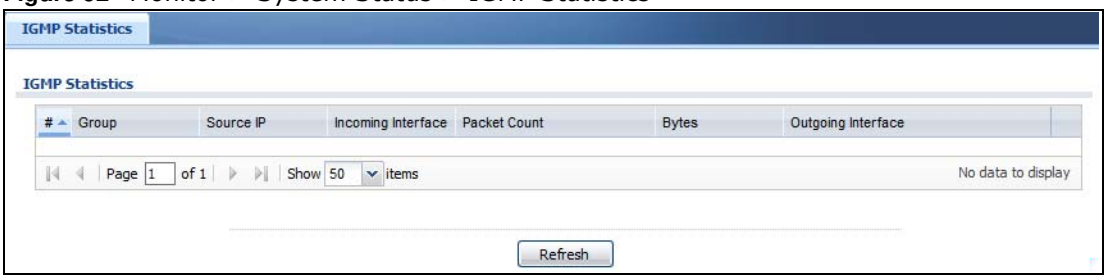
Table 37 Monitor > System Status > Session Monitor (continued)

LABEL	DESCRIPTION
Service	This field displays when View is set to all sessions. Select the service or service group whose sessions you want to view. The USG identifies the service by comparing the protocol and destination port of each packet to the protocol and port of each services that is defined.
Source	This field displays when View is set to all sessions. Type the source IP address whose sessions you want to view. You cannot include the source port.
Destination	This field displays when View is set to all sessions. Type the destination IP address whose sessions you want to view. You cannot include the destination port.
Rx	This field displays the amount of information received by the source in the active session.
Tx	This field displays the amount of information transmitted by the source in the active session.
Duration	This field displays the length of the active session in seconds.
Active Sessions	This is the total number of established sessions that passed through the USG which matched the search criteria.
Show	Select the number of active sessions displayed on each page. You can use the arrow keys on the right to change pages.
#	This field is the rank of each record. The names are sorted by the name of user in active session. You can use the pull down menu on the right to choose sorting method.
User	This field displays the user in each active session. If you are looking at the sessions by users (or all sessions) report, click + or - to display or hide details about a user's sessions.
Service	This field displays the protocol used in each active session. If you are looking at the sessions by services report, click + or - to display or hide details about a protocol's sessions.
Source	This field displays the source IP address and port in each active session. If you are looking at the sessions by source IP report, click + or - to display or hide details about a source IP address's sessions.
Destination	This field displays the destination IP address and port in each active session. If you are looking at the sessions by destination IP report, click + or - to display or hide details about a destination IP address's sessions.
Rx	This field displays the amount of information received by the source in the active session.
Tx	This field displays the amount of information transmitted by the source in the active session.
Duration	This field displays the length of the active session in seconds.

6.6 IGMP Statistics

The Internet Group Management Protocol (IGMP) Statistics is used by USG IP hosts to inform adjacent router about multicast group memberships. It can also be used for one-to-many networking applications such as online streaming video and gaming, distribution of company newsletters, updating address book of mobile computer users in the field allowing more efficient use of resources when supporting these types of applications. Click Monitor > System Status > IGMP Statistics to open the following screen.

Figure 92 Monitor > System Status > IGMP Statistics



The following table describes the labels in this screen.

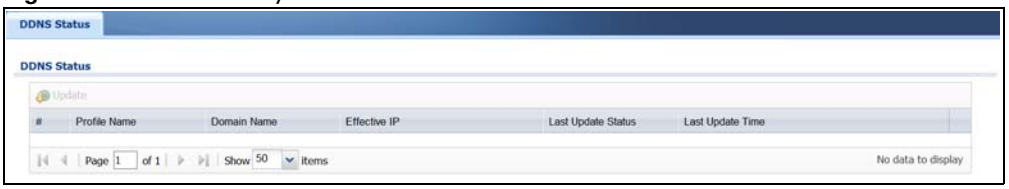
Table 38 Monitor > System Status > IGMP Statistics

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific I GMP Statistics.
Group	This field displays the group of devices in the IGMP.
Source IP	This field displays the host source IP information of the IGMP.
Incoming Interface	This field displays the incoming interface that's connected on the IGMP.
Packet Count	This field displays the packet size of the data being transferred.
Bytes	This field displays the size of the data being transferred in Byes.
Outgoing Interface	This field displays the outgoing interface that's connected on the IGMP.

6.7 The DDNS Status Screen

The DDNS Status screen shows the status of the USG's DDNS domain names. Click Monitor > System Status > DDNS Status to open the following screen.

Figure 93 Monitor > System Status > DDNS Status



The following table describes the labels in this screen.

Table 39 Monitor > System Status > DDNS Status

LABEL	DESCRIPTION
Update	Click this to have the USG update the profile to the DDNS server. The USG attempts to resolve the IP address for the domain name.
#	This field is a sequential value, and it is not associated with a specific DDNS server.
Profile Name	This field displays the descriptive profile name for this entry.
Domain Name	This field displays each domain name the USG can route.
Effective IP	This is the (resolved) IP address of the domain name.

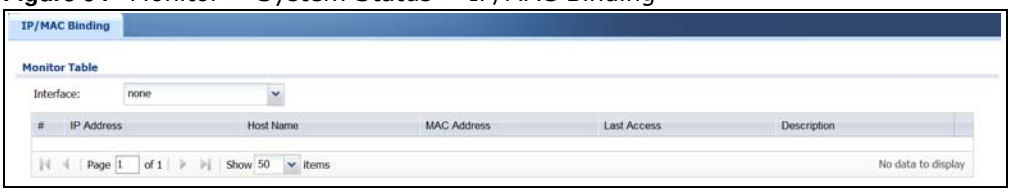
Table 39 Monitor > System Status > DDNS Status (continued)

LABEL	DESCRIPTION
Last Update Status	This shows whether the last attempt to resolve the IP address for the domain name was successful or not. Updating means the USG is currently attempting to resolve the IP address for the domain name.
Last Update Time	This shows when the last attempt to resolve the IP address for the domain name occurred (in year-month-day hour:minute:second format).

6.8 IP/MAC Binding

Click Monitor > System Status > IP/MAC Binding to open the IP/MAC Binding screen. This screen lists the devices that have received an IP address from USG interfaces with IP/MAC binding enabled and have ever established a session with the USG. Devices that have never established a session with the USG do not display in the list.

Figure 94 Monitor > System Status > IP/MAC Binding



The following table describes the labels in this screen.

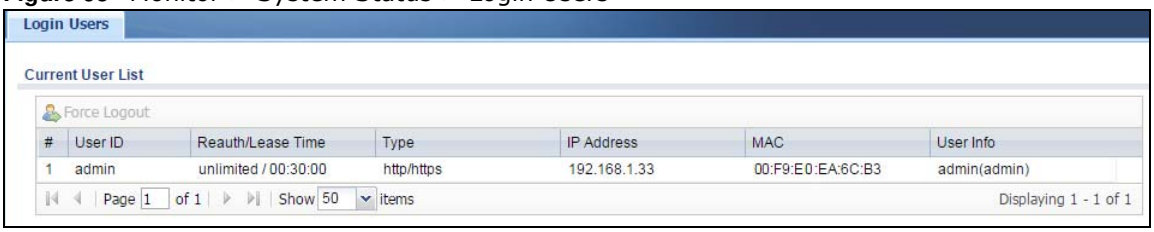
Table 40 Monitor > System Status > IP/MAC Binding

LABEL	DESCRIPTION
Interface	Select a USG interface that has IP/MAC binding enabled to show to which devices it has assigned an IP address.
#	This field is a sequential value, and it is not associated with a specific IP/MAC binding entry.
IP Address	This is the IP address that the USG assigned to a device.
Host Name	This field displays the name used to identify this device on the network (the computer name). The USG learns these from the DHCP client requests.
MAC Address	This field displays the MAC address to which the IP address is currently assigned.
Last Access	This is when the device last established a session with the USG through this interface.
Description	This field displays the description of the IP/MAC binding.

6.9 The Login Users Screen

Use this screen to look at a list of the users currently logged into the USG. To access this screen, click Monitor > System Status > Login Users.

Figure 95 Monitor > System Status > Login Users



The following table describes the labels in this screen.

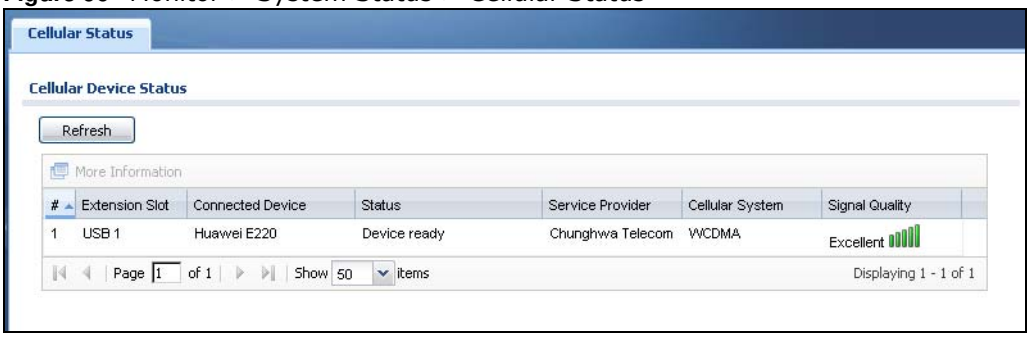
Table 41 Monitor > System Status > Login Users

LABEL	DESCRIPTION
Force Logout	Select a user ID and click this icon to end a user's session.
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the USG.
Reauth Lease T.	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user.
Type	This field displays the way the user logged in to the USG.
IP Address	This field displays the IP address of the computer used to log in to the USG.
MAC	This field displays the MAC address of the computer used to log in to the USG.
User Info	This field displays the types of user accounts the USG uses. If the user type is ext-user (external user), this field will show its external-group information when you move your mouse over it. If the external user matches two external-group objects, both external-group object names will be shown.
Refresh	Click this button to update the information in the screen.

6.10 Cellular Status Screen

This screen displays your mobile broadband connection status. Click Monitor > System Status > Cellular Status to display this screen.

Figure 96 Monitor > System Status > Cellular Status



The following table describes the labels in this screen.

Table 42 Monitor > System Status > Cellular Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information in the screen.
More Information	Click this to display more information on your mobile broadband, such as the signal strength, IMEA/ESN and IMSI. This is only available when the mobile broadband device attached and activated on your USG. Refer to Section 6.11 on page 115.
#	This field is a sequential value, and it is not associated with any interface.
Extension Slot	This field displays where the entry's cellular card is located.
Connected Device	This field displays the model name of the cellular card.
Status	• No device - no mobile broadband device is connected to the USG. • No Service - no mobile broadband network is available in the area; you cannot connect to the Internet. • Limited Service - returned by the service provider in cases where the SIM card is expired, the user failed to pay for the service and so on; you cannot connect to the Internet. • Device detected - displays when you connect a mobile broadband device. • Device error - a mobile broadband device is connected but there is an error. • Probe device fail - the USG's test of the mobile broadband device failed. • Probe device ok - the USG's test of the mobile broadband device succeeded. • Init device fail - the USG was not able to initialize the mobile broadband device. • Init device ok - the USG initialized the mobile broadband card. • Check lock fail - the USG's check of whether or not the mobile broadband device is locked failed. • Device locked - the mobile broadband device is locked. • SIM error - there is a SIM card error on the mobile broadband device. • SIM locked-PUK - the PUK is locked on the mobile broadband device's SIM card. • SIM locked-PIN - the PIN is locked on the mobile broadband device's SIM card. • Unlock PUK fail - Your attempt to unlock a WCDMA mobile broadband device's PUK failed because you entered an incorrect PUK. • Unlock PIN fail - Your attempt to unlock a WCDMA mobile broadband device's PIN failed because you entered an incorrect PIN. • Unlock device fail - Your attempt to unlock a CDMA2000 mobile broadband device failed because you entered an incorrect device code. • Device unlocked - You entered the correct device code and unlocked a CDMA2000 mobile broadband device. • Get dev-info fail - The USG cannot get cellular device information. • Get dev-info ok - The USG succeeded in retrieving mobile broadband device information. • Searching network - The mobile broadband device is searching for a network. • Get signal fail - The mobile broadband device cannot get a signal from a network. • Network found - The mobile broadband device found a network. • Apply config - The USG is applying your configuration to the mobile broadband device. • Inactive - The mobile broadband interface is disabled. • Active - The mobile broadband interface is enabled. • Incorrect device - The connected mobile broadband device is not compatible with the USG. • Correct device - The USG detected a compatible mobile broadband device. • Set band fail - Applying your band selection was not successful. • Set band ok - The USG successfully applied your band selection. • Set profile fail - Applying your ISP settings was not successful. • Set profile ok - The USG successfully applied your ISP settings. • PPP fail - The USG failed to create a PPP connection for the cellular interface. • Need auth-password - You need to enter the password for the mobile broadband card in the cellular edit screen. • Device ready - The USG successfully applied all of your configuration and you can use the mobile broadband connection.

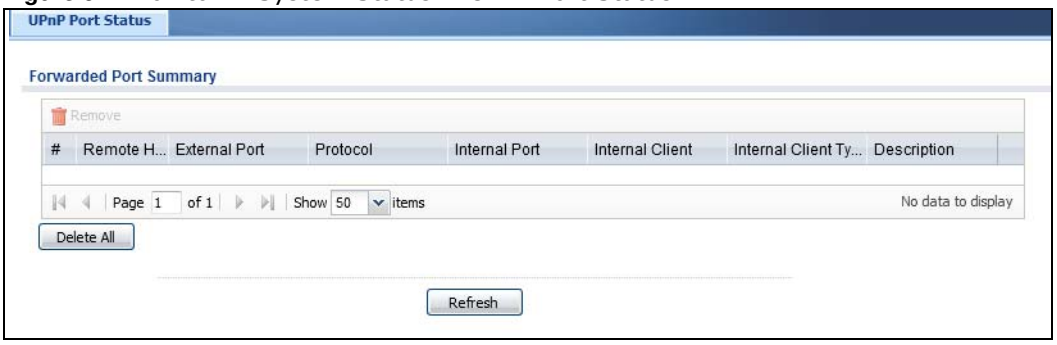
Table 42 Monitor > System Status > Cellular Status (continued)

LABEL	DESCRIPTION
Service Provider	This displays the name of your network service provider. This shows Limited Service if the service provider has stopped service to the mobile broadband card. For example if the bill has not been paid or the account has expired.
Cellular System	This field displays what type of cellular network the mobile broadband connection is using. The network type varies depending on the mobile broadband card you inserted and could be UMTS, UMTS/ HSDPA, GPRS or EDGE when you insert a GSM mobile broadband card, or 1xRTT, EVDO Rev.0 or EVDO Rev.A when you insert a CDMA mobile broadband card.
Signal Quality	This displays the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your USG and the service provider's base station.

6.11 The UPnP Port Status Screen

Use this screen to look at the NAT port mapping rules that UPnP creates on the USG. To access this screen, click Monitor > System Status > UPnP Port Status.

Figure 97 Monitor > System Status > UPnP Port Status



The following table describes the labels in this screen.

Table 43 Monitor > System Status > UPnP Port Status

LABEL	DESCRIPTION
Remove	Select an entry and click this button to remove it from the list.
#	This is the index number of the UPnP-created NAT mapping rule entry.
Remote Host	This field displays the source IP address (on the WAN) of inbound IP packets. Since this is often a wildcard, the field may be blank. When the field is blank, the USG forwards all traffic sent to the External Port on the WAN interface to the Internal Client on the Internal Port. When this field displays an external IP address, the NAT rule has the USG forward inbound packets to the Internal Client from that IP address only.
External Port	This field displays the port number that the USG "listens" on (on the WAN port) for connection requests destined for the NAT rule's Internal Port and Internal Client. The USG forwards incoming packets (from the WAN) with this port number to the Internal Client on the Internal Port (on the LAN). If the field displays "0", the USG ignores the Internal Port value and forwards requests on all external port numbers (that are otherwise unmapped) to the Internal Client.
Protocol	This field displays the protocol of the NAT mapping rule (TCP or UDP).

Table 43 Monitor > System Status > UPnP Port Status (continued)

LABEL	DESCRIPTION
Internal Port	This field displays the port number on the Internal Client to which the USG should forward incoming connection requests.
Internal Client	This field displays the DNS host name or IP address of a client on the LAN. Multiple NAT clients can use a single port simultaneously if the internal client field is set to 255.255.255.255 for UDP mappings.
Internal Client Type	This field displays the type of the client application on the LAN.
Description	This field displays a text explanation of the NAT mapping rule.
Delete All	Click this to remove all mapping rules from the NAT table.
Refresh	Click this button to update the information in the screen.

6.12 USB Storage Screen

This screen displays information about a connected USB storage device. Click Monitor > System Status > USB Storage to display this screen.

Figure 98 Monitor > System Status > USB Storage



The following table describes the labels in this screen.

Table 44 Monitor > System Status > USB Storage

LABEL	DESCRIPTION
Device description	This is a basic description of the type of USB device.
Usage	This field displays how much of the USB storage device's capacity is currently being used out of its total capacity and what percentage that makes.
Filesystem	This field displays what file system the USB storage device is formatted with. This field displays Unknown if the file system of the USB storage device is not supported by the USG, such as NTFS.
Speed	This field displays the connection speed the USB storage device supports.

Table 44 Monitor > System Status > USB Storage (continued)

LABEL	DESCRIPTION
Status	Ready - you can have the USG use the USB storage device. Click Remove Now to stop the USG from using the USB storage device so you can remove it. Unused - the connected USB storage device was manually unmounted by using the Remove Now button or for some reason the USG cannot mount it. Click Use It to have the USG mount a connected USB storage device. This button is grayed out if the file system is not supported (unknown) by the USG. none - no USB storage device is connected.
Detail	This field displays any other information the USG retrieves from the USB storage device. • Deactivated - the use of a USB storage device is disabled (turned off) on the USG. • OutofSpace - the available disk space is less than the disk space full threshold. • Mounting - the USG is mounting the USB storage device. • Removing - the USG is unmounting the USB storage device. • none - the USB device is operating normally or not connected.

6.13 Ethernet Neighbor Screen

The Ethernet Neighbor screen allows you to view the USG's neighboring devices in one place.

It uses Smart Connect, that is Link Layer Discovery Protocol (LLDP) for discovering and configuring LLDP-aware devices in the same broadcast domain as the USG that you're logged into using the web configurator.

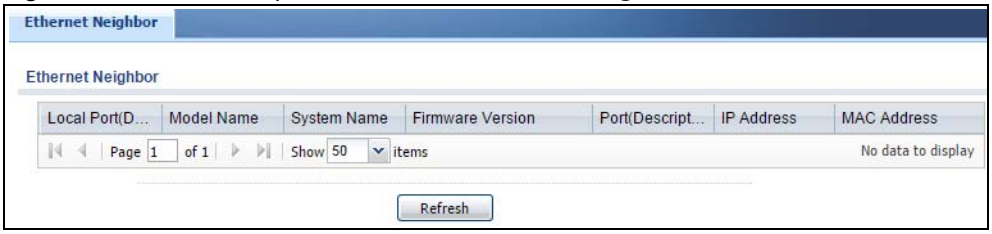
LLDP is a layer-2 protocol that allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps you discover network changes and perform necessary network reconfiguration and management.

Note: Enable Smart Connect in the System > ZON screen.

See also System > ZON for more information on the ZyXEL One Network (ZON) utility that uses the ZyXEL Discovery Protocol (ZDP) for discovering and configuring ZDP-aware ZyXEL devices in the same network as the computer on which the ZON utility is installed.

Click Monitor > System Status > Ethernet Neighbor to see the following screen

Figure 99 Monitor > System Status > Ethernet Neighbor



The following table describes the fields in the previous screen.

Table 45 Monitor > System Status > Ethernet Neighbor

LABEL	DESCRIPTION
Local Port (Description)	This field displays the port of the USG, on which the neighboring device is discovered. For USGs that support Port Role, if ports 3 to 5 are grouped together and there is a connection to P5 only, the USG will display P3 as the interface port number (even though there is no connection to that port).
Model Name	This field displays the model name of the discovered device.
System Name	This field displays the system name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
Port (Description)	This field displays the first internal port on the discovered device. Internal is an interface type displayed in the Network > Interface > Ethernet > Edit screen. For example, if P1 and P2 are WAN, P3 to P5 are LAN, and P6 is DMZ, then USG will display P3 as the first internal interface port number. For USGs that support Port Role, if ports 3 to 5 are grouped together and there is a connection to P5 only, the USG will display P3 as the first internal interface port number (even though there is no connection to that port).
IP Address	This field displays the IP address of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.
Refresh	Click this button to update the information in the screen.

6.14 Wireless

Wireless contains AP information and Station Info menus.

6.14.1 Wireless AP Information: Radio List

Click Monitor > Wireless > AP Information > Radio List to display the Radio List screen.

Figure 100 Monitor > Wireless > Radio List



The following table describes the labels in this screen.

Table 46 Monitor > Wireless > Radio List

LABEL	DESCRIPTION
More Information	Click this icon to see the traffic statistics, station count, SSID, Security Mode and VLAN ID information on the AP.
#	This field is a sequential value, and it is not associated with a specific radio.
AP Description	This field displays the description of the AP.

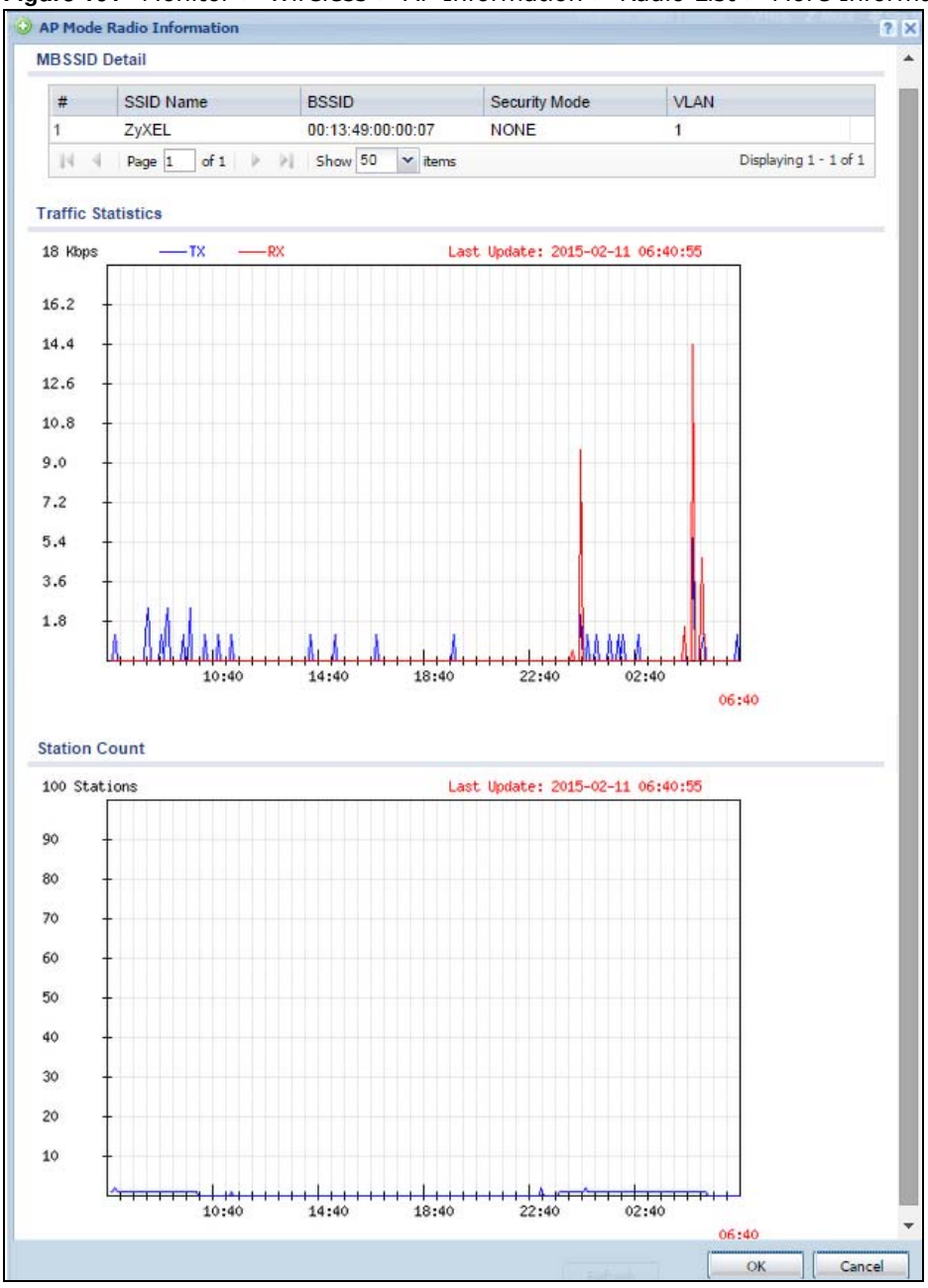
Table 46 Monitor > Wireless > Radio List

LABEL	DESCRIPTION
Model	This field displays the AP's hardware model information. It displays N/A (not applicable) only when the AP disconnects from the USG and the information is unavailable as a result.
MAC Address	This field displays the MAC address of the AP.
Radio	This field displays the Radio number. For example 1.
OP Mode	This field displays the operating mode of the AP. It displays n/a for the profile for a radio not using an AP profile. AP Mode means the AP can receive connections from wireless clients and pass their data traffic through to the USG to be managed (or subsequently passed on to an upstream gateway for managing). MON Mode means the AP monitors the broadcast area for other APs, then passes their information on to the USG. If an AP is set to this mode it cannot receive connections from wireless clients.
Profile	This field displays the AP Profile for the Radio. It displays n/A for the radio profile not using an AP profile. It displays default if using a default profile.
Frequency Band	This field displays the WLAN frequency band using the IEEE 802.11 a/b/g/n/ac standard of 2.4 or 5 GHz.
Channel ID	This field displays the WLAN channels using the IEEE 802.11 protocols.
Tx Power	This field displays the transmission power the USG is using.
Station	This field displays the station count information.
Rx PKT	This field displays the data packets of incoming traffic on the AP.
Tx PKT	This field displays the data packet of outgoing traffic on the AP.
Rx FCS Error Count	This field displays the erroneous data packet count received and detected by Frame Check Sequence (FCS)
Tx Retry Count	This field displays the data packet count that were transmitted for retry.

6.14.2 Radio List More Information

This screen allows you to view detailed information about a selected radio's SSID(s), wireless traffic and wireless clients for the preceding 24 hours. To access this window, select an entry and click the More Information button in the Radio List screen.

Figure 101 Monitor > Wireless > AP Information > Radio List > More Information



The following table describes the labels in this screen.

Table 47 Monitor > Wireless > AP Info > Radio List > More Information

LABEL	DESCRIPTION
MBSSID Detail	This list shows information about the SSID(s) that is associated with the radio.
#	This is the items sequential number in the list. It has no bearing on the actual data in this list.
SSID Name	This displays an SSID associated with this radio. There can be up to eight maximum.
BSSID	This displays the MAC address associated with the SSID.
Security Mode	This displays the security mode in which the SSID is operating.
VLAN	This displays the VLAN ID associated with the SSID.
Traffic Statistics	This graph displays the overall traffic information about the radio over the preceding 24 hours.
y-axis	This axis represents the amount of data moved across this radio per second.
x-axis	This axis represents the amount of time over which the data moved across this radio.
Station Count	This graph displays information about all the wireless clients that have connected to the radio over the preceding 24 hours.
y-axis	The y-axis represents the number of connected wireless clients.
x-axis	The x-axis shows the time over which a wireless client was connected.
Last Update	This field displays the date and time the information in the window was last updated.
OK	Click this to close this window.
Cancel	Click this to close this window.

6.14.3 Wireless Station Info

This screen displays information about connected wireless stations. Click Monitor > Wireless > Station Information to display this screen.

Figure 102 Monitor > Wireless > Station List



The following table describes the labels in this screen.

Table 48 Monitor > Wireless > Station List

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific station.
MAC Address	This field displays the MAC address of the station.
Associated AP	This field displays the AP that is associated with the station.
SSID Name	This indicates the name of the wireless network to which the station is connected. A single AP can have multiple SSIDs or networks.
Security Mode	This field displays the security mode the station is using.

Table 48 Monitor > Wireless > Station List

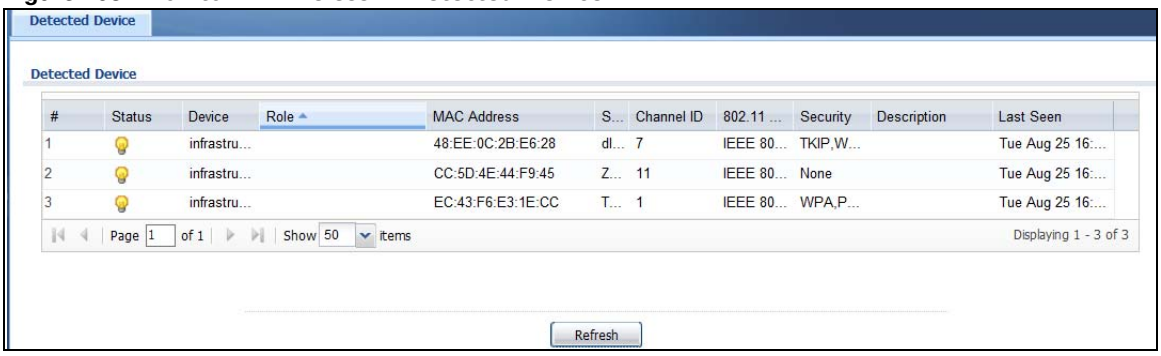
LABEL	DESCRIPTION
Signal Strength	This field displays the signal strength of the station. The signal strength mainly depends on the antenna output power and the distance between the station and the AP.
Channel	This indicates the number the channel used by the station to connect to the network.
Band	This indicates the frequency band which is currently being used by the station.
IP Address	This field displays the IP address of the station. An 169.x.x.x IP address is a private IP address that means the station didn't get the IP address from a DHCP server.
Tx Rate	This field displays the transmit data rate of the station.
Rx Rate	This field displays the receive data rate of the station.
Tx	This field displays the number of packets transmitted from the station.
Rx	This field displays the number of packets received by the station.
Association Time	This field displays the time duration the station was online and offline.
Refresh	Click this to refresh the items displayed on this page.

6.14.4 Detected Device

Use this screen to view information about wireless devices detected by the AP. Click Monitor > Wireless > Detected Device to access this screen.

Note: At least one radio of the APs connected to the USG must be set to monitor mode (in the Configuration > Wireless > AP Management screen) in order to detect other wireless devices in its vicinity.

Figure 103 Monitor > Wireless > Detected Device



The following table describes the labels in this screen.

Table 49 Monitor > Wireless > Detected Device

LABEL	DESCRIPTION
#	This is the station's index number in this list.
Status	This indicates the detected device's status.
Device	This indicates the detected device's network type (such as infrastructure or ad-hoc).
MAC Address	This indicates the detected device's MAC address.
SSID Name	This indicates the detected device's SSID.
Channel ID	This indicates the detected device's channel ID.
802.11 Mode	This indicates the 802.11 mode (a/b/g/n/ac) transmitted by the detected device.

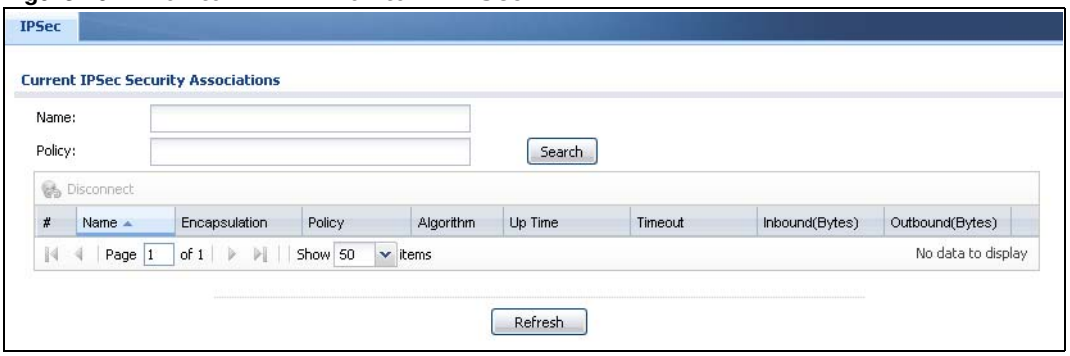
Table 49 Monitor > Wireless > Detected Device (continued)

LABEL	DESCRIPTION
Security	This indicates the encryption method (if any) used by the detected device.
Description	This displays the detected device's description. For more on managing friendly and rogue APs, see the Configuration > Wireless > MON Mode screen.
Last Seen	This indicates the last time the device was detected by the USG.
Refresh	Click this to refresh the items displayed on this page.

6.15 The IPSec Monitor Screen

You can use the IPSec Monitor screen to display and to manage active IPSec To access this screen, click Monitor > VPN Monitor > IPSec. The following screen appears. SAs. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 104 Monitor > VPN Monitor > IPSec



Each field is described in the following table.

Table 50 Monitor > VPN Monitor > IPSec

LABEL	DESCRIPTION
Name	Type the name of a IPSec SA here and click Search to find it (if it is associated). You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. See Section 6.15.1 on page 124 for more details.
Policy	Type the IP address(es) or names of the local and remote policies for an IPSec SA and click Search to find it. You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. See Section 6.15.1 on page 124 for more details.
Search	Click this button to search for an IPSec SA that matches the information you specified above.
Disconnect	Select an IPSec SA and click this button to disconnect it.
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPSec SA.
Policy	This field displays the content of the local and remote policies for this IPSec SA. The IP addresses, not the address objects, are displayed.
IKE Name	This field displays the Internet Key Exchange (IKE) name.
Cookies	This field displays the cookies information that initiates the IKE.
My Address	This field displays the IP address of local computer.

Table 50 Monitor > VPN Monitor > IPSec (continued)

LABEL	DESCRIPTION
Secure Gateway	This field displays the secure gateway information.
Up Time	This field displays how many seconds the IPSec SA has been active. This field displays N/ A if the IPSec SA uses manual keys.
Timeout	This field displays how many seconds remain in the SA life time, before the USG automatically disconnects the IPSec SA. This field displays N/ A if the IPSec SA uses manual keys.
Inbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the remote IPSec router to the USG since the IPSec SA was established.
Outbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the USG to the remote IPSec router since the IPSec SA was established.

6.15.1 Regular Expressions in Searching IPSec SAs

A question mark (?) lets a single character in the VPN connection or policy name vary. For example, use "a?c" (without the quotation marks) to specify abc, acc and so on.

Wildcards (*) let multiple VPN connection or policy names match the pattern. For example, use "*abc" (without the quotation marks) to specify any VPN connection or policy name that ends with "abc". A VPN connection named "testabc" would match. There could be any number (of any type) of characters in front of the "abc" at the end and the VPN connection or policy name would still match. A VPN connection or policy name named "testacc" for example would not match.

A * in the middle of a VPN connection or policy name has the USG check the beginning and end and ignore the middle. For example, with "abc*123", any VPN connection or policy name starting with "abc" and ending in "123" matches, no matter how many characters are in between.

The whole VPN connection or policy name has to match if you do not use a question mark or asterisk.

6.16 The SSL Screen

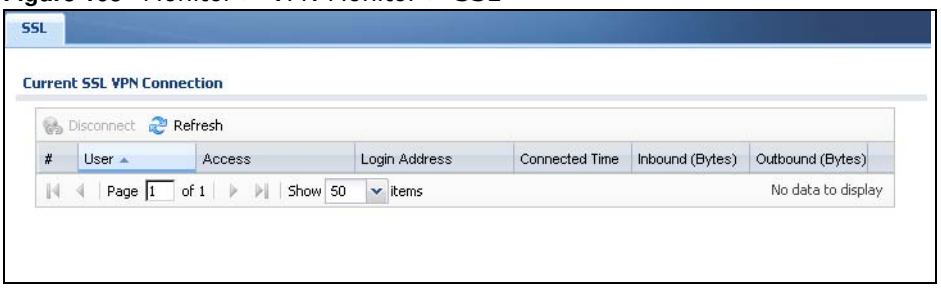
The USG keeps track of the users who are currently logged into the VPN SSL client. Click Monitor > VPN Monitor > SSL to display the user list.

Use this screen to do the following:

- View a list of active SSL VPN connections.
- Log out individual users and delete related session information.

Once a user logs out, the corresponding entry is removed from the screen.

Figure 105 Monitor > VPN Monitor > SSL



The following table describes the labels in this screen.

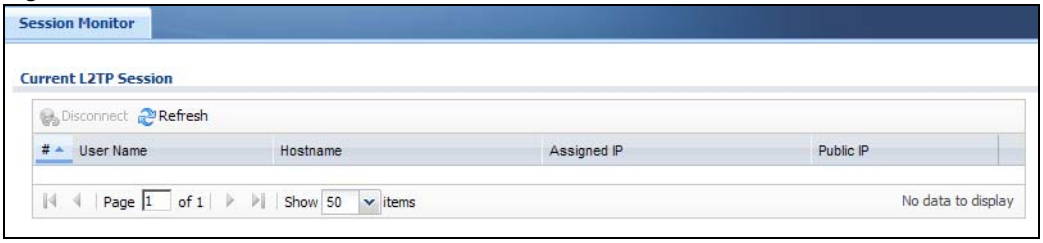
Table 51 Monitor > VPN Monitor > SSL

LABEL	DESCRIPTION
Disconnect	Select a connection and click this button to terminate the user's connection and delete corresponding session information from the USG.
Refresh	Click Refresh to update this screen.
#	This field is a sequential value, and it is not associated with a specific SSL.
User	This field displays the account user name used to establish this SSL VPN connection.
Access	This field displays the name of the SSL VPN application the user is accessing.
Login Address	This field displays the IP address the user used to establish this SSL VPN connection.
Connected Time	This field displays the time this connection was established.
Inbound (Bytes)	This field displays the number of bytes received by the USG on this connection.
Outbound (Bytes)	This field displays the number of bytes transmitted by the USG on this connection.

6.17 The L2TP over IPSec Session Monitor Screen

Click Monitor > VPN Monitor > L2TP over IPSec to open the following screen. Use this screen to display and manage the USG's connected L2TP VPN sessions.

Figure 106 Monitor > VPN Monitor > L2TP over IPSec



The following table describes the fields in this screen.

Table 52 Monitor > VPN Monitor > L2TP over IPSec

LABEL	DESCRIPTION
Disconnect	Select a connection and click this button to disconnect it.
Refresh	Click Refresh to update this screen.
#	This field is a sequential value, and it is not associated with a specific L2TP VPN session.
User Name	This field displays the remote user's user name.

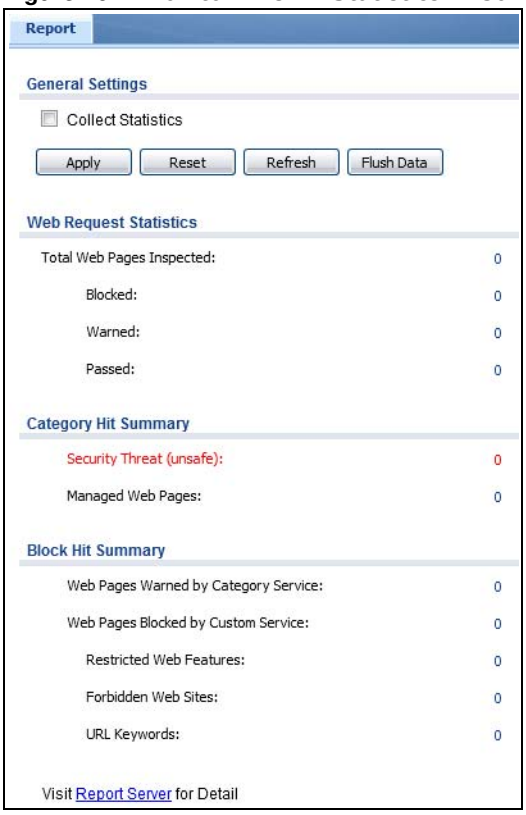
Table 52 Monitor > VPN Monitor > L2TP over IPSec (continued)

LABEL	DESCRIPTION
Hostname	This field displays the name of the computer that has this L2TP VPN connection with the USG.
Assigned IP	This field displays the IP address that the USG assigned for the remote user's computer to use within the L2TP VPN tunnel.
Public IP	This field displays the public IP address that the remote user is using to connect to the Internet.

6.18 The Content Filter Screen

Click Monitor > UTM Statistics > Content Filter to display the following screen. This screen displays content filter statistics.

Figure 107 Monitor > UTM Statistics > Content Filter



The following table describes the labels in this screen.

Table 53 Monitor > UTM Statistics > Content Filter

LABEL	DESCRIPTION
General Settings	
Collect Statistics	Select this check box to have the USG collect content filtering statistics. The collection starting time displays after you click Apply. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the USG or click Flush Data. Collecting starts over and a new collection start time displays.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics and update the report display.
Web Request Statistics	
Total Web Pages Inspected	This field displays the number of web pages that the USG's content filter feature has checked.
Blocked	This is the number of web pages that the USG blocked access.
Warned	This is the number of web pages for which the USG displayed a warning message to the access requesters.
Passed	This is the number of web pages to which the USG allowed access.
Category Hit Summary	
Security Threat (unsafe)	This is the number of requested web pages that the USG's content filtering service identified as posing a threat to users.
Managed Web Pages	This is the number of requested web pages that the USG's content filtering service identified as belonging to a category that was selected to be managed.
Block Hit Summary	
Web Pages Warned by Category Service	This is the number of web pages that matched an external database content filtering category selected in the USG and for which the USG displayed a warning before allowing users access.
Web Pages Blocked by Custom Service	This is the number of web pages to which the USG did not allow access due to the content filtering custom service configuration.
Restricted Web Features	This is the number of web pages to which the USG limited access or removed cookies due to the content filtering custom service's restricted web features configuration.
Forbidden Web Sites	This is the number of web pages to which the USG did not allow access because they matched the content filtering custom service's forbidden web sites list.
URL Keywords	This is the number of web pages to which the USG did not allow access because they contained one of the content filtering custom service's list of forbidden keywords.
Web Pages Blocked Without Policy	This is the number of web pages to which the USG did not allow access because they were not rated by the external database content filtering service.
Report Server	Click this link to go to http://www.myZyXEL.com where you can view content filtering reports after you have activated the category-based content filtering subscription service.

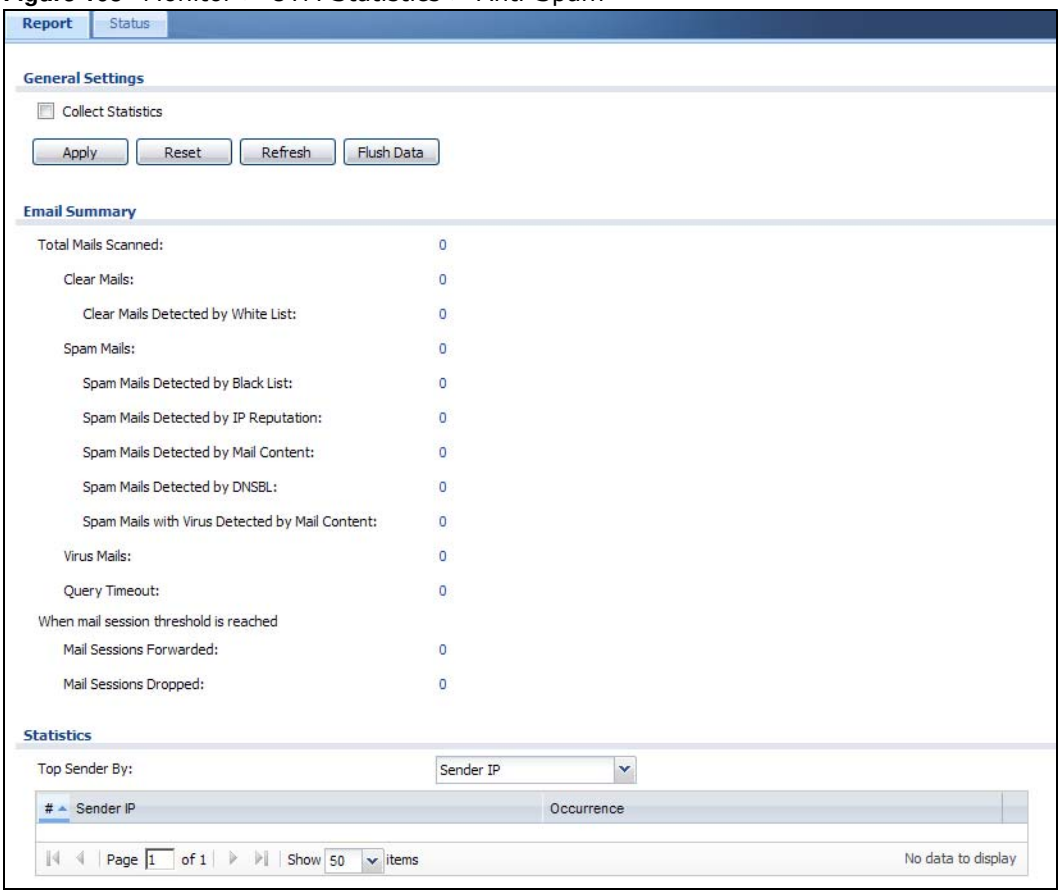
6.19 The Anti-Spam Screens

The Anti-Spam menu contains the Report and Status screens.

6.19.1 Anti-Spam Report

Click Monitor > UTM Statistics > Anti-Spam to display the following screen. This screen displays spam statistics.

Figure 108 Monitor > UTM Statistics > Anti-Spam



The following table describes the labels in this screen.

Table 54 Monitor > UTM Statistics > Anti-Spam

LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the USG collect anti-spam statistics. The collection starting time displays after you click Apply. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the USG or click Flush Data. Collecting starts over and a new collection start time displays.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.
Refresh	Click this button to update the report display.

Table 54 Monitor > UTM Statistics > Anti-Spam (continued)

LABEL	DESCRIPTION
Flush Data	Click this button to discard all of the screen's statistics and update the report display.
Total Mails Scanned	This field displays the number of e-mails that the USG's anti-spam feature has checked.
Clear Mails	This is the number of e-mails that the USG has determined to not be spam.
Clear Mails Detected by Whitelist	This is the number of e-mails that matched an entry in the USG's anti-spam white list.
Spam Mails	This is the number of e-mails that the USG has determined to be spam.
Spam Mails Detected by Black List	This is the number of e-mails that matched an entry in the USG's anti-spam black list.
Spam Mails Detected by IP Reputation	This is the number of e-mails that the USG has determined to be spam by IP Reputation. Spam or Unwanted Bulk Email is determined by the sender's IP address.
Spam Mails Detected by Mail Content	This is the number of e-mails that the USG has determined to have malicious contents.
Spam Mails Detected by DNSBL	The USG can check the sender and relay IP addresses in an e-mail's header against DNS (Domain Name Service)-based spam Black Lists (DNSBLs). This is the number of e-mails that had a sender or relay IP address in the header which matched one of the DNSBLs that the USG uses.
Spam Mails with Virus Detected by Mail Content	This is the number of e-mails that the USG has determined to have malicious contents and attached with virus.
Virus Mails	This is the number of e-mails that the USG has determined to be attached with virus.
Query Timeout	This is how many queries that were sent to the USG's configured list of DNSBL domains or Mail Scan services and did not receive a response in time.
Mail Sessions Forwarded	This is how many e-mail sessions the USG allowed because they exceeded the maximum number of e-mail sessions that the anti-spam feature can check at a time. You can see the USG's threshold of concurrent e-mail sessions in the Anti-Spam > Status screen. Use the Anti-Spam > General screen to set whether the USG forwards or drops sessions that exceed this threshold.
Mail Sessions Dropped	This is how many e-mail sessions the USG dropped because they exceeded the maximum number of e-mail sessions that the anti-spam feature can check at a time. You can see the USG's threshold of concurrent e-mail sessions in the Anti-Spam > Status screen. Use the Anti-Spam > General screen to set whether the USG forwards or drops sessions that exceed this threshold.
Top Sender By	Use this field to list the top e-mail or IP addresses from which the USG has detected the most spam. Select Sender IP to list the source IP addresses from which the USG has detected the most spam. Select Sender Email Address to list the top e-mail addresses from which the USG has detected the most spam.
#	This field displays the entry's rank in the list of the top entries.
Sender IP	This column displays when you display the entries by Sender IP. It shows the source IP address of spam e-mails that the USG has detected.

Table 54 Monitor > UTM Statistics > Anti-Spam (continued)

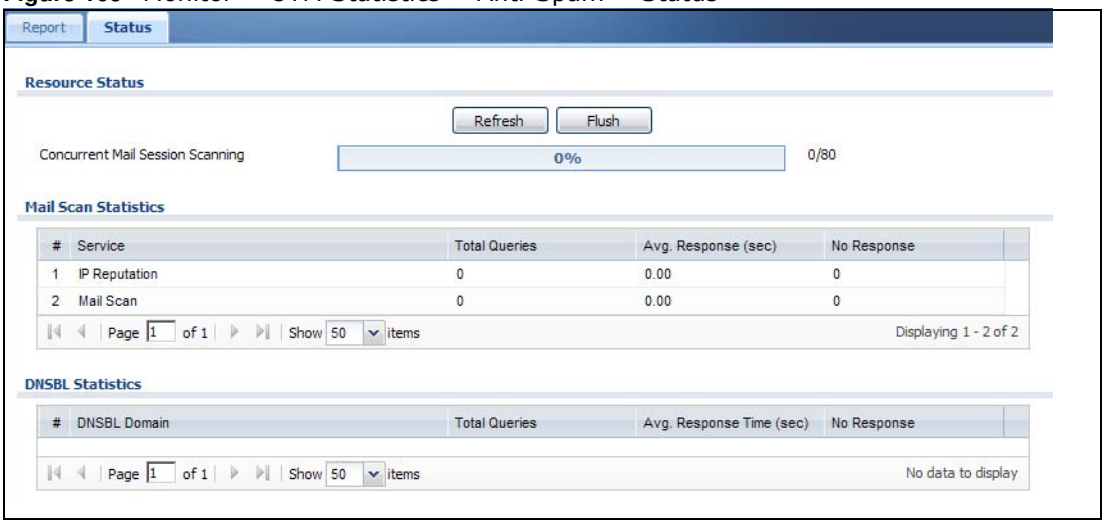
LABEL	DESCRIPTION
Sender Email Address	This column displays when you display the entries by Sender Email Address. This column displays the e-mail addresses from which the USG has detected the most spam.
Occurrence	This field displays how many spam e-mails the USG detected from the sender.

6.19.2 The Anti-Spam Status Screen

Click Monitor > UTM Statistics > Anti-Spam > Status to display the Anti-Spam Status screen.

Use the Anti-Spam Status screen to see how many e-mail sessions the anti-spam feature is scanning and statistics for the DNSBLs.

Figure 109 Monitor > UTM Statistics > Anti-Spam > Status



The following table describes the labels in this screen.

Table 55 Monitor > UTM Statistics > Anti-Spam > Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information displayed on this screen.
Flush	Click this button to clear the DNSBL statistics. This also clears the concurrent mail session scanning bar's historical high.
Concurrent Mail Session Scanning	The darker shaded part of the bar shows how much of the USG's total spam checking capability is currently being used. The lighter shaded part of the bar and the pop-up show the historical high. The first number to the right of the bar is how many e-mail sessions the USG is presently checking for spam. The second number is the maximum number of e-mail sessions that the USG can check at once. An e-mail session is when an e-mail client and e-mail server (or two e-mail servers) connect through the USG.
Mail Scan Statistics	These are the statistics for the service the USG uses. These statistics are for when the USG actually queries the service servers.
#	This is the entry's index number in the list.
Service	This displays the name of the service.
Total Queries	This is the total number of queries the USG has sent to this service.

Table 55 Monitor > UTM Statistics > Anti-Spam > Status (continued)

LABEL	DESCRIPTION
Avg. Response Time (sec)	This is the average for how long it takes to receive a reply from this service.
No Response	This is how many queries the USG sent to this service without receiving a reply.
DNSBL Statistics	These are the statistics for the DNSBL the USG uses. These statistics are for when the USG actually queries the DNSBL servers. Matches for DNSBL responses stored in the cache do not affect these statistics.
#	This is the entry's index number in the list.
DNSBL Domain	These are the DNSBLs the USG uses to check sender and relay IP addresses in e-mails.
Total Queries	This is the total number of DNS queries the USG has sent to this DNSBL.
Avg. Response Time (sec)	This is the average for how long it takes to receive a reply from this DNSBL.
No Response	This is how many DNS queries the USG sent to this DNSBL without receiving a reply.

6.20 Log Screens

Log messages are stored in two separate logs, one for regular log messages and one for debugging messages. In the regular log, you can look at all the log messages by selecting All Logs, or you can select a specific category of log messages (for example, security policy or user). You can also look at the debugging log by selecting Debug Log. All debugging messages have the same priority.

6.20.1 View Log

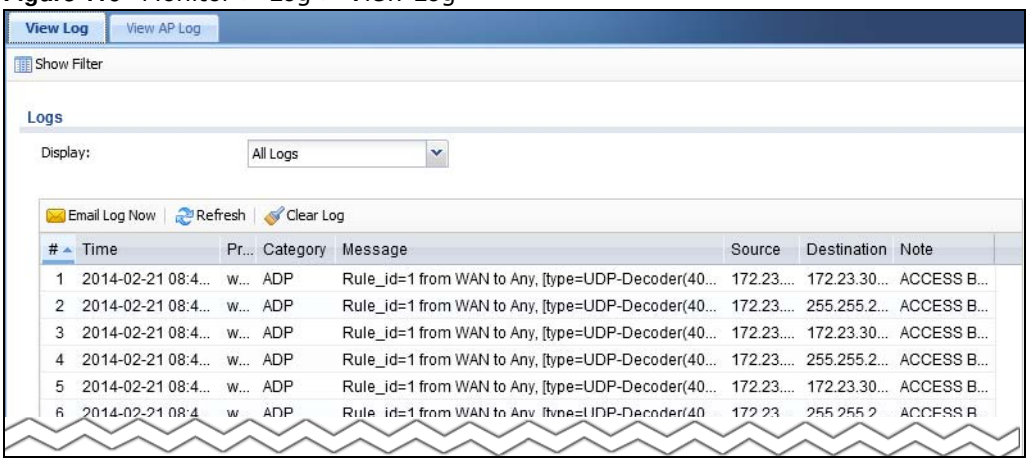
To access this screen, click Monitor > Log. The log is displayed in the following screen.

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

- The maximum possible number of log messages in the USG varies by model.

Events that generate an alert (as well as a log message) display in red. Regular logs display in black. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order. The Web Configurator saves the filter settings if you leave the View Log screen and return to it later.

Figure 110 Monitor > Log > View Log



The following table describes the labels in this screen.

Table 56 Monitor > Log > View Log

LABEL	DESCRIPTION
Show Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the Display, Email Log Now, Refresh, and Clear Log fields are available. If the filter settings are shown, the Display, Priority, Source Address, Destination Address, Service, Keyword, and Search fields are available.
Display	Select the category of log message(s) you want to view. You can also view All Logs at one time, or you can view the Debug Log.
Email Log Now	Click this button to send log message(s) to the Active e-mail address(es) specified in the Send Log To field on the Log Settings page.
Refresh	Click this button to update the information in the screen.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: any, emerg, alert, crit, error, warn, notice, and info, from highest priority to lowest priority. This field is read-only if the Category is Debug Log.
Category	This field displays the log that generated the log message. It is the same value used in the Display and (other) Category fields.
Message	This field displays the reason the log message was generated. The text "[count=*x*]", where *x* is a number, appears at the end of the Message field if log consolidation is turned on and multiple entries were aggregated to generate into this one.
Source	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.
Destination	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.

Table 56 Monitor > Log > View Log (continued)

LABEL	DESCRIPTION
Priority	This field displays the priority of the log message. It has the same range of values as the Priority field above.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Note	This field displays any additional information about the log message.

7 Licensing

7.1 Registration Overview

Use the Configuration > Licensing > Registration screens to register your USG and manage its service subscriptions.

- Use the Registration screen (see Section 7.1.2 on page 135) to go to portal.myzyxel.com to register your USG and activate a service, such as content filtering.
- Use the Service screen (see Section 7.1.3 on page 135) to display the status of your service registrations and upgrade licenses.

Note: The USG models need a license for UTM (Unified Threat management) functionality.

7.1.1 What you Need to Know

This section introduces the topics covered in this chapter.

myZyXEL.com

myZyXEL.com is ZyXEL's online services center where you can register your USG and manage subscription services available for the USG. To update signature files or use a subscription service, you have to register the USG and activate the corresponding service at myZyXEL.com (through the USG).

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

You need your USG's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

Subscription Services Available

The USG can use anti-spam, SSL VPN, and content filtering subscription services.

The USG models need a license for UTM (Unified Threat Management) functionality - see Section 1.1 on page 19 for details.

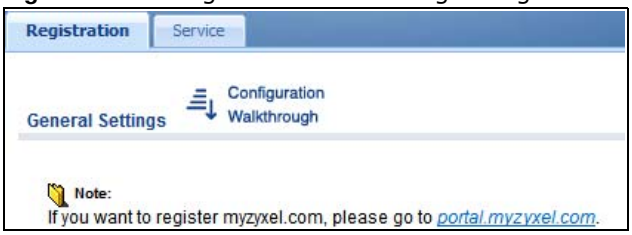
You can purchase an iCard and enter the license key from it, at www.myzyxel.com to have the USG use UTM services or have the USG use more SSL VPN tunnels. See below the respective chapters in this guide for more information about UTM features.

7.1.2 Registration Screen

Click the link in this screen to register your USG at myZyXEL.com. The USG should already have Internet access before you can access it. Click Configuration > Licensing > Registration in the navigation panel to open the screen as shown next.

Click on the icon to go to the OneSecurity.com website where there is guidance on configuration walkthrough and other information.

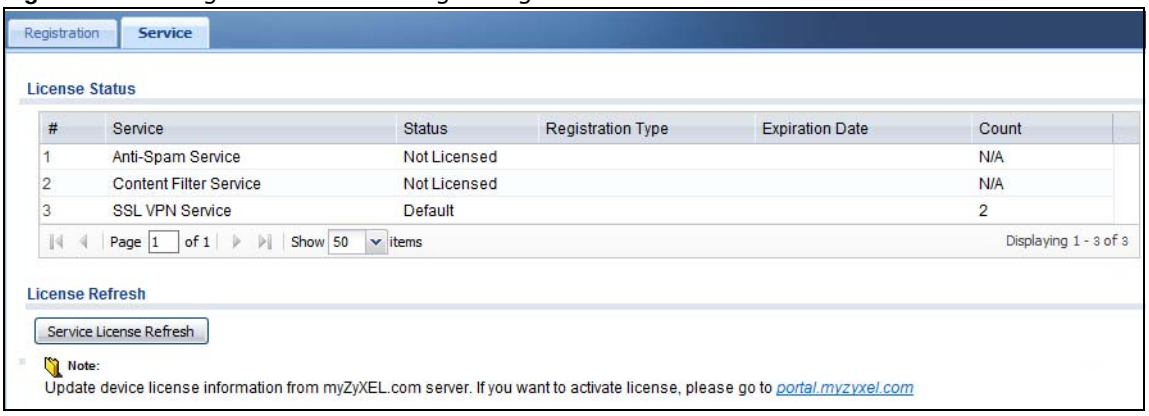
Figure 111 Configuration > Licensing > Registration > portal.myzyxel.com



7.1.3 Service Screen

Use this screen to display the status of your service registrations and upgrade licenses. To activate or extend a standard service subscription, purchase an iCard and enter the iCard's PIN number (license key) in this screen. Click Configuration > Licensing > Registration > Service to open the screen as shown next.

Figure 112 Configuration > Licensing > Registration > Service



The following table describes the labels in this screen.

Table 57 Configuration > Licensing > Registration > Service

LABEL	DESCRIPTION
License Status	
#	This is the entry's position in the list.
Service	This lists the services that available on the USG.
Status	This field displays whether a service is activated (Licensed) or not (Not Licensed) or expired (Expired).
Registration Type	This field displays whether you applied for a trial application (Trial) or registered a service with your iCard's PIN number (Standard). This field is blank when a service is not activated.

Table 57 Configuration > Licensing > Registration > Service (continued)

LABEL	DESCRIPTION
Expiration Date	This field displays the date your service expires.
Count	This field displays how many VPN tunnels you can use with your current license. This field does not apply to the other services.
Service License Refresh	Click this button to renew service license information (such as the registration status and expiration day).

8 Wireless

8.1 Overview

Use the Wireless screens to configure how the USG manages the Access Points (APs) that are connected to it.

8.1.1 What You Can Do in this Chapter

- The AP Management screen (Section 8.2 on page 138) manages all of the APs connected to the USG.
- The DCS screen (Section 8.2 on page 138) configures dynamic radio channel selection.

8.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Station / Wireless Client

A station or wireless client is any wireless-capable device that can connect to an AP using a wireless signal.

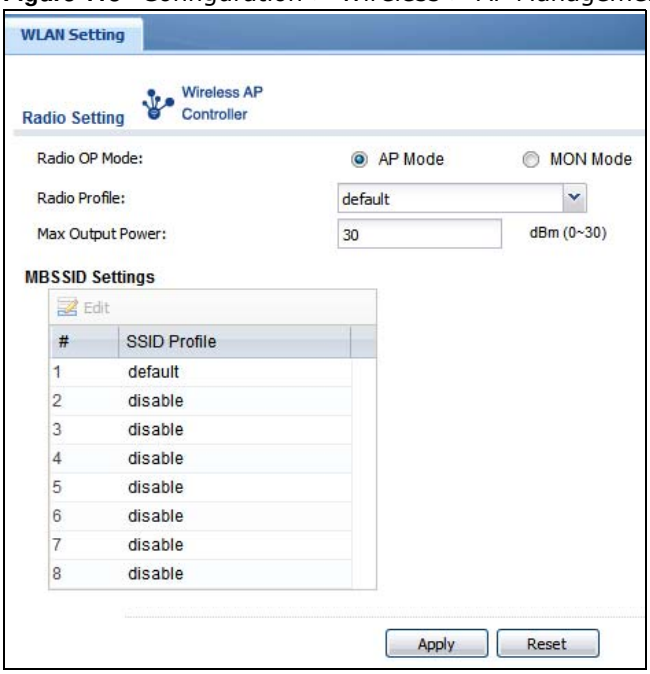
Dynamic Channel Selection (DCS)

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel upon which it broadcasts by scanning the area around it and determining what channels are currently being used by other devices.

8.2 AP Management Screen

Use this screen to manage the USG's general wireless settings. Click Configuration > Wireless > AP Management to access this screen.

Figure 113 Configuration > Wireless > AP Management



Each field is described in the following table.

Table 58 Configuration > Wireless > AP Management

LABEL	DESCRIPTION
Radio Setting	
Radio OP Mode	Select the operating mode. AP Mode means the radio can receive connections from wireless clients and pass their data traffic through to the USG to be managed (or subsequently passed on to an upstream gateway for managing). MON Mode means the radio monitors the broadcast area for other APs, then passes their information on to the USG where it can be determined if those APs are friendly or rogue. If a radio is set to this mode it cannot receive connections from wireless clients.
Radio Profile	Select the radio profile the radio uses.
Max Output Power	Enter the output power (between 0 to 30 dBm) of the USG in this field. If there is a high density of APs in an area, decrease the output power of the USG to reduce interference with other APs. Note: Reducing the output power also reduces the USG's effective broadcast radius.
MBSSID Settings	
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
#	This field shows the index number of the SSID
SSID Profile	This field displays the SSID profile that is associated with the radio profile.

Table 58 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to close the window with changes unsaved.

8.3 DCS Screen

Use this screen to configure dynamic radio channel selection. Click Configuration > Wireless > DCS to access this screen.

Figure 114 Configuration > Wireless > DCS



Each field is described in the following table.

Table 59 Configuration > Wireless > DCS

LABEL	DESCRIPTION
Select Now	Click this to have the USG scan for and select an available channel immediately.

8.4 Technical Reference

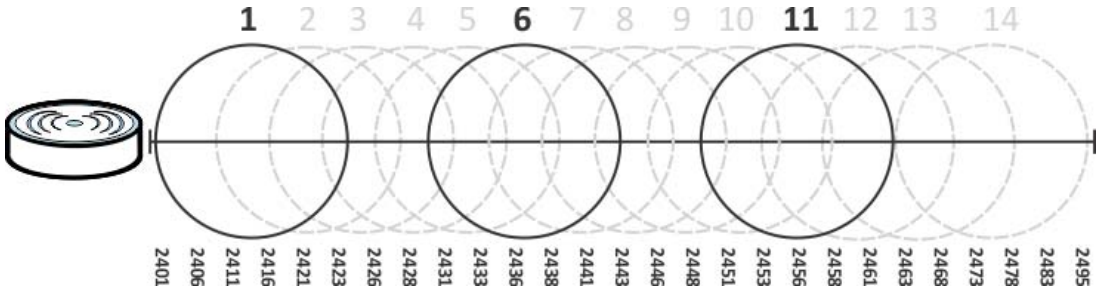
The following section contains additional technical information about the features described in this chapter.

8.4.1 Dynamic Channel Selection

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of interference. Dynamic channel selection frees the network administrator from this task by letting the AP do it automatically. The AP can scan the area around it looking for the channel with the least amount of interference.

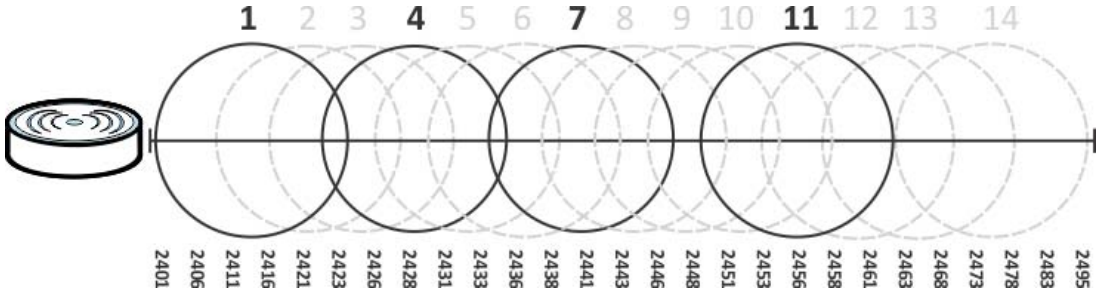
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

Figure 115 An Example Three-Channel Deployment



Three channels are situated in such a way as to create almost no interference with one another if used exclusively: 1, 6 and 11. When an AP broadcasts on any of these three channels, it should not interfere with neighboring APs as long as they are also limited to same trio.

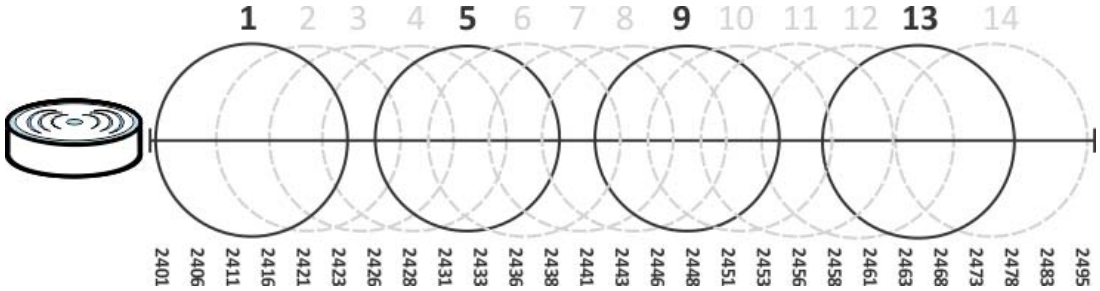
Figure 116 An Example Four-Channel Deployment



However, some regions require the use of other channels and often use a safety scheme with the following four channels: 1, 4, 7 and 11. While they are situated sufficiently close to both each other and the three so-called "safe" channels (1,6 and 11) that interference becomes inevitable, the severity of it is dependent upon other factors: proximity to the affected AP, signal strength, activity, and so on.

Finally, there is an alternative four channel scheme for ETSI, consisting of channels 1, 5, 9, 13. This offers significantly less overlap that the other one.

Figure 117 An Alternative Four-Channel Deployment



9

Interfaces

9.1 Interface Overview

Use the Interface screens to configure the USG's interfaces. You can also create interfaces on top of other interfaces.

- Ports are the physical ports to which you connect cables.
- Interfaces are used within the system operationally. You use them in configuring various features. An interface also describes a network that is directly connected to the USG. For example, You connect the LAN network to the LAN interface.
- Zones are groups of interfaces used to ease security policy configuration.

9.1.1 What You Can Do in this Chapter

- Use the Port Role screen (Section 9.2 on page 146) to create port groups and to assign physical ports and port groups to Ethernet interfaces.
- Use the Ethernet screens (Section 9.3 on page 147) to configure the Ethernet interfaces. Ethernet interfaces are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- Use the PPP screens (Section 9.4 on page 167) for PPPoE or PPTP Internet connections.
- Use the Cellular screens (Section 9.5 on page 174) to configure settings for interfaces for Internet connections through an installed mobile broadband card.
- Use the Tunnel screens (Section 9.6 on page 183) to configure tunnel interfaces to be used in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels.
- Use the VLAN screens (Section 9.7 on page 189) to divide the physical network into multiple logical networks. VLAN interfaces receive and send tagged frames. The USG automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- Use the Bridge screens (Section 9.8 on page 202) to combine two or more network segments into a single network.
- Use the Auxiliary screens (Section 9.9 on page 214) to configure the USG's auxiliary interface to use an external modem.
- Use the Virtual Interface screen (Section 9.9.1 on page 214) to create virtual interfaces on top of Ethernet interfaces to tell the USG where to route packets. You can create virtual Ethernet interfaces, virtual VLAN interfaces, and virtual bridge interfaces.
- Use the Trunk screens (Section 9.11 on page 219) to configure load balancing.

9.1.2 What You Need to Know

Interface Characteristics

Interfaces generally have the following characteristics (although not all characteristics apply to each type of interface).

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

Types of Interfaces

You can create several types of interfaces in the USG.

- Setting interfaces to the same port role forms a port group. Port groups creates a hardware connection between physical ports at the layer-2 (data link, MAC address) level. Port groups are created when you uUse the Interface > Port Roles or Interface > Port Groups screen to set multiple physical ports to be part of the same interface.
- Ethernet interfaces are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- Tunnel interfaces send IPv4 or IPv6 packets from one network to a specific network through the Internet or a public network.
- VLAN interfaces receive and send tagged frames. The USG automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- Bridge interfaces create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the USG. You can also assign an IP address and subnet mask to the bridge.
- PPP interfaces support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- Cellular interfaces are for mobile broadband WAN connections via a connected mobile broadband device.
- Virtual interfaces provide additional routing information in the USG. There are three types: virtual Ethernet interfaces, virtual VLAN interfaces, and virtual bridge interfaces.
- Trunk interfaces manage load balancing between interfaces.

Port groups and trunks have a lot of characteristics that are specific to each type of interface. The other types of interfaces--Ethernet, PPP, cellular, VLAN, bridge, and virtual--have a lot of similar

characteristics. These characteristics are listed in the following table and discussed in more detail below.

Table 60 Ethernet, PPP, Cellular, VLAN, Bridge, and Virtual Interface Characteristics

CHARACTERISTICS	ETHERNET	ETHERNET	PPP	CELLULAR	VLAN	BRIDGE	VIRTUAL
Name*	wan1, wan2	lan1, lan2, dmz	ppp*x*	cellular*x*	vlan*x*	br*x*	**
Configurable Zone	No	No	Yes	Yes	Yes	Yes	No
IP Address Assignment							
Static IP address	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	No	Yes	Yes	Yes	Yes	No
Routing metric	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Interface Parameters							
Bandwidth restrictions	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Packet size (MTU)	Yes	Yes	Yes	Yes	Yes	Yes	No
DHCP							
DHCP server	No	Yes	No	No	Yes	Yes	No
DHCP relay	No	Yes	No	No	Yes	Yes	No
Connectivity Check	Yes	No	Yes	Yes	Yes	Yes	No

Note: - * The format of interface names other than the Ethernet and ppp interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (*x*). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, Ethernet interface names are wan1, wan2, lan1, lan2, dmz; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the Web Configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

Relationships Between Interfaces

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

Table 61 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
Ethernet interface	physical port
VLAN interface	Ethernet interface
bridge interface	Ethernet interface* VLAN interface*

Table 61 Relationships Between Different Types of Interfaces (continued)

INTERFACE	REQUIRED PORT / INTERFACE
PPP interface	Ethernet interface* VLAN interface* bridge interface WAN1, WAN2, OPT*
virtual interface (virtual Ethernet interface) (virtual VLAN interface) (virtual bridge interface)	 Ethernet interface* VLAN interface* bridge interface
trunk	Ethernet interface Cellular interface VLAN interface bridge interface PPP interface

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

IPv6 Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address

compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) from the left is the network prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 62 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the USG's WAN interface is connected to an ISP with a router and the USG is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates another address which combines its interface ID and global and subnet information advertised from the router. (In IPv6, all network interfaces can be associated with several addresses.) This is a routable global IP address.

Prefix Delegation

Prefix delegation enables an IPv6 router (the USG) to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The USG uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the router passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

IPv6 Router Advertisement

An IPv6 router sends router advertisement messages periodically to advertise its presence and other parameters to the hosts in the same network.

DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

9.1.3 What You Need to Do First

For IPv6 settings, go to the Configuration > System > IPv6 screen to enable IPv6 support on the USG first.

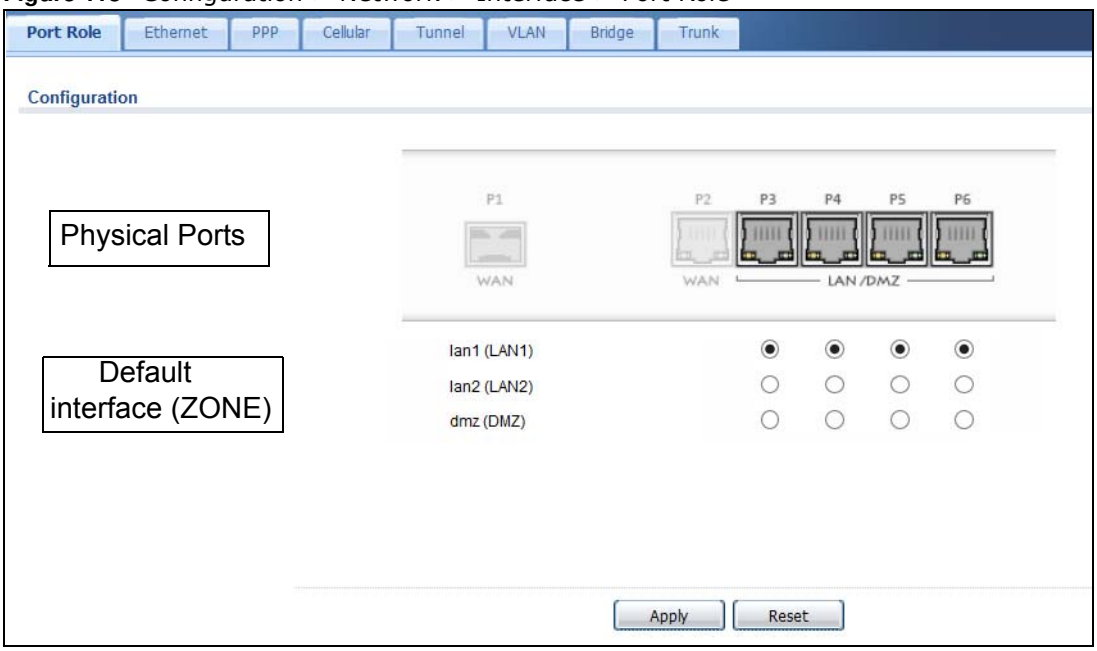
9.2 Port Role Screen

To access this screen, click Configuration > Network > Interface > Port Role. Use the Port Role screen to set the USG's flexible ports as part of the lan1, lan2, or dmz interfaces. This creates a hardware connection between the physical ports at the layer-2 (data link, MAC address) level. This provides wire-speed throughput but no security.

Note the following if you are configuring from a computer connected to a lan1, lan2, or dmz port and change the port's role:

- A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the USG's lan1, lan2, or dmz IP address.
- Use the appropriate lan1, lan2, or dmz IP address to access the USG.

Figure 118 Configuration > Network > Interface > Port Role



The physical Ethernet ports are shown at the top and the Ethernet interfaces and zones are shown at the bottom of the screen. Use the radio buttons to select for which interface (network) you want to use each physical port. For example, select a port's LAN radio button to use the port as part of the LAN interface. The port will use the USG's LAN IP address and MAC address.

When you assign more than one physical port to a network, you create a port group. Port groups have the following characteristics:

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

Click Apply to save your changes and apply them to the USG.

Click Reset to change the port groups to their current configuration (last-saved values).

9.3 Ethernet Summary Screen

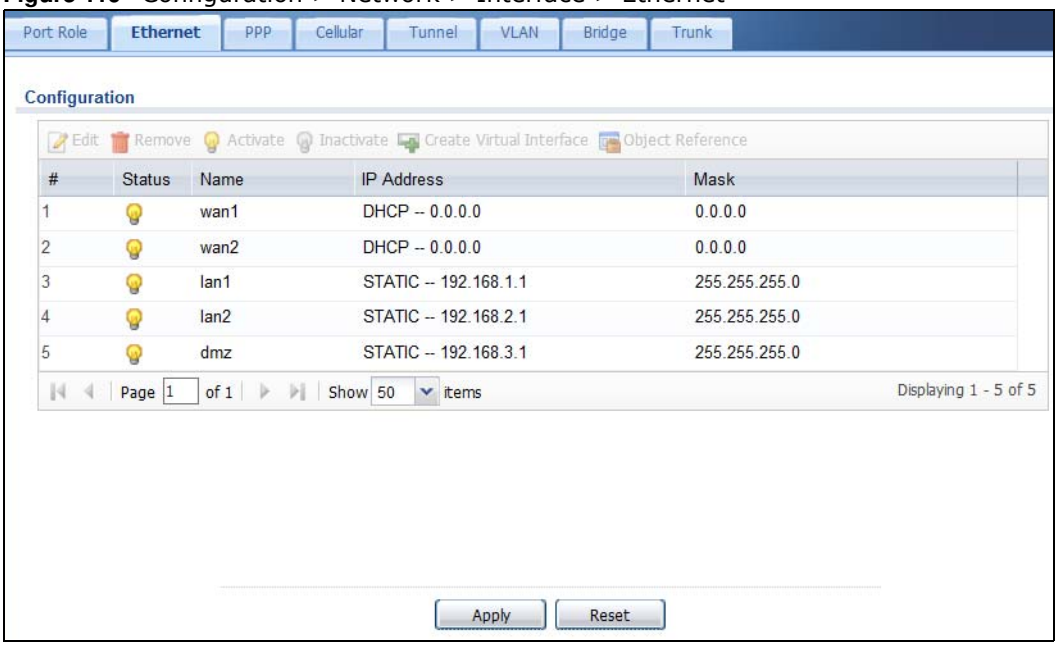
This screen lists every Ethernet interface and virtual interface created on top of Ethernet interfaces. If you enabled IPv6 in the Configuration > System > IPv6 screen, you can also configure Ethernet interfaces used for your IPv6 networks on this screen. To access this screen, click Configuration > Network > Interface > Ethernet.

Unlike other types of interfaces, you cannot create new Ethernet interfaces nor can you delete any of them. If an Ethernet interface does not have any physical ports assigned to it, the Ethernet interface is effectively removed from the USG, but you can still configure it.

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

Use Ethernet interfaces to control which physical ports exchange routing information with other routers and how much information is exchanged through each one. The more routing information is exchanged, the more efficient the routers should be. However, the routers also generate more network traffic, and some routing protocols require a significant amount of configuration and management. The USG supports two routing protocols, RIP and OSPF. See Chapter 10 on page 239 for background information about these routing protocols.

Figure 119 Configuration > Network > Interface > Ethernet



Each field is described in the following table.

Table 63 Configuration > Network > Interface > Ethernet

LABEL	DESCRIPTION
Configuration / IPv6 Configuration	Use the Configuration section for IPv4 network settings. Use the IPv6 Configuration section for IPv6 network settings if you connect your USG to an IPv6 network. Both sections have similar fields as described below.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a virtual interface, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an interface, select it and click Activate.
Inactivate	To turn off an interface, select it and click Inactivate.
Create Virtual Interface	To open the screen where you can create a virtual Ethernet interface, select an Ethernet interface and click Create Virtual Interface.
Object References	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.

Table 63 Configuration > Network > Interface > Ethernet (continued)

LABEL	DESCRIPTION
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0 (in the IPv4 network) or :: (in the IPv6 network), the interface does not have an IP address yet. In the IPv4 network, this screen also shows whether the IP address is a static IP address (STATIC) or dynamically assigned (DHCP). IP addresses are always static in virtual interfaces. In the IPv6 network, this screen also shows whether the IP address is a static IP address (STATIC), link-local IP address (LINK LOCAL), dynamically assigned (DHCP), or an IPv6 StateLess Address AutoConfiguration IP address (SLAAC). See Section 9.1.2 on page 142 for more information about IPv6.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

9.3.1 Ethernet Edit

The Ethernet Edit screen lets you configure IP address assignment, interface parameters, RIP settings, OSPF settings, DHCP settings, connectivity check, and MAC address settings. To access this screen, click an Edit icon in the Ethernet Summary screen. (See Section 9.3 on page 147.)

The OPT interface's Edit > Configuration screen is shown here as an example. The screens for other interfaces are similar and contain a subset to the OPT interface screen's fields.

Note: If you create IP address objects based on an interface's IP address, subnet, or gateway, the USG automatically updates every rule or setting that uses the object whenever the interface's IP address settings change. For example, if you change the LAN's IP address, the USG automatically updates the corresponding interface-based, LAN subnet address object.

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

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

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

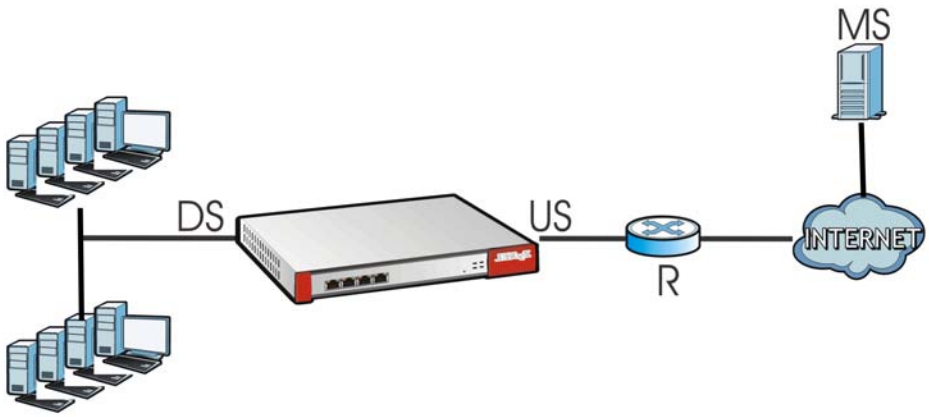
- Enable and disable OSPF in the underlying physical port or port group.
- Select the area to which the interface belongs.
- Override the default link cost and authentication method for the selected area.
- Select in which direction(s) routing information is exchanged - The USG can receive routing information, send routing information, or do both.

Set the priority used to identify the DR or BDR if one does not exist.

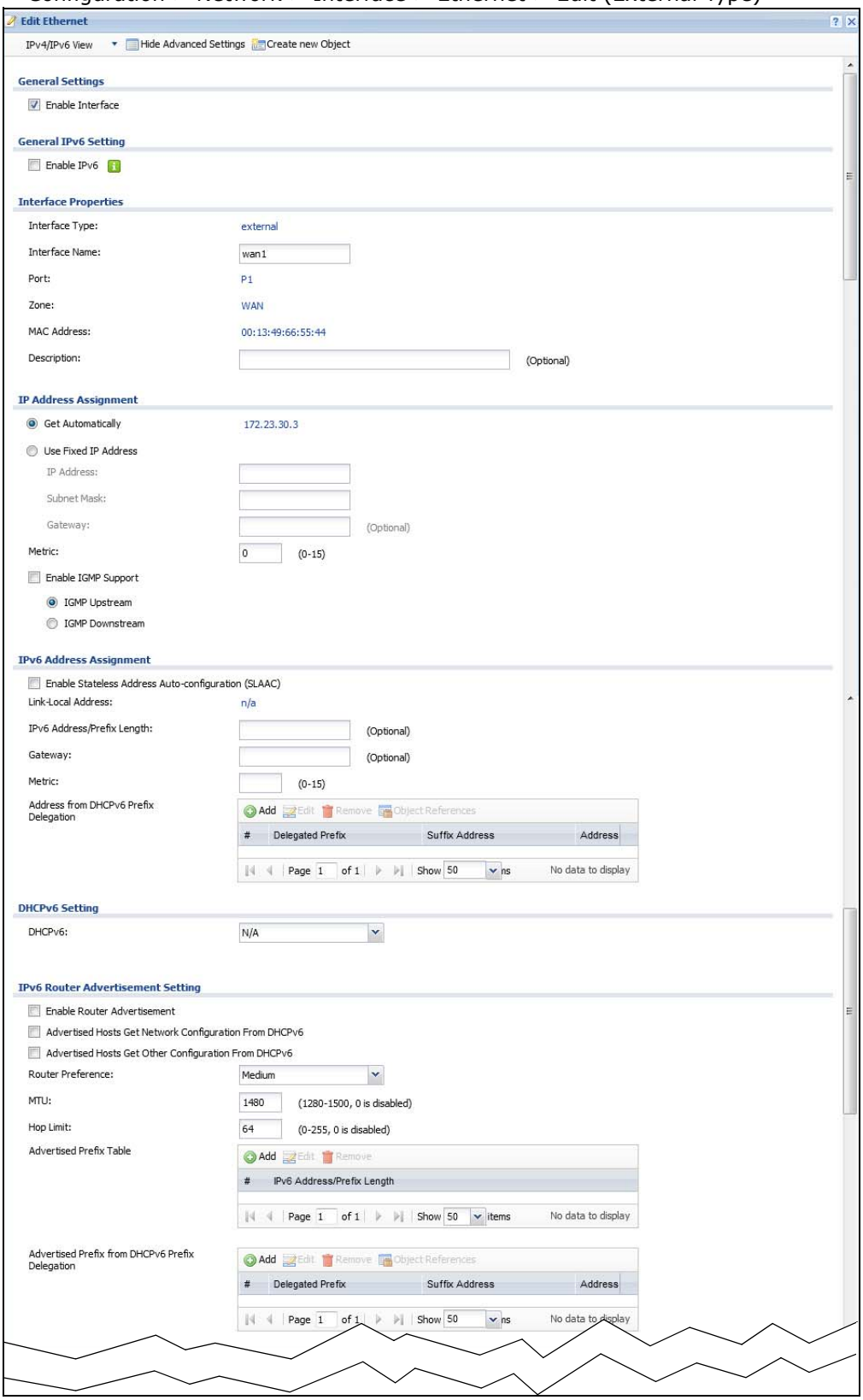
IGMP Proxy

Internet Group Management Protocol (IGMP) proxy is used for multicast routing. IGMP proxy enables the USG to issue IGMP host messages on behalf of hosts that the USG discovered on its IGMP-enabled interfaces. The USG acts as a proxy for its hosts. Refer to the following figure.

- DS: Downstream traffic
- US: Upstream traffic
- R: Router
- MS: Multicast Server
- Enable IGMP Upstream (US) on the USG interface that connects to a router (R) running IGMP that is closer to the multicast server (MS).
- Enable IGMP Downstream on the USG interface which connects to the multicast hosts.



- Configuration > Network > Interface > Ethernet > Edit (External Type)



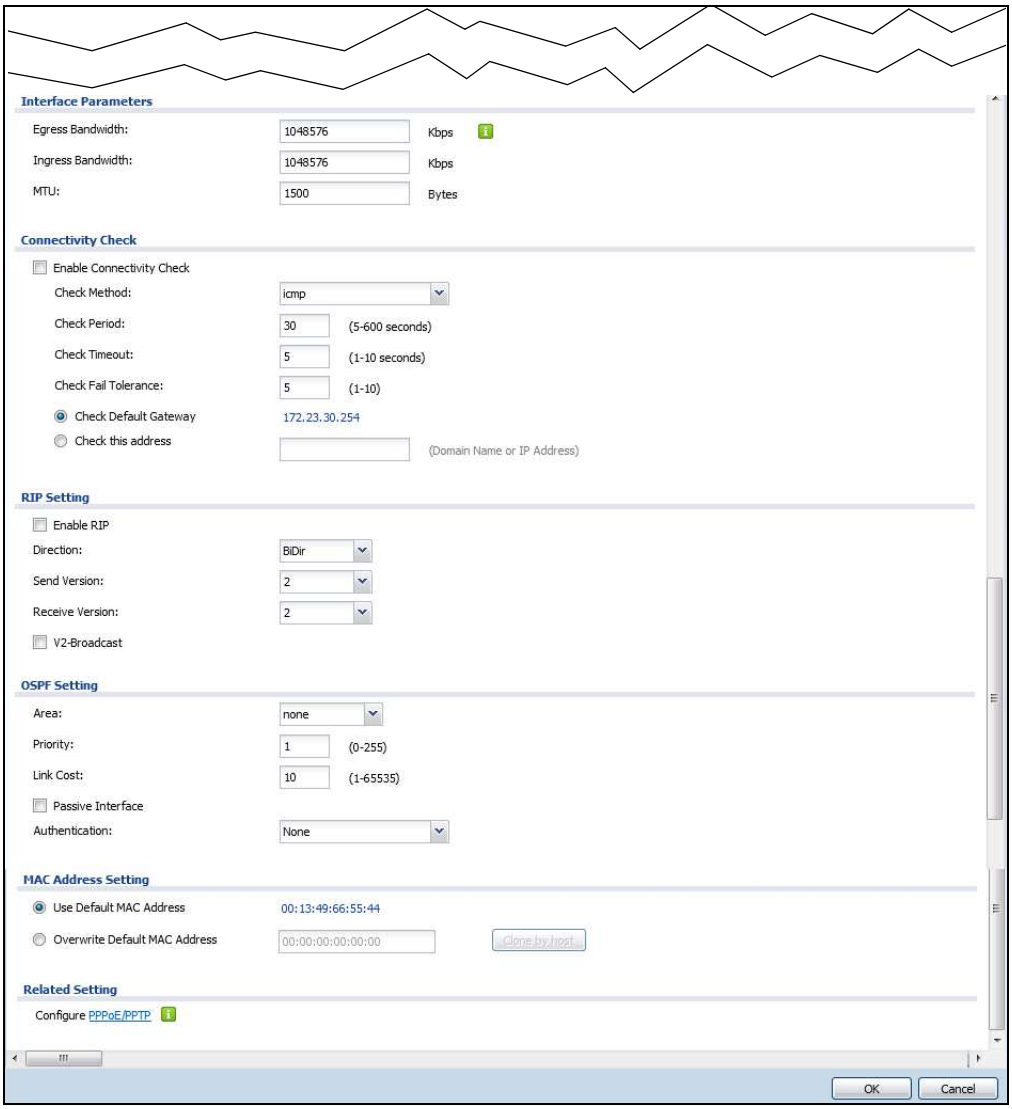
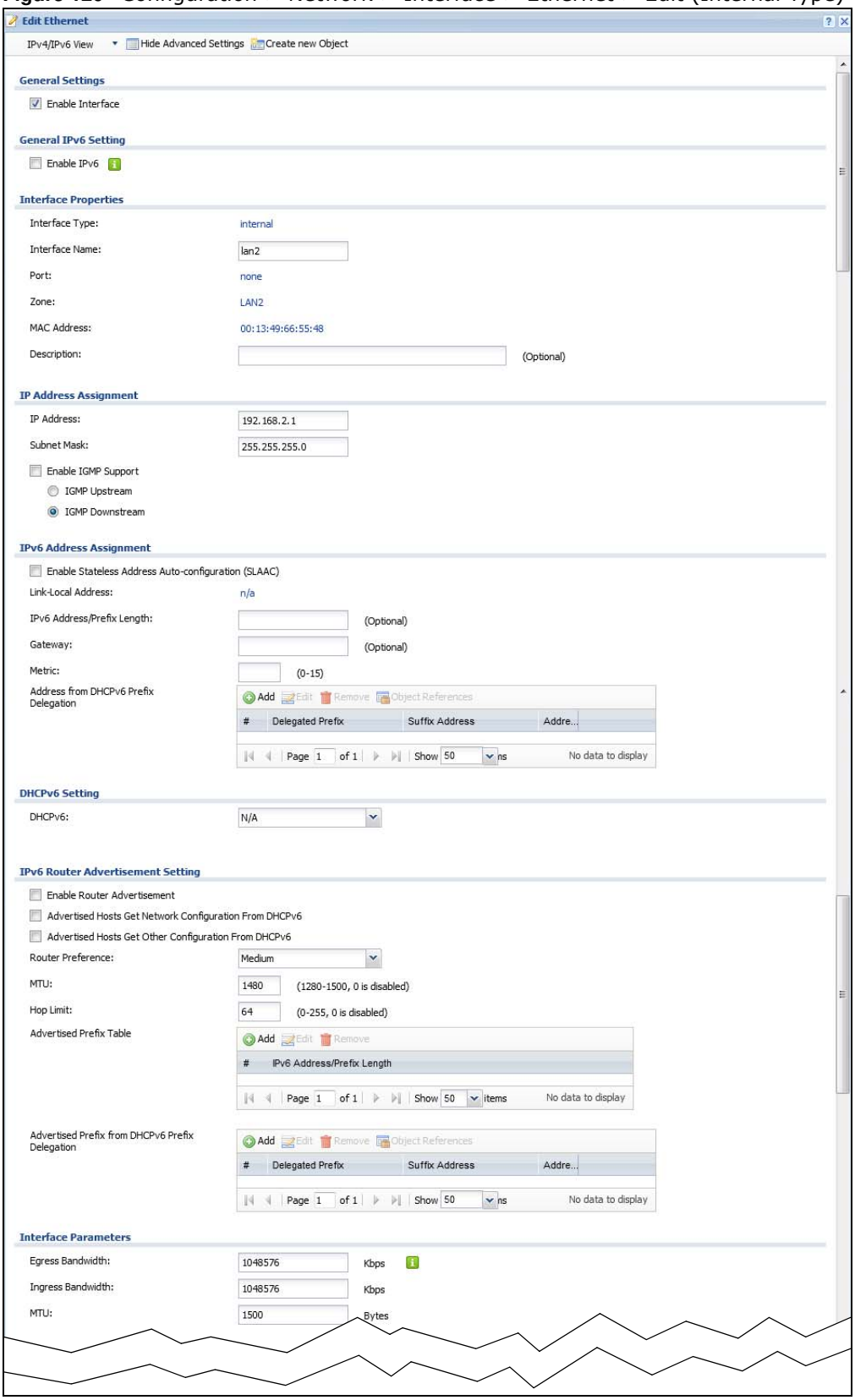

Interface Parameters
Egress Bandwidth: 1048576 Kbps
Ingress Bandwidth: 1048576 Kbps
MTU: 1500 Bytes
Connectivity Check
Enable Connectivity Check
Check Method: icmp
Check Period: 30 (5-600 seconds)
Check Timeout: 5 (1-10 seconds)
Check Fail Tolerance: 5 (1-10)
Check Default Gateway 172.23.30.254
Check this address (Domain Name or IP Address)
RIP Setting
Enable RIP
Direction: BiDir
Send Version: 2
Receive Version: 2
V2-Broadcast
OSPF Setting
Area: none
Priority: 1 (0-255)
Link Cost: 10 (1-65535)
Passive Interface
Authentication: None
MAC Address Setting
Use Default MAC Address 00:13:49:66:55:44
Overwrite Default MAC Address 00:00:00:00:00:00 Clone by host...
Related Setting
Configure PPPoE/PPTP
OK
Cancel

Figure 120 Configuration > Network > Interface > Ethernet > Edit (Internal Type)



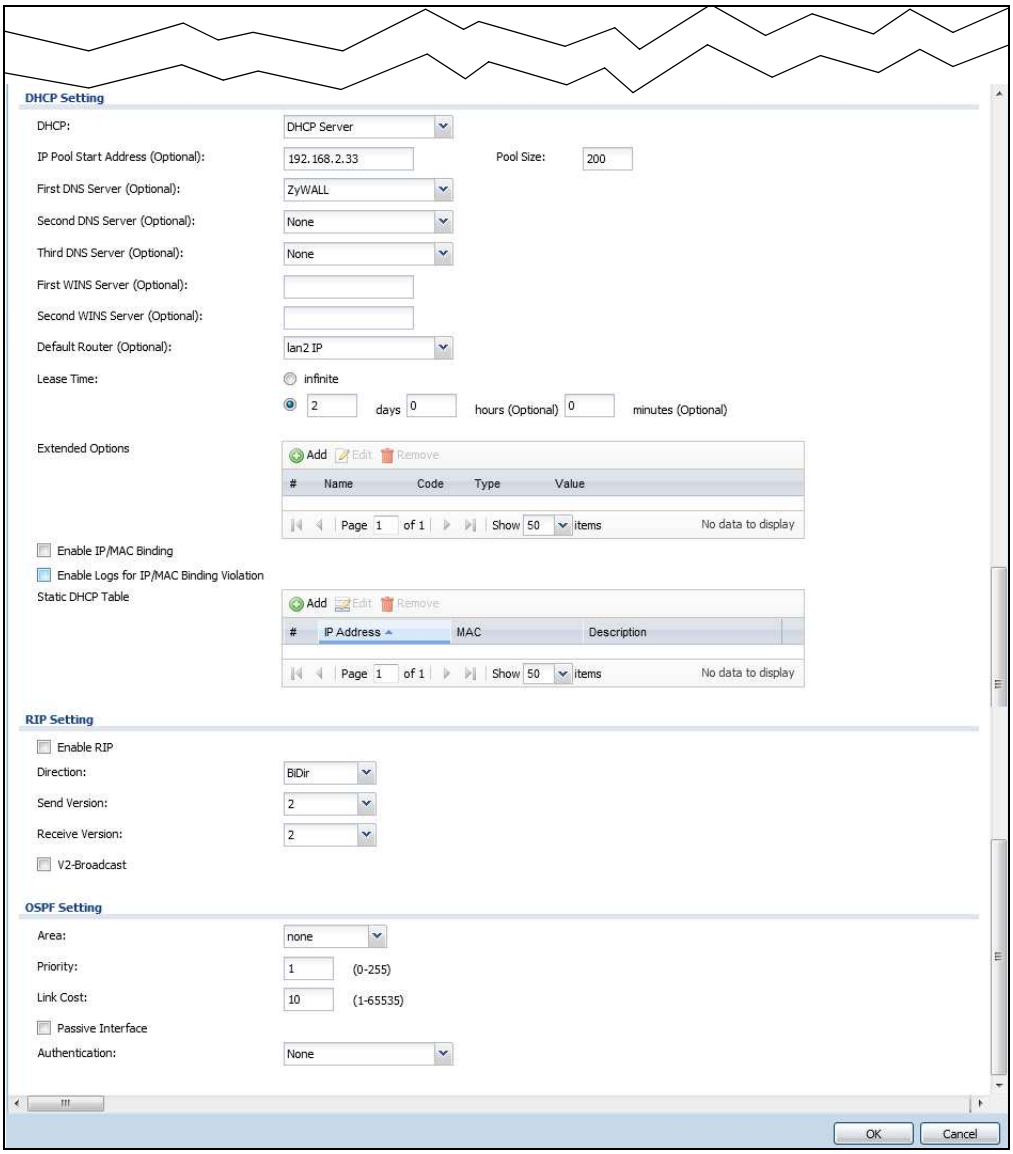
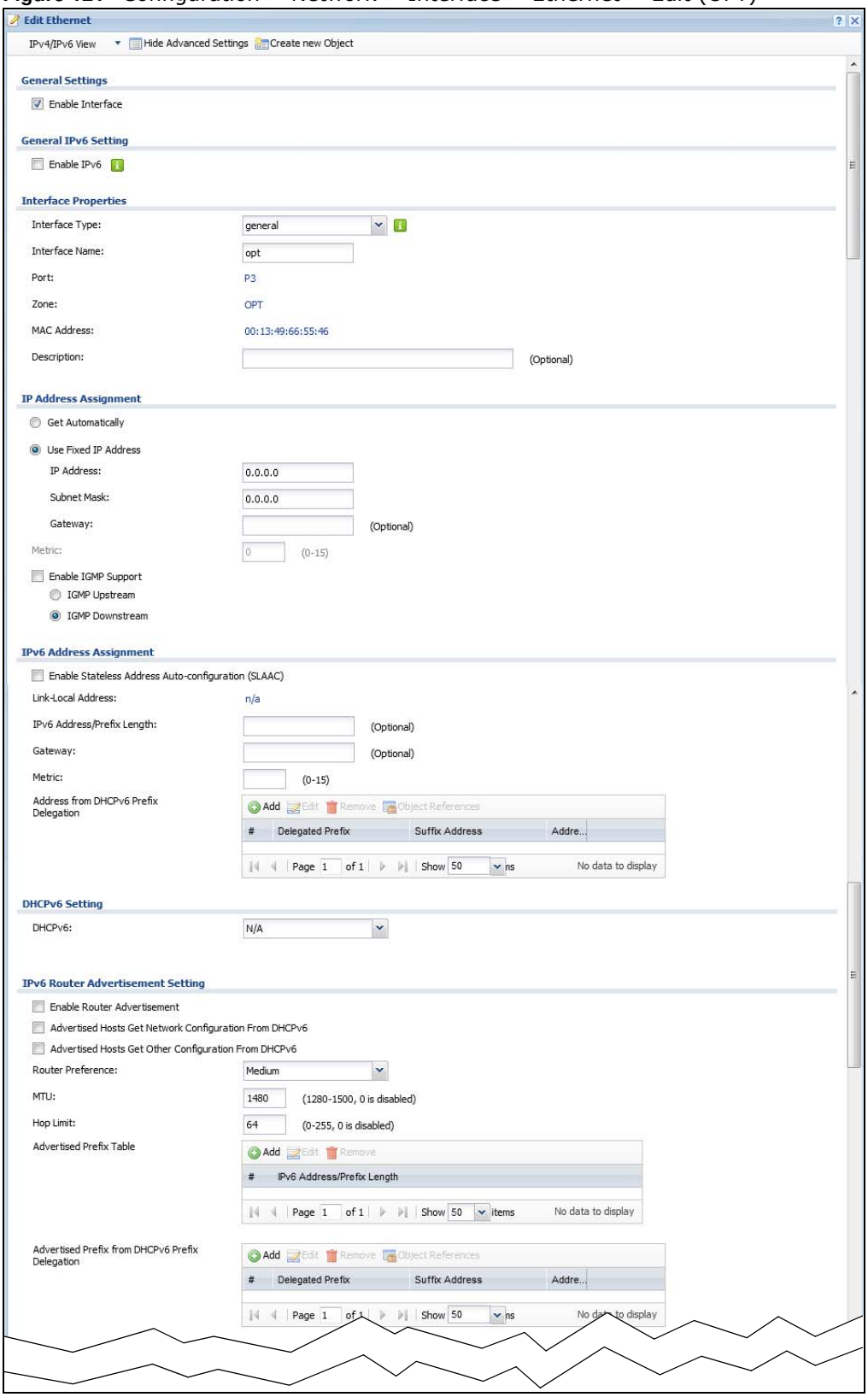
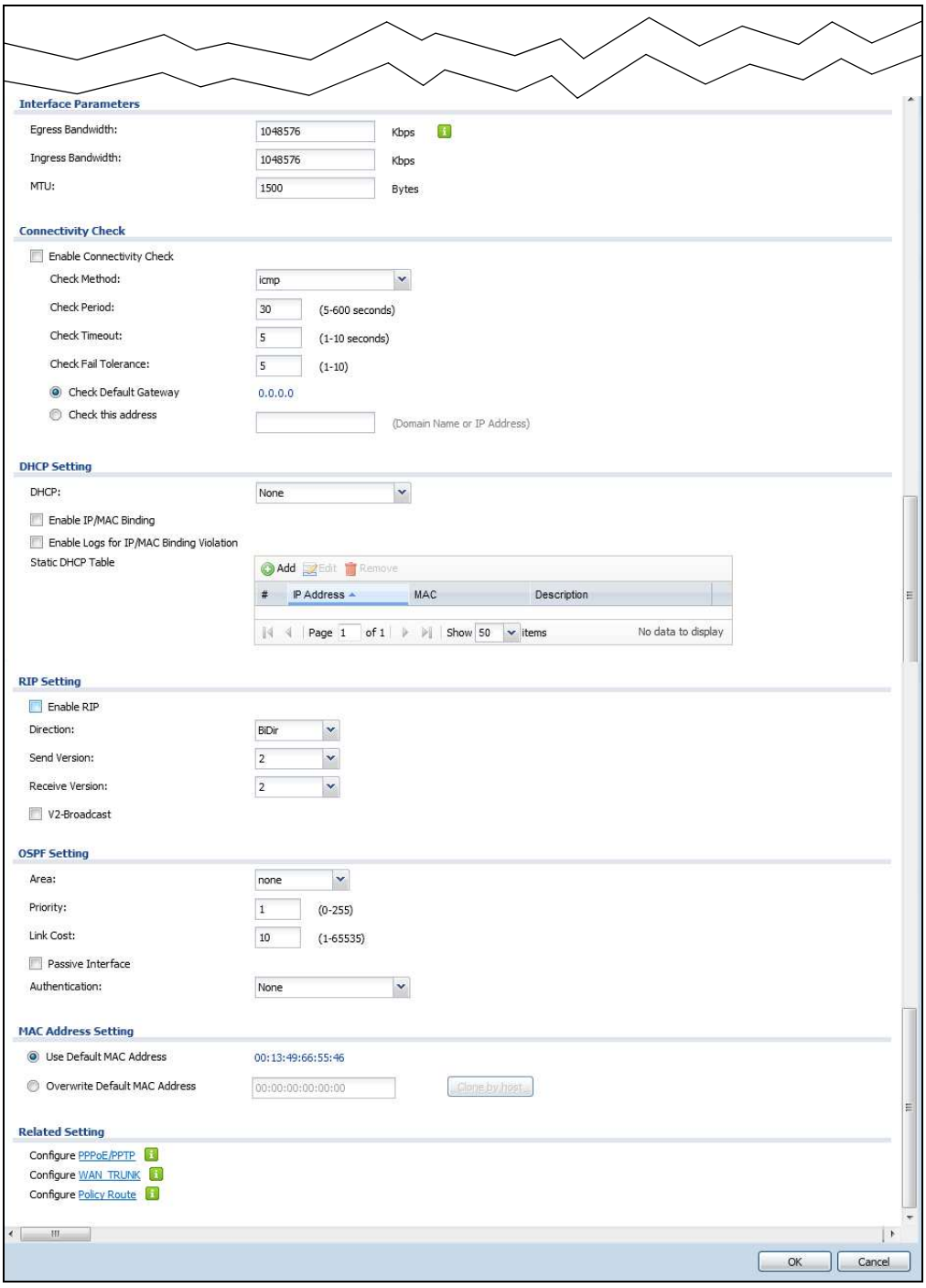

DHCP Setting
DHCP:
DHCP Server
IP Pool Start Address (Optional):
192.168.2.33
Pool Size:
200
First DNS Server (Optional):
ZyWALL
Second DNS Server (Optional):
None
Third DNS Server (Optional):
None
First WINS Server (Optional):
Second WINS Server (Optional):
Default Router (Optional):
lan2 IP
Lease Time:
infinite
2
days
0
hours (Optional)
0
minutes (Optional)
Extended Options
Add
Edit
Remove
Name Code Type Value
Page 1 of 1 Show 50 items
No data to display
Enable IP/MAC Binding
Enable Logs for IP/MAC Binding Violation
Static DHCP Table
Add
Edit
Remove
IP Address MAC Description
Page 1 of 1 Show 50 items
No data to display
RIP Setting
Enable RIP
Direction:
BiDir
Send Version:
2
Receive Version:
2
V2-Broadcast
OSPF Setting
Area:
none
Priority:
1
(0-255)
Link Cost:
10
(1-65535)
Passive Interface
Authentication:
None
OK
Cancel

Figure 121 Configuration > Network > Interface > Ethernet > Edit (OPT)




Interface Parameters
Egress Bandwidth: 1048576 Kbps
Ingress Bandwidth: 1048576 Kbps
MTU: 1500 Bytes
Connectivity Check
Enable Connectivity Check
Check Method: icmp
Check Period: 30 (5-600 seconds)
Check Timeout: 5 (1-10 seconds)
Check Fail Tolerance: 5 (1-10)
Check Default Gateway 0.0.0.0
Check this address (Domain Name or IP Address)
DHCP Setting
DHCP: None
Enable IP/MAC Binding
Enable Logs for IP/MAC Binding Violation
Static DHCP Table
Add Edit Remove
IP Address MAC Description
Page 1 of 1 Show 50 items No data to display
RIP Setting
Enable RIP
Direction: BiDir
Send Version: 2
Receive Version: 2
V2-Broadcast
OSPF Setting
Area: none
Priority: 1 (0-255)
Link Cost: 10 (1-65535)
Passive Interface
Authentication: None
MAC Address Setting
Use Default MAC Address 00:13:49:66:55:46
Overwrite Default MAC Address 00:00:00:00:00:00 Clone by host...
Related Setting
Configure PPPoE/PPTP
Configure WAN_TRUNK
Configure Policy Route
OK
Cancel

This screen's fields are described in the table below.

Table 64 Configuration > Network > Interface > Ethernet > Edit

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	This field is configurable for the OPT interface only. Select to which type of network you will connect this interface. When you select internal or external the rest of the screen's options automatically adjust to correspond. The USG automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic. internal is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The USG automatically adds default SNAT settings for traffic flowing from this interface to an external interface. external is for connecting to an external network (like the Internet). The USG automatically adds this interface to the default WAN trunk. For general, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Port	This is the name of the Ethernet interface's physical port.
Zone	Select the zone to which this interface is to belong. You use zones to apply security settings such as security policy, and remote management.
MAC Address	This field is read-only. This is the MAC address that the Ethernet interface uses.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
IP Address Assignment	These IP address fields configure an IPv4 IP address on the interface itself. If you change this IP address on the interface, you may also need to change a related address object for the network connected to the interface. For example, if you use this screen to change the IP address of your LAN interface, you should also change the corresponding LAN subnet address object.
Get Automatically	This option appears when Interface Type is external or general. Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	This option appears when Interface Type is external or general. Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.

Table 64 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Gateway	This option appears when Interface Type is external or general. Enter the IP address of the gateway. The USG sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	This option appears when Interface Type is external or general. Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
Enable IGMP Support	Select this to allow the USG to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable IGMP Upstream on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable IGMP Downstream on the interface which connects to the multicast hosts.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Link-Local address	This displays the IPv6 link-local address and the network prefix that the USG generates itself for the interface.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the USG obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 145 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.

Table 64 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The USG will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 146 for more information.
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 Client. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If the interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what additional information to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 9.3.3 on page 165 for more information.
Remove	Select an entry and click this to delete it from this table.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the USG obtained from an uplink router (Server is selected) or will advertise to its clients (Client is selected).
Interface	When Relay is selected, select this check box and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When Relay is selected, select this check box and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 146 for more information.

Table 64 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the USG indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the USG indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the USG indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the USG indicate to hosts that DNS information is not available in this network.
Router Preference	Select the router preference (Low, Medium or High) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the USG. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the USG discards the packet and sends an error message to the sender to inform this.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the USG to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	This table is available when the Interface Type is internal. Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The USG will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.

Table 64 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Address	This is the final network prefix combined by the delegated prefix and the suffix. Note: This field displays the combined address after you click **OK** and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the USG can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the USG can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the USG divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	These fields appear when Interface Properties is External or General. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the USG stops routing to the gateway. The USG resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the USG regularly ping the gateway you specify to make sure it is still available. Select tcp to have the USG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the USG stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
DHCP Setting	This section appears when Interface Type is internal or general.
DHCP	Select what type of DHCP service the USG provides to the network. Choices are: None - the USG does not provide any DHCP services. There is already a DHCP server on the network. DHCP Relay - the USG routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. DHCP Server - the USG assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The USG is the DHCP server for the network.
	These fields appear if the USG is a DHCP Relay.

Table 64 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the USG is a DHCP Server.
IP Pool Start Address	Enter the IP address from which the USG begins allocating IP addresses. If you want to assign a static IP address to a specific computer, use the Static DHCP Table. If this field is blank, the Pool Size must also be blank. In this case, the USG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the USG can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the IP Pool Start Address must also be blank. In this case, the USG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server, Second DNS Server, Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. Custom Defined - enter a static IP address. From ISP - select the DNS server that another interface received from its DHCP server. USG - the DHCP clients use the IP address of this interface and the USG works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to DHCP Server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select Custom Defined and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: infinite - select this if IP addresses never expire. days, hours, and minutes - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected DHCP server. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 9.3.4 on page 166.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the name of the DHCP option.
Code	This is the code number of the DHCP option.
Type	This is the type of the set value for the DHCP option.

Table 64 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Value	This is the value set for the DHCP option.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the USG generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the USG assigns to computers connected to the interface. Otherwise, the USG assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
RIP Setting	See Section 10.6 on page 239 for more information about RIP.
Enable RIP	Select this to enable RIP in this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. BiDir - This interface sends and receives routing information. In-Only - This interface receives routing information. Out-Only - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are 1, 2, and 1 and 2.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are 1, 2, and 1 and 2.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the USG uses multicasting.
OSPF Setting	See Section 10.7 on page 241 for more information about OSPF.
Area	Select the area in which this interface belongs. Select None to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.

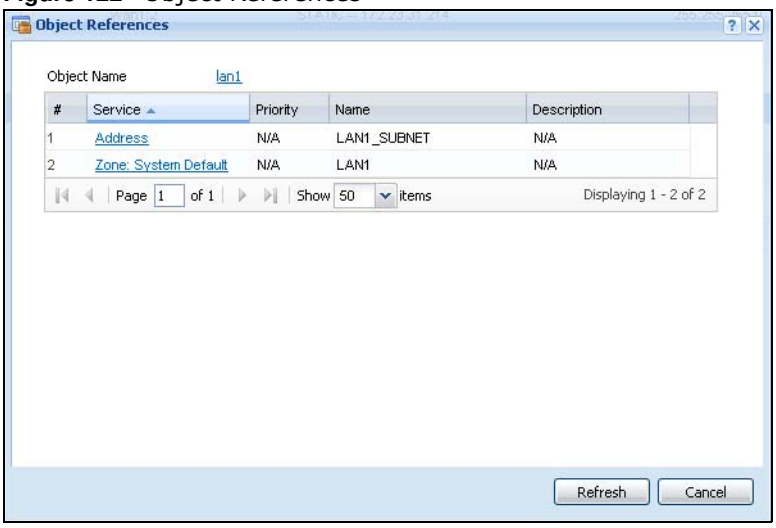
Table 64 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: Same-as-Area - use the default authentication method in the area None - disable authentication Text - authenticate OSPF routing information using a plain-text password MD5 - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the Authentication is Text. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MAC Address Setting	This section appears when Interface Properties is External or General. Have the interface use either the factory assigned default MAC address, a manually specified MAC address, or clone the MAC address of another device or computer.
Use Default MAC Address	Select this option to have the interface use the factory assigned default MAC address. By default, the USG uses the factory assigned MAC address to identify itself.
Overwrite Default MAC Address	Select this option to have the interface use a different MAC address. Either enter the MAC address in the fields or click Clone by host and enter the IP address of the device or computer whose MAC you are cloning. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.
Related Setting	
Configure PPPoE/PPTP	Click PPPoE/ PPTP if this interface's Internet connection uses PPPoE or PPTP.
Configure VLAN	Click VLAN if you want to configure a VLAN interface for this Ethernet interface.
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can set this interface to be part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the policy route summary screen where you can manually associate traffic with this interface. You must manually configure a policy route to add routing and SNAT settings for an interface with the Interface Type set to general. You can also configure a policy route to override the default routing and SNAT behavior for an interface with an Interface Type of internal or external.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

9.3.2 Object References

When a configuration screen includes an Object Reference icon, select a configuration object and click Object Reference to open the Object References screen. This screen displays which configuration settings reference the selected object. The fields shown vary with the type of object.

Figure 122 Object References



The following table describes labels that can appear in this screen.

Table 65 Object References

LABEL	DESCRIPTION
Object Name	This identifies the object for which the configuration settings that use it are displayed. Click the object's name to display the object's configuration screen in the main window.
#	This field is a sequential value, and it is not associated with any entry.
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.
Priority	If it is applicable, this field lists the referencing configuration item's position in its list, otherwise N/ A displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration item has a description configured, it displays here.
Refresh	Click this to update the information in this screen.
Cancel	Click Cancel to close the screen.

9.3.3 Add/Edit DHCPv6 Request/Release Options

When you configure an interface as a DHCPv6 server or client, you can additionally add DHCPv6 request or lease options which have the USG to add more information in the DHCPv6 packets. To open the screen, click Configuration > Network > Interface > Ethernet > Edit, select DHCPv6 Server or DHCPv6 Client in the DHCPv6 Setting section, and then click Add in the DHCPv6 Request Options or DHCPv6 Lease Options table.

Figure 123 Configuration > Network > Interface > Ethernet > Edit > Add DHCPv6 Request/Lease Options

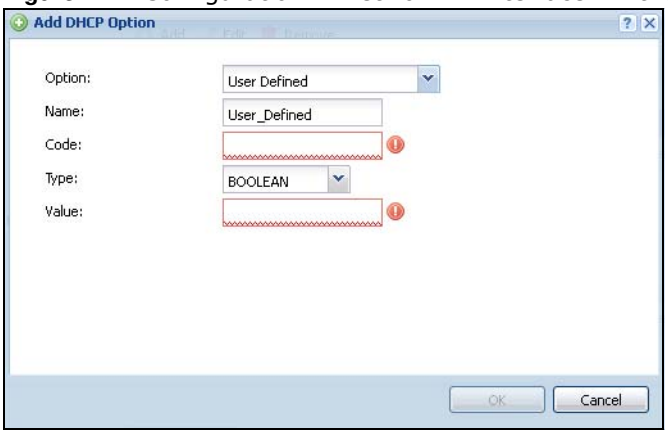


Select a DHCPv6 request or lease object in the Select one object field and click OK to save it. Click Cancel to exit without saving the setting.

9.3.4 Add/Edit DHCP Extended Options

When you configure an interface as a DHCPv4 server, you can additionally add DHCP extended options which have the USG to add more information in the DHCP packets. The available fields vary depending on the DHCP option you select in this screen. To open the screen, click Configuration > Network > Interface > Ethernet > Edit, select DHCP Server in the DHCP Setting section, and then click Add or Edit in the Extended Options table.

Figure 124 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options



The following table describes labels that can appear in this screen.

Table 66 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

LABEL	DESCRIPTION
Option	Select which DHCP option that you want to add in the DHCP packets sent through the interface. See the next table for more information.
Name	This field displays the name of the selected DHCP option. If you selected User Defined in the Option field, enter a descriptive name to identify the DHCP option. You can enter up to 16 characters ("a-z", "A-Z, "0-9", "-", and "_") with no spaces allowed. The first character must be alphabetical (a-z, A-Z).
Code	This field displays the code number of the selected DHCP option. If you selected User Defined in the Option field, enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. If you selected User Defined in the Option field, select an appropriate type for the value that you will enter in the next field. Only advanced users should configure User Defined. Misconfiguration could result in interface lockout.
Value	Enter the value for the selected DHCP option. For example, if you selected TFTP Server Name (66) and the type is TEXT, enter the DNS domain name of a TFTP server here. This field is mandatory.
First IP Address, Second IP Address, Third IP Address	If you selected Time Server (4), NTP Server (41), SIP Server (120), CAPWAP AC (138), or TFTP Server (150), you have to enter at least one IP address of the corresponding servers in these fields. The servers should be listed in order of your preference.
First Enterprise ID, Second Enterprise ID	If you selected VIVC (124) or VIVS (125), you have to enter at least one vendor's 32-bit enterprise number in these fields. An enterprise number is a unique number that identifies a company.
First Class, Second Class	If you selected VIVC (124), enter the details of the hardware configuration of the host on which the client is running, or of industry consortium compliance.

Table 66 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

LABEL	DESCRIPTION
First Information, Second Information	If you selected VIVS (125), enter additional information for the corresponding enterprise number in these fields.
OK	Click this to close this screen and update the settings to the previous Edit screen.
Cancel	Click Cancel to close the screen.

The following table lists the available DHCP extended options (defined in RFCs) on the USG. See RFCs for more information.

Table 67 DHCP Extended Options

OPTION NAME	CODE	DESCRIPTION
Time Offset	2	This option specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Time Server	4	This option specifies a list of Time servers available to the client.
NTP Server	42	This option specifies a list of the NTP servers available to the client by IP address.
TFTP Server Name	66	This option is used to identify a TFTP server when the "sname" field in the DHCP header has been used for DHCP options. The minimum length of the value is 1.
Bootfile	67	This option is used to identify a bootfile when the "file" field in the DHCP header has been used for DHCP options. The minimum length of the value is 1.
SIP Server	120	This option carries either an IPv4 address or a DNS domain name to be used by the SIP client to locate a SIP server.
VIVC	124	Vendor-Identifying Vendor Class option A DHCP client may use this option to unambiguously identify the vendor that manufactured the hardware on which the client is running, the software in use, or an industry consortium to which the vendor belongs.
VIVS	125	Vendor-Identifying Vendor-Specific option DHCP clients and servers may use this option to exchange vendor-specific information.
CAPWAP AC	138	CAPWAP Access Controller addresses option The Control And Provisioning of Wireless Access Points Protocol allows a Wireless Termination Point (WTP) to use DHCP to discover the Access Controllers to which it is to connect. This option carries a list of IPv4 addresses indicating one or more CAPWAP ACs available to the WTP.
TFTP Server	150	The option contains one or more IPv4 addresses that the client may use. The current use of this option is for downloading configuration from a VoIP server via TFTP; however, the option may be used for purposes other than contacting a VoIP configuration server.

9.4 PPP Interfaces

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

Figure 125 Example: PPPoE/PPTP Interfaces



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

- You must also configure an ISP account object for the PPPoE/PPTP interface to use.

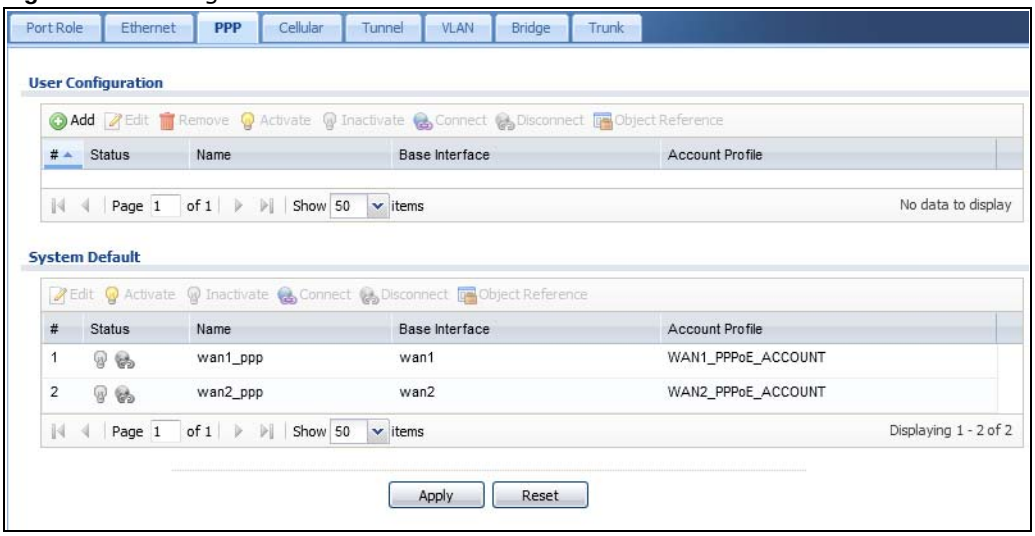
  Each ISP account specifies the protocol (PPPoE or PPTP), as well as your ISP account information. If you change ISPs later, you only have to create a new ISP account, not a new PPPoE/PPTP interface. You should not have to change any network policies.
- You do not set up the subnet mask or gateway.

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

9.4.1 PPP Interface Summary

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

Figure 126 Configuration > Network > Interface > PPP



Each field is described in the table below.

Table 68 Configuration > Network > Interface > PPP

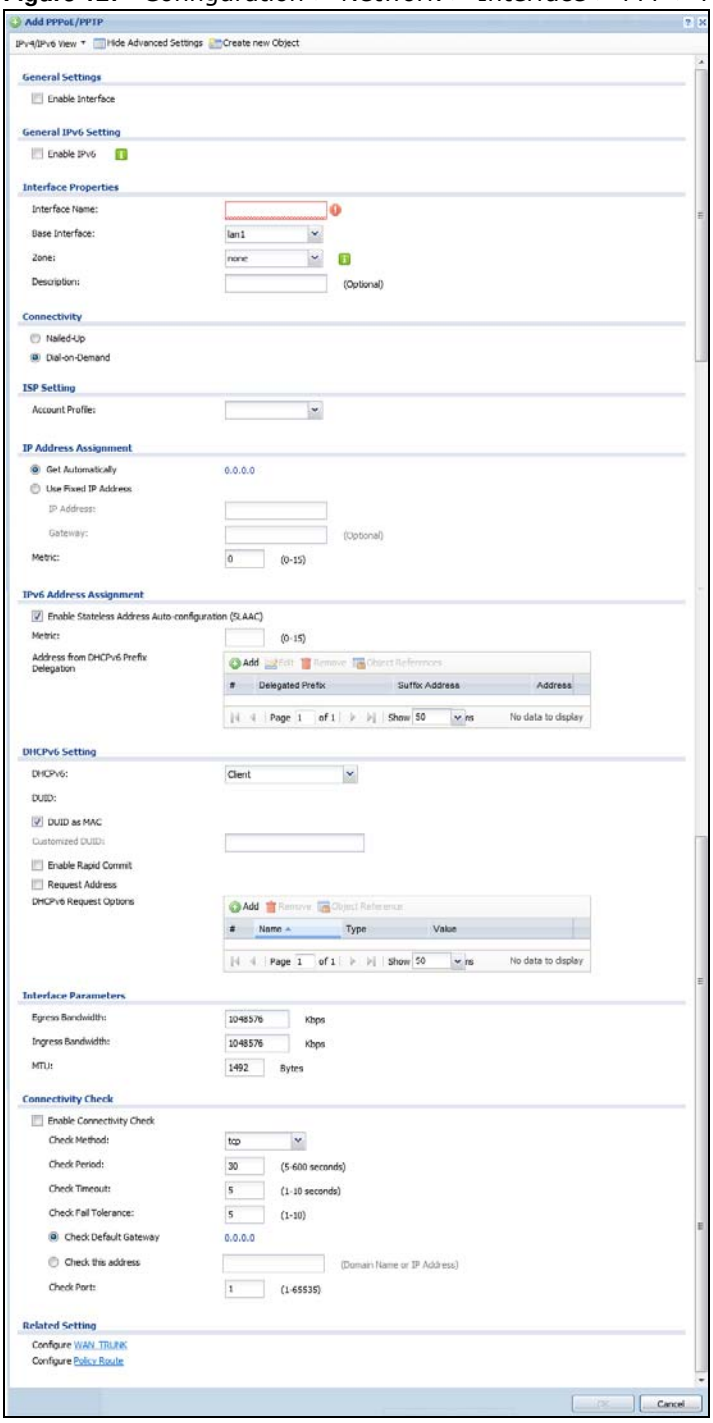
LABEL	DESCRIPTION
User Configuration / System Default	The USG comes with the (non-removable) System Default PPP interfaces pre-configured. You can create (and delete) User Configuration PPP interfaces. System Default PPP interfaces vary by model.
Add	Click this to create a new user-configured PPP interface.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured PPP interface, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Connect	To connect an interface, select it and click Connect. You might use this in testing the interface or to manually establish the connection for a Dial-on-Demand PPPoE/PPTP interface.
Disconnect	To disconnect an interface, select it and click Disconnect. You might use this in testing the interface.
Object References	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Base Interface	This field displays the interface on the top of which the PPPoE/PPTP interface is.
Account Profile	This field displays the ISP account used by this PPPoE/PPTP interface.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

9.4.2 PPP Interface Add or Edit

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

This screen lets you configure a PPPoE or PPTP interface. If you enabled IPv6 in the Configuration > System > IPv6 screen, you can also configure PPP interfaces used for your IPv6 networks on this screen. To access this screen, click the Add icon or an Edit icon in the PPP Interface screen.

Figure 127 Configuration > Network > Interface > PPP > Add



Each field is explained in the following table.

Table 69 Configuration > Network > Interface > PPP > Add

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create an ISP Account or a DHCPv6 request object that you may use for the ISP or DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Base Interface	Select the interface upon which this PPP interface is built. Note: Multiple PPP interfaces can use the same base interface.
Zone	Select the zone to which this PPP interface belongs. The zone determines the security settings the USG uses for the interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Connectivity	
Nailed-Up	Select this if the PPPoE/PPTP connection should always be up. Clear this to have the USG establish the PPPoE/PPTP connection only when there is traffic. You might use this option if a lot of traffic needs to go through the interface or it does not cost extra to keep the connection up all the time.
Dial-on-Demand	Select this to have the USG establish the PPPoE/PPTP connection only when there is traffic. You might use this option if there is little traffic through the interface or if it costs money to keep the connection available.
ISP Setting	
Account Profile	Select the ISP account that this PPPoE/PPTP interface uses. The drop-down box lists ISP accounts by name. Use `Create new Object` if you need to configure a new ISP account (see Chapter 29 on page 529 for details).
Protocol	This field is read-only. It displays the protocol specified in the ISP account.
User Name	This field is read-only. It displays the user name for the ISP account.
Service Name	This field is read-only. It displays the PPPoE service name specified in the ISP account. This field is blank if the ISP account uses PPTP.
IP Address Assignment	Click `Show Advanced Settings` to display more settings. Click `Hide Advanced Settings` to display fewer settings.
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address automatically. The subnet mask and gateway are always defined automatically in PPPoE/PPTP interfaces.
Use Fixed IP Address	Select this if you want to specify the IP address manually.

Table 69 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
IP Address	This field is enabled if you select Use Fixed IP Address. Enter the IP address for this interface.
Metric	Enter the priority of the gateway (the ISP) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Metric	Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the USG obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 145 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The USG will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DHCPv6	Select Client to obtain an IP address and DNS information from the service provider for the interface. Otherwise, select N/A to diable the function.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 146 for more information.
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.

Table 69 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Request Address	Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options	Use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server.
Add	Click this to create an entry in this table. See Section 9.3.4 on page 166 for more information.
Remove	Select an entry and click this to delete it from this table.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the USG will advertise to its clients.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the USG can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the USG can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the USG divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the USG stops routing to the gateway. The USG resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the USG regularly ping the gateway you specify to make sure it is still available. Select tcp to have the USG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the USG stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.

Table 69 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
Check Port	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Policy Route	Click Policy Route to go to the screen where you can manually configure a policy route to associate traffic with this interface.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

9.5 Cellular Configuration Screen

Mobile broadband is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

Note: The actual data rate you obtain varies depending on the mobile broadband device you use, the signal strength to the service provider's base station, and so on.

You can configure how the USG's mobile broadband device connects to a network (refer to Section 9.5.1 on page 177):

- You can set the mobile broadband device to connect only to the home network, which is the network to which you are originally subscribed.
- You can set the mobile broadband device to connect to other networks if the signal strength of the home network is too low or it is unavailable.

3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

4G

4G is the fourth generation of the mobile telecommunications technology and a successor of 3G. Both the WiMAX and Long Term Evolution (LTE) standards are the 4G candidate systems. 4G only supports all-IP-based packet-switched telephony services and is required to offer gigabit speed access.

Note: Note: The actual data rate you obtain varies depending on your mobile environment. The environmental factors may include the number of mobile devices which are currently connected to the mobile network, the signal strength to the mobile network, and so on.

See the following table for a comparison between 2G, 2.5G, 2.75G, 3G and 4G wireless technologies.

Table 70 2G, 2.5G, 2.75G, 3G, 3.5G and 4G Wireless Technologies

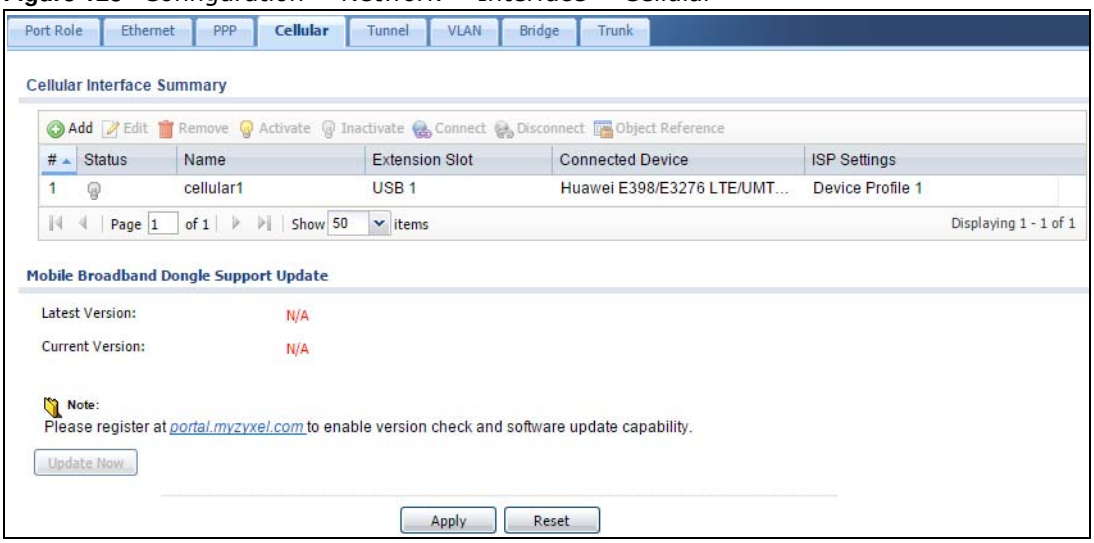
NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	CDMA-BASED	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	Slow
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio. CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.		
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface. The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		
4G/LTE	Packet-switched	The LTE (Long Term Evolution) standard is based on the GSM and UMTS network technologies.		Fast

To change your mobile broadband WAN settings, click Configuration > Network > Interface > Cellular.

Note: Install (or connect) a compatible mobile broadband USB device to use a cellular connection.

Note: The WAN IP addresses of a USG with multiple WAN interfaces must be on different subnets.

Figure 128 Configuration > Network > Interface > Cellular



The following table describes the labels in this screen.

Table 71 Configuration > Network > Interface > Cellular

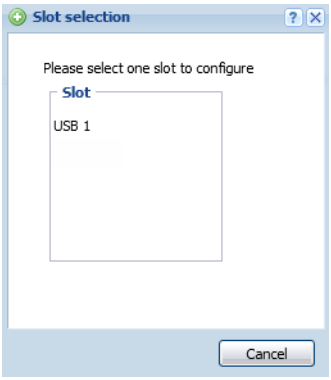
LABEL	DESCRIPTION
Add	Click this to create a new cellular interface.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Connect	To connect an interface, select it and click Connect. You might use this in testing the interface or to manually establish the connection.
Disconnect	To disconnect an interface, select it and click Disconnect. You might use this in testing the interface.
Object References	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Extension Slot	This field displays where the entry's cellular card is located.
Connected Device	This field displays the name of the cellular card.
ISP Settings	This field displays the profile of ISP settings that this cellular interface is set to use.
Mobile Broadband Dongle Support	You should have registered your USG at myzyxel.com. Myzyxel.com hosts a list of supported mobile broadband dongle devices. You should have an Internet connection to access this website.
Latest Version	This displays the latest supported mobile broadband dongle list version number.

Table 71 Configuration > Network > Interface > Cellular (continued)

LABEL	DESCRIPTION
Current Version	This displays the currently supported (by the USG) mobile broadband dongle list version number.
Update Now	If the latest version number is greater than the current version number, then click this button to download the latest list of supported mobile broadband dongle devices to the USG.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

9.5.1 Cellular Choose Slot

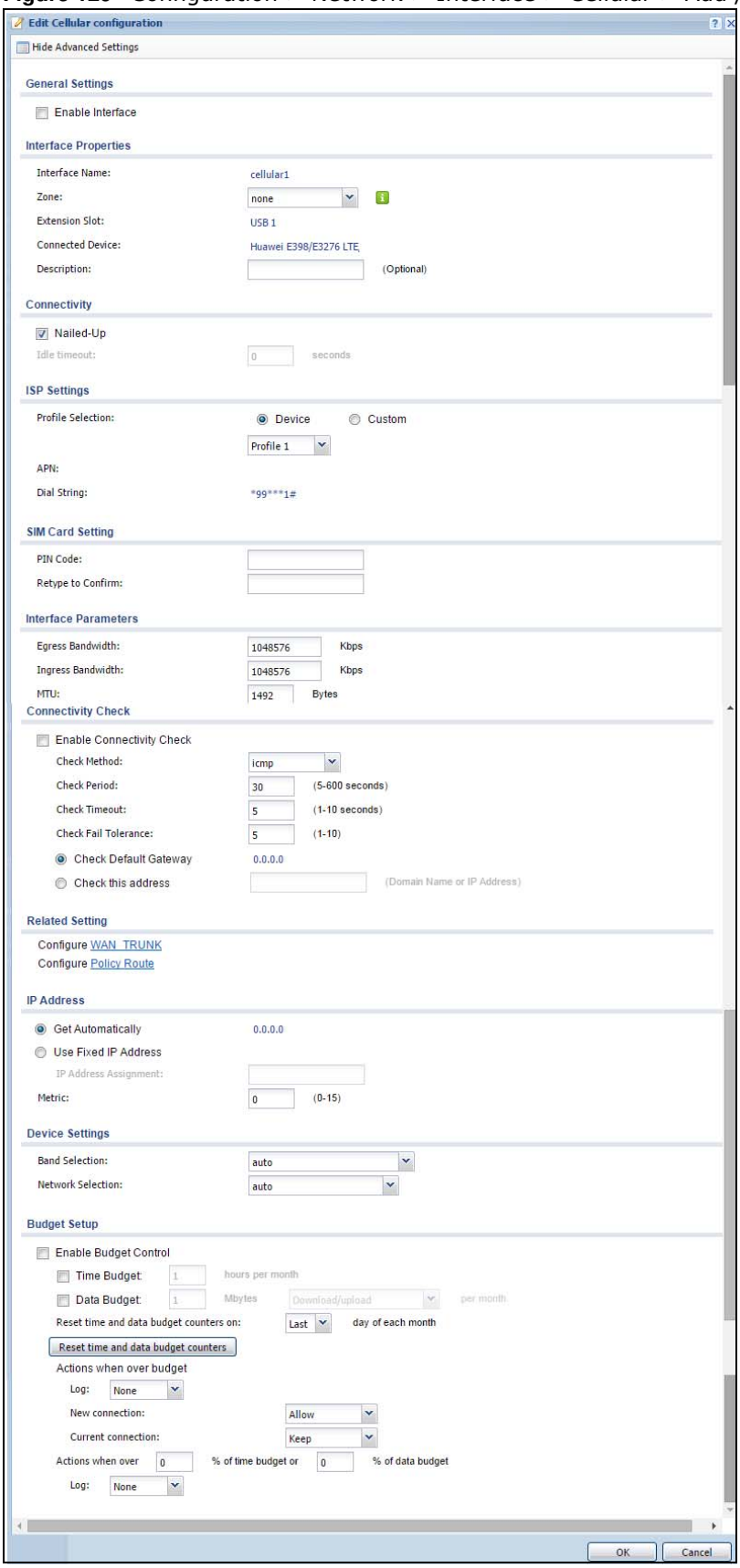
To change your mobile broadband settings, click Configuration > Network > Interface > Cellular > Add (or Edit). In the pop-up window that displays, select the slot that contains the mobile broadband device, then the Add Cellular configuration screen displays.



9.5.2 Add / Edit Cellular Configuration

This screen displays after you select the slot that contains the mobile broadband device in the previous pop-up window.

Figure 129 Configuration > Network > Interface > Cellular > Add / Edit



The following table describes the labels in this screen.

Table 72 Configuration > Network > Interface > Cellular > Add / Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this option to turn on this interface.
Interface Properties	
Interface Name	Select a name for the interface.
Zone	Select the zone to which you want the cellular interface to belong. The zone determines the security settings the USG uses for the interface.
Extension Slot	This is the USB slot that you are configuring for use with a mobile broadband card.
Connected Device	This displays the manufacturer and model name of your mobile broadband card if you inserted one in the USG. Otherwise, it displays none.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Connectivity	
Nailed-Up	Select this if the connection should always be up. Clear this to have the USG to establish the connection only when there is traffic. You might not nail up the connection if there is little traffic through the interface or if it costs money to keep the connection available.
Idle timeout	This value specifies the time in seconds (0~360) that elapses before the USG automatically disconnects from the ISP's server. Zero disables the idle timeout.
ISP Settings	
Profile Selection	Select Device to use one of the mobile broadband device's profiles of device settings. Then select the profile (use Profile 1 unless your ISP instructed you to do otherwise). Select Custom to configure your device settings yourself.
APN	This field is read-only if you selected Device in the profile selection. Select Custom in the profile selection to be able to manually input the APN (Access Point Name) provided by your service provider. This field applies with a GSM or HSDPA mobile broadband card. Enter the APN from your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 63 ASCII printable characters. Spaces are allowed.
Dial String	Enter the dial string if your ISP provides a string, which would include the APN, to initialize the mobile broadband card. You can enter up to 63 ASCII printable characters. Spaces are allowed. This field is available only when you insert a GSM mobile broadband card.
Authentication Type	The USG supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: None: No authentication for outgoing calls. CHAP - Your USG accepts CHAP requests only. PAP - Your USG accepts PAP requests only.

Table 72 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
User Name	This field displays when you select an authentication type other than None. This field is read-only if you selected Device in the profile selection. If this field is configurable, enter the user name for this mobile broadband card exactly as the service provider gave it to you. You can use 1 ~ 64 alphanumeric and #:%-_@$./ characters. The first character must be alphanumeric or -_@$./. Spaces are not allowed.
Password	This field displays when you select an authentication type other than None. This field is read-only if you selected Device in the profile selection and the password is included in the mobile broadband card's profile. If this field is configurable, enter the password for this SIM card exactly as the service provider gave it to you. You can use 0 ~ 63 alphanumeric and `~!@#$%^&*()_-+={}|;:'<,>./ characters. Spaces are not allowed.
Retype to Confirm	This field displays when you select an authentication type other than None. This field is read-only if you selected Device in the profile selection and the password is included in the mobile broadband card's profile. If this field is configurable, re-enter the password for this SIM card exactly as the service provider gave it to you.
SIM Card Setting	
PIN Code	This field displays with a GSM or HSDPA mobile broadband card. A PIN (Personal Identification Number) code is a key to a mobile broadband card. Without the PIN code, you cannot use the mobile broadband card. Enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the mobile broadband card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, enter an arbitrary number.
Retype to Confirm	Type the PIN code again to confirm it.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the USG can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the USG can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the USG divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the USG stops routing to the gateway. The USG resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the USG regularly ping the gateway you specify to make sure it is still available. Select tcp to have the USG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.

Table 72 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the USG stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the policy route summary screen where you can configure a policy route to override the default routing and SNAT behavior for the interface.
IP Address Assignment	
Get Automatically	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 Assignment	Enter the cellular interface's WAN IP address in this field if you selected Use Fixed IP Address.
Metric	Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
Device Settings	
Band Selection	This field appears if you selected a mobile broadband device that allows you to select the type of network to use. Select the type of mobile broadband service for your mobile broadband connection. If you are unsure what to select, check with your mobile broadband service provider to find the mobile broadband service available to you in your region. Select auto to have the card connect to an available network. Choose this option if you do not know what networks are available. You may want to manually specify the type of network to use if you are charged differently for different types of network or you only have one type of network available to you. Select GPRS / EDGE (GSM) only to have this interface only use a 2.5G or 2.75G network (respectively). If you only have a GSM network available to you, you may want to select this so the USG does not spend time looking for a WCDMA network. Select UMTS / HSDPA (WCDMA) only to have this interface only use a 3G or 3.5G network (respectively). You may want to do this if you want to make sure the interface does not use the GSM network. Select LTE only to have this interface only use a 4G LTE network. This option only appears when a USB dongle for 4G technology is inserted.

Table 72 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
Network Selection	Home network is the network to which you are originally subscribed. Select Home to have the mobile broadband device connect only to the home network. If the home network is down, the USG's mobile broadband Internet connection is also unavailable. Select Auto (Default) to allow the mobile broadband device to connect to a network to which you are not subscribed when necessary, for example when the home network is down or another mobile broadband base station's signal is stronger. This is recommended if you need continuous Internet connectivity. If you select this, you may be charged using the rate of a different network.
Budget Setup	
Enable Budget Control	Select this to set a monthly limit for the user account of the installed mobile broadband card. You can set a limit on the total traffic and/or call time. The USG takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this and specify the amount of time (in hours) that the mobile broadband connection can be used within one month. If you change the value after you configure and enable budget control, the USG resets the statistics.
Data Budget	Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted via the mobile broadband connection within one month. Select Download to set a limit on the downstream traffic (from the ISP to the USG). Select Upload to set a limit on the upstream traffic (from the USG to the ISP). Select Download/ Upload to set a limit on the total traffic in both directions. If you change the value after you configure and enable budget control, the USG resets the statistics.
Reset time and data budget counters on	Select the date on which the USG resets the budget every month. If the date you selected is not available in a month, such as 30th or 31st, the USG resets the budget on the last day of the month.
Reset time and data budget counters	This button is available only when you enable budget control in this screen. Click this button to reset the time and data budgets immediately. The count starts over with the mobile broadband connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second.
Actions when over budget	Specify the actions the USG takes when the time or data limit is exceeded.
Log	Select None to not create a log, Log to create a log, or Log-alert to create an alert log. If you select Log or Log-alert you can also select recurring every to have the USG send a log or alert for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log or alert.
New connection	Select Allow to permit new mobile broadband connections or Disallow to drop/block new mobile broadband connections.
Current connection	Select Keep to maintain an existing mobile broadband connection or Drop to disconnect it. You cannot set New connection to Allow and Current connection to Drop at the same time. If you set New connection to Disallow and Current connection to Keep, the USG allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.

Table 72 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
Actions when over % of time budget or % of data budget	Specify the actions the USG takes when the specified percentage of time budget or data limit is exceeded. Enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the USG resets the statistics.
Log	Select None to not create a log when the USG takes this action, Log to create a log, or Log-alert to create an alert log. If you select Log or Log-alert you can also select recurring every to have the USG send a log or alert for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log or alert.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

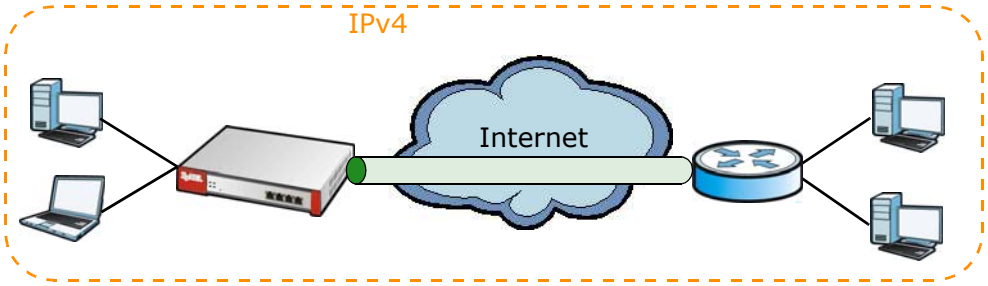
9.6 Tunnel Interfaces

The USG uses tunnel interfaces in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels.

GRE Tunneling

GRE tunnels encapsulate a wide variety of network layer protocol packet types inside IP tunnels. A GRE tunnel serves as a virtual point-to-point link between the USG and another router over an IPv4 network. At the time of writing, the USG only supports GRE tunneling in IPv4 networks.

Figure 130 GRE Tunnel Example



IPv6 Over IPv4 Tunnels

To route traffic between two IPv6 networks over an IPv4 network, an IPv6 over IPv4 tunnel has to be used.

Figure 131 IPv6 over IPv4 Network



On the USG, you can either set up a manual IPv6-in-IPv4 tunnel or an automatic 6to4 tunnel. The following describes each method:

IPv6-in-IPv4 Tunneling

Use this mode on the WAN of the USG if

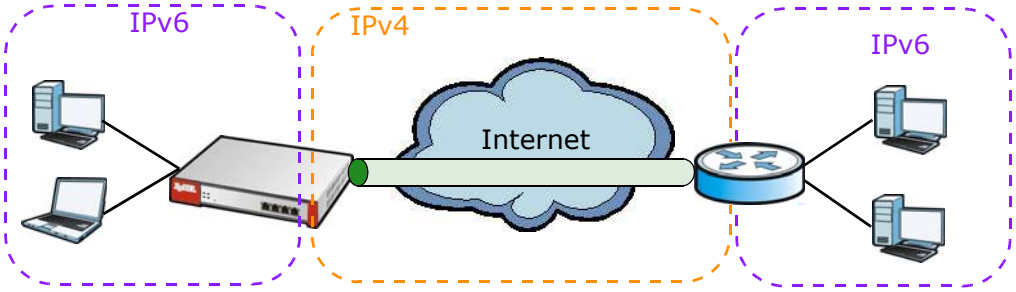
- your USG has a public IPv4 IP address given from your ISP,

and

- you want to transmit your IPv6 packets to one and only one remote site whose LAN network is also an IPv6 network.

With this mode, the USG encapsulates IPv6 packets within IPv4 packets across the Internet. You must know the WAN IP address of the remote gateway device. This mode is normally used for a site-to-site application such as two branch offices.

Figure 132 IPv6-in-IPv4 Tunnel



In the USG, you must also manually configure a policy route for an IPv6-in-IPv4 tunnel to make the tunnel work.

6to4 Tunneling

This mode also enables IPv6 packets to cross IPv4 networks. Unlike IPv6-in-IPv4 tunneling, you do not need to configure a policy route for a 6to4 tunnel. Through your properly pre-configuring the destination router's IP address in the IP address assignments to hosts, the USG can automatically forward 6to4 packets to the destination they want to go. A 6to4 relay router is required to route 6to4 packets to a native IPv6 network if the packet's destination do not match your specified criteria.

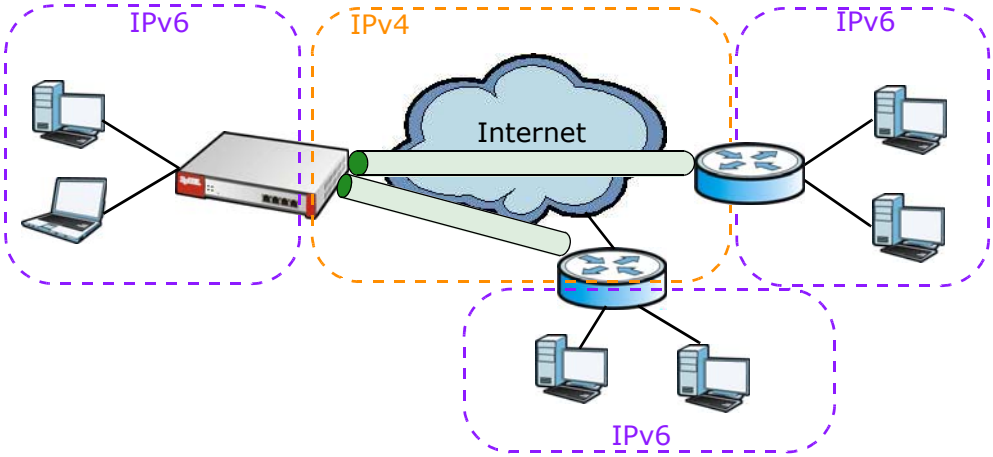
In this mode, the USG should get a public IPv4 address for the WAN. The USG adds an IPv4 IP header to an IPv6 packet when transmitting the packet to the Internet. In reverse, the USG removes the IPv4 header from an IPv6 packet when receiving it from the Internet.

An IPv6 address using the 6to4 mode consists of an IPv4 address, the format is as the following:

2002:[a public IPv4 address in hexadecimal]::/48

For example, a public IPv4 address is 202.156.30.41. The converted hexadecimal IP string is ca.9c.1Ee.29. The IPv6 address prefix becomes 2002:ca9c:1e29::/48.

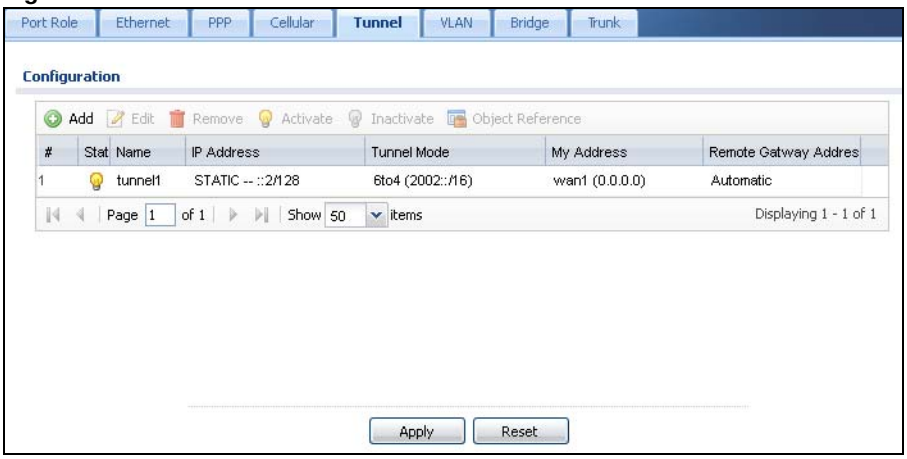
Figure 133 6to4 Tunnel



9.6.1 Configuring a Tunnel

This screen lists the USG's configured tunnel interfaces. To access this screen, click Network > Interface > Tunnel.

Figure 134 Network > Interface > Tunnel



Each field is explained in the following table.

Table 73 Network > Interface > Tunnel

LABEL	DESCRIPTION
Add	Click this to create a new GRE tunnel interface.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Object References	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with any interface.

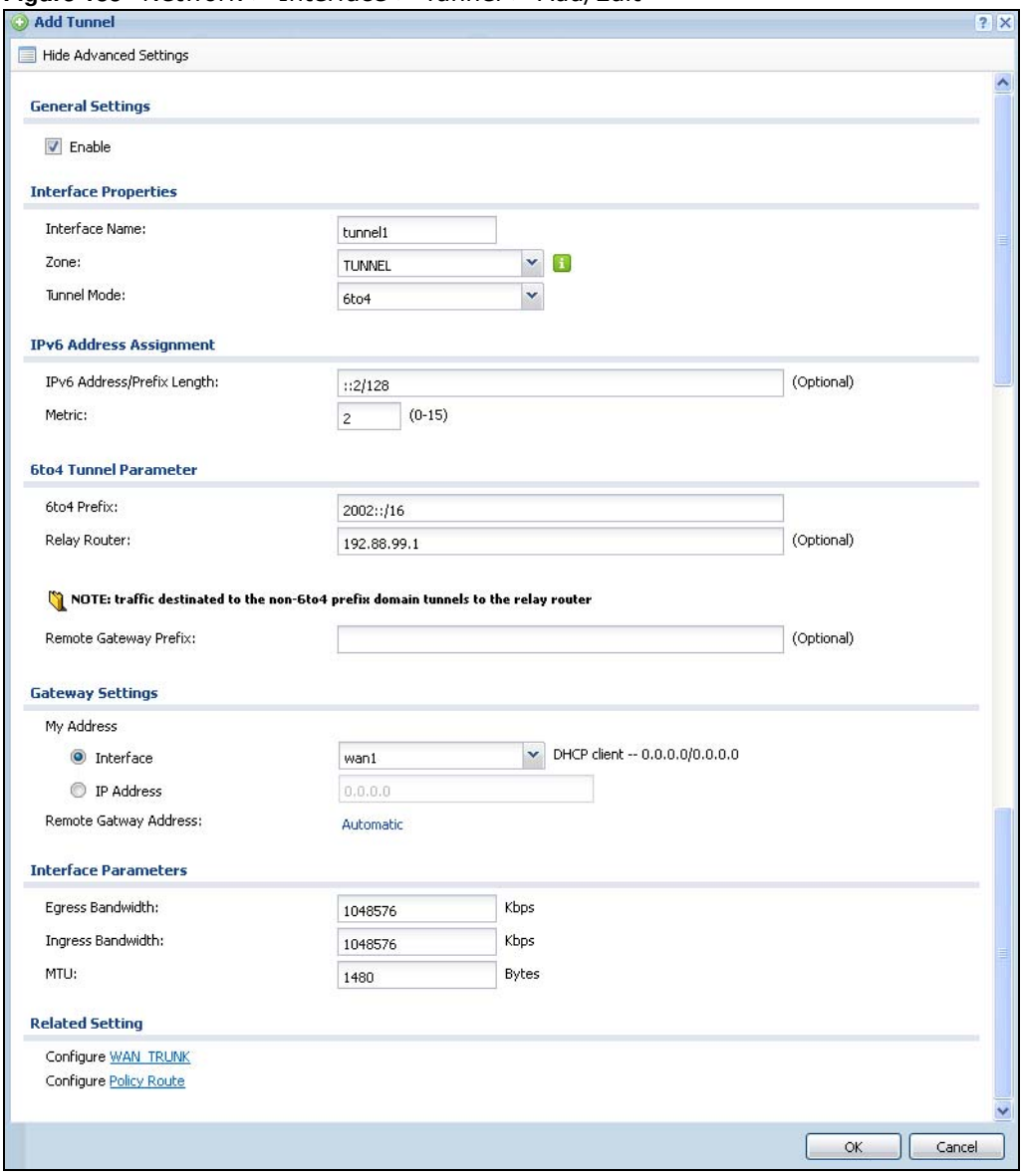
Table 73 Network > Interface > Tunnel (continued)

LABEL	DESCRIPTION
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
IP Address	This is the IP address of the interface. If the interface is active (and connected), the USG tunnels local traffic sent to this IP address to the Remote Gateway Address.
Tunnel Mode	This is the tunnel mode of the interface (GRE, IPv6-in-IPv4 or 6to4). This field also displays the interface's IPv4 IP address and subnet mask if it is a GRE tunnel. Otherwise, it displays the interface's IPv6 IP address and prefix length.
My Address	This is the interface or IP address uses to identify itself to the remote gateway. The USG uses this as the source for the packets it tunnels to the remote gateway.
Remote Gateway Address	This is the IP address or domain name of the remote gateway to which this interface tunnels traffic.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to begin configuring this screen afresh.

9.6.2 Tunnel Add or Edit Screen

This screen lets you configure a tunnel interface. Click Configuration > Network > Interface > Tunnel > Add (or Edit) to open the following screen.

Figure 135 Network > Interface > Tunnel > Add/Edit



Each field is explained in the following table.

Table 74 Network > Interface > Tunnel > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Interface Name	This field is read-only if you are editing an existing tunnel interface. Enter the name of the tunnel interface. The format is tunnel*x*, where *x* is 0 - 3. For example, tunnel0.
Zone	Use this field to select the zone to which this interface belongs. This controls what security settings the USG applies to this interface.

Table 74 Network > Interface > Tunnel > Add/Edit (continued)

LABEL	DESCRIPTION
Tunnel Mode	Select the tunneling protocol of the interface (GRE, IPv6-in-IPv4 or 6to4). See Section 9.6 on page 183 for more information.
IP Address Assignment	This section is available if you are configuring a GRE tunnel.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Metric	Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
IPv6 Address Assignment	This section is available if you are configuring an IPv6-in-IPv4 or a 6to4 tunnel.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Metric	Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
6to4 Tunnel Parameter	This section is available if you are configuring a 6to4 tunnel which encapsulates IPv6 to IPv4 packets.
6to4 Prefix	Enter the IPv6 prefix of a destination network. The USG forwards IPv6 packets to the hosts in the matched network. If you enter a prefix starting with 2002, the USG will forward the matched packets to the IPv4 IP address converted from the packets' destination address. The IPv4 IP address can be converted from the next 32 bits after the prefix you specified in this field. See 6to4 Tunneling on page 184 for an example. The USG forwards the unmatched packets to the specified Relay Router.
Relay Router	Enter the IPv4 address of a 6to4 relay router which helps forward packets between 6to4 networks and native IPv6 networks.
Remote Gateway Prefix	Enter the IPv4 network address and network bits of a remote 6to4 gateway, for example, 14.15.0.0/16. This field works if you enter a 6to4 Prefix not starting with 2002 (2003 for example). The USG forwards the matched packets to a remote gateway with the network address you specify here, and the bits converted after the 6to4 Prefix in the packets. For example, you configure the 6to4 prefix to 2003:A0B::/32 and the remote gateway prefix to 14.15.0.0/16. If a packet's destination is 2003:A0B:1011:5::8, the USG forwards the packet to 14.15.16.17, where the network address is 14.15.0.0 and the host address is the remain bits converted from 1011 after the packet's 6to4 prefix (2003:A0B).
Gateway Settings	
My Address	Specify the interface or IP address to use as the source address for the packets this interface tunnels to the remote gateway. The remote gateway sends traffic to this interface or IP address.
Remote Gateway Address	Enter the IP address or domain name of the remote gateway to which this interface tunnels traffic. Automatic displays in this field if you are configuring a 6to4 tunnel. It means the 6to4 tunnel will help forward packets to the corresponding remote gateway automatically by looking at the packet's destination address.

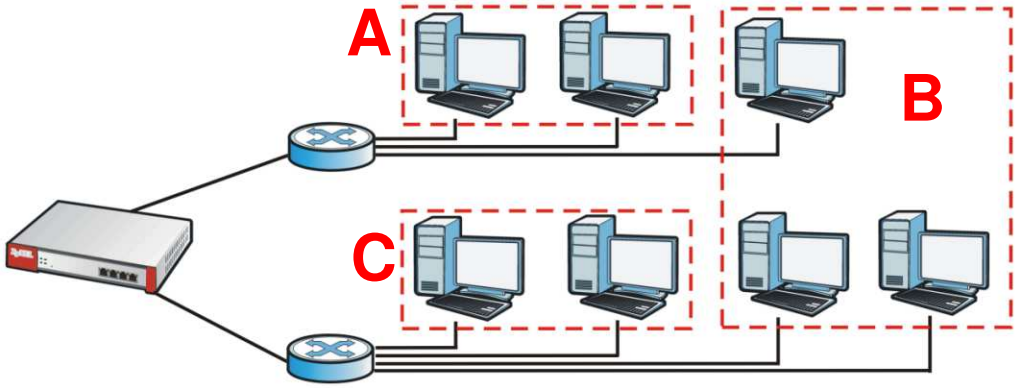
Table 74 Network > Interface > Tunnel > Add/Edit (continued)

LABEL	DESCRIPTION
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the USG can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the USG can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the USG divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	This section is available if you are configuring a GRE tunnel. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the USG stops routing to the gateway. The USG resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the USG regularly ping the gateway you specify to make sure it is still available. Select tcp to have the USG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the USG stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Related Setting	
WAN TRUNK	Click this link to go to a screen where you can configure WAN trunk load balancing.
Policy Route	Click this link to go to the screen where you can manually configure a policy route to associate traffic with this interface.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

9.7 VLAN Interfaces

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

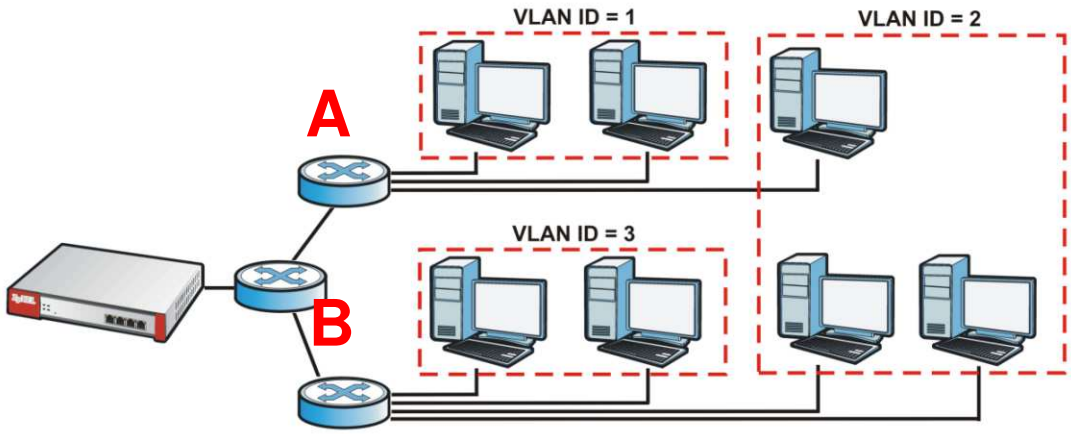
Figure 136 Example: Before VLAN



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

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

Figure 137 Example: After VLAN



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

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

This approach provides a few advantages.

- Increased performance - In VLAN 2, the extra switch should route traffic inside the sales department faster than the router does. In addition, broadcasts are limited to smaller, more logical groups of users.

- Higher security - If each computer has a separate physical connection to the switch, then broadcast traffic in each VLAN is never sent to computers in another VLAN.
- Better manageability - You can align network policies more appropriately for users. For example, you can create different content filtering rules for each VLAN (each department in the example above), and you can set different bandwidth limits for each VLAN. These rules are also independent of the physical network, so you can change the physical network without changing policies.

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

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

VLAN Interfaces Overview

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

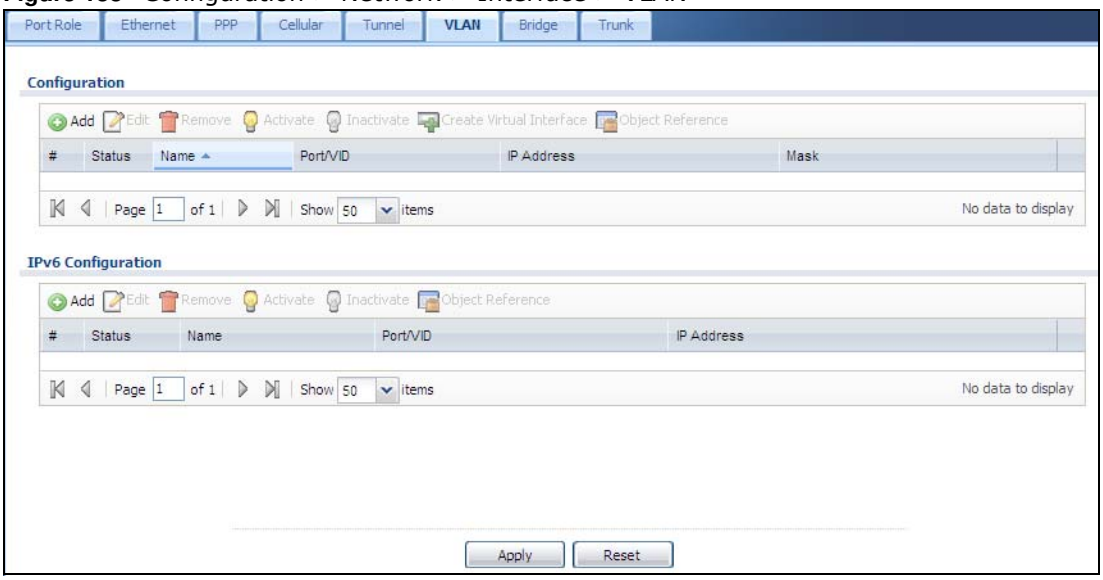
Note: Each VLAN interface is created on top of only one Ethernet interface.

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

9.7.1 VLAN Summary Screen

This screen lists every VLAN interface and virtual interface created on top of VLAN interfaces. If you enabled IPv6 in the Configuration > System > IPv6 screen, you can also configure VLAN interfaces used for your IPv6 networks on this screen. To access this screen, click Configuration > Network > Interface > VLAN.

Figure 138 Configuration > Network > Interface > VLAN



Each field is explained in the following table.

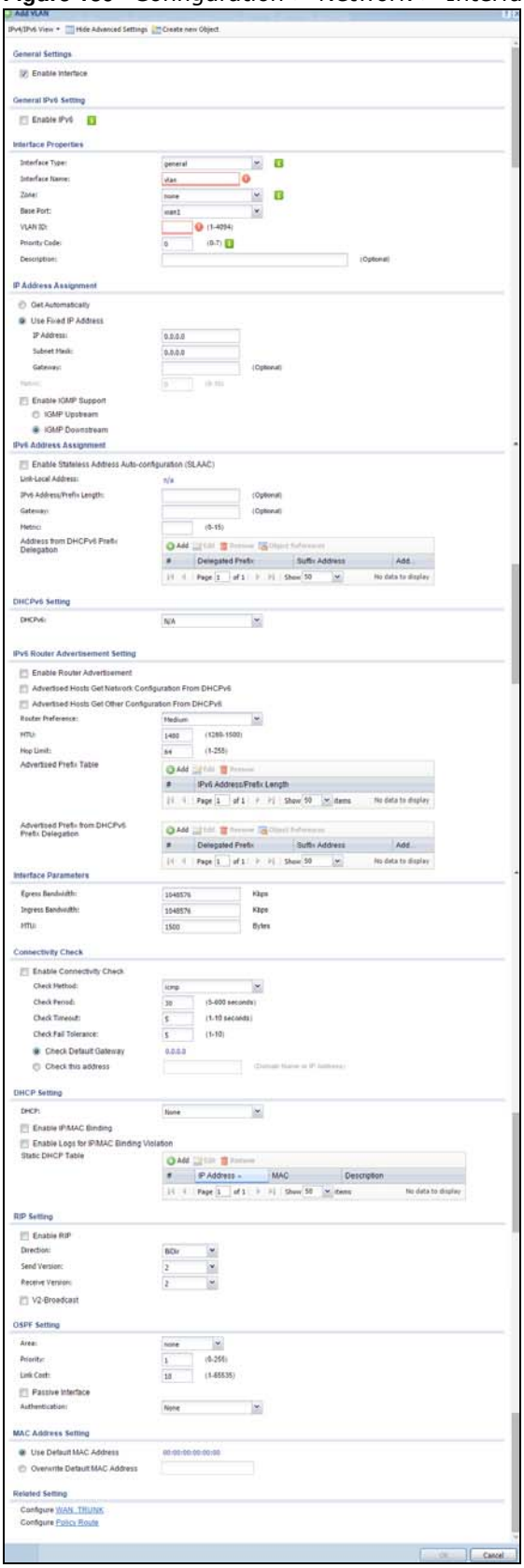
Table 75 Configuration > Network > Interface > VLAN

LABEL	DESCRIPTION
Configuration / IPv6 Configuration	Use the Configuration section for IPv4 network settings. Use the IPv6 Configuration section for IPv6 network settings if you connect your USG to an IPv6 network. Both sections have similar fields as described below.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Create Virtual Interface	To open the screen where you can create a virtual interface, select an interface and click Create Virtual Interface.
Object References	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
Port/VID	For VLAN interfaces, this field displays • the Ethernet interface on which the VLAN interface is created • the VLAN ID For virtual interfaces, this field is blank.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (STATIC) or dynamically assigned (DHCP). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

9.7.2 VLAN Add/Edit

Select an existing entry in the previous scrren and click Edit or click Add to create a new entry. The following screen appears.

Figure 139 Configuration > Network > Interface > VLAN > Add /Edit



Each field is explained in the following table.

Table 76 Configuration > Network > Interface > VLAN > Add / Edit

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to turn this interface on. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	Select one of the following option depending on the type of network to which the USG is connected or if you want to additionally manually configure some related settings. internal is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The USG automatically adds default SNAT settings for traffic flowing from this interface to an external interface. external is for connecting to an external network (like the Internet). The USG automatically adds this interface to the default WAN trunk. For general, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	This field is read-only if you are editing an existing VLAN interface. Enter the number of the VLAN interface. You can use a number from 0~4094. For example, use vlan0, vlan8, and so on. The total number of VLANs you can configure on the USG depends on the model.
Zone	Select the zone to which the VLAN interface belongs.
Base Port	Select the Ethernet interface on which the VLAN interface runs.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)
Priority Code	This is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest. See Table 158 on page 408. The setting configured in Configuration > BWM overwrites the priority setting here.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically. You should not select this if the interface is assigned to a VRRP group.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select Use Fixed IP Address. Enter the IP address for this interface.

Table 76 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Subnet Mask	This field is enabled if you select Use Fixed IP Address. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select Use Fixed IP Address. Enter the IP address of the gateway. The USG sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
Enable IGMP Support	Select this to allow the USG to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable IGMP Upstream on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable IGMP Downstream on the interface which connects to the multicast hosts.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Link-Local address	This displays the IPv6 link-local address and the network prefix that the USG generates itself for the interface.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to configure a static IP address for this interface. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the USG obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 145 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.

Table 76 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The USG will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 146 for more information.
DUID as MAC	Select this to have the DUID generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 Client. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If this interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 9.3.3 on page 165 for more information.
Remove	Select an entry and click this to change the settings.
Object Reference	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the USG obtained from an uplink router (Server is selected) or will advertise to its clients (Client is selected).
Interface	When Relay is selected, select this check box and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When Relay is selected, select this check box and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	

Table 76 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 146 for more information.
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the USG indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the USG indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the USG indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the USG indicate to hosts that DNS information is not available in this network.
Router Preference	Select the router preference (Low, Medium or High) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the USG. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the USG divides it into smaller fragments.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the USG to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The USG will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.

Table 76 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Address	This is the final network prefix combined by the delegated prefix and the suffix. Note: This field displays the combined address after you click **OK** and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the USG can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the USG can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the USG divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	The USG can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often to check the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the USG stops routing to the gateway. The USG resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select `icmp` to have the USG regularly ping the gateway you specify to make sure it is still available. Select `tcp` to have the USG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the USG stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the `Check Method` to `tcp`. Specify the port number to use for a TCP connectivity check.
DHCP Setting	The DHCP settings are available for the OPT, LAN and DMZ interfaces.
DHCP	Select what type of DHCP service the USG provides to the network. Choices are: `None` - the USG does not provide any DHCP services. There is already a DHCP server on the network. `DHCP Relay` - the USG routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. `DHCP Server` - the USG assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The USG is the DHCP server for the network.
	These fields appear if the USG is a `DHCP Relay`.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.

Table 76 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
	These fields appear if the USG is a DHCP Server.
IP Pool Start Address	Enter the IP address from which the USG begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click Add Static DHCP. If this field is blank, the Pool Size must also be blank. In this case, the USG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the USG can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the IP Pool Start Address must also be blank. In this case, the USG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. Custom Defined - enter a static IP address. From ISP - select the DNS server that another interface received from its DHCP server. USG - the DHCP clients use the IP address of this interface and the USG works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to DHCP Server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select Custom Defined and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: infinite - select this if IP addresses never expire days, hours, and minutes - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected DHCP server. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 9.3.4 on page 166.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the option's name.
Code	This is the option's code number.
Type	This is the option's type.
Value	This is the option's value.

Table 76 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Enable IP/MAC Binding	Select this option to have the USG enforce links between specific IP addresses and specific MAC addresses for this VLAN. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the USG generate a log if a device connected to this VLAN attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the USG assigns to computers connected to the interface. Otherwise, the USG assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC Address	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
RIP Setting	See Section 10.6 on page 239 for more information about RIP.
Enable RIP	Select this to enable RIP on this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. BiDir - This interface sends and receives routing information. In-Only - This interface receives routing information. Out-Only - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are 1, 2, and 1 and 2.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are 1, 2, and 1 and 2.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the USG uses multicasting.
OSPF Setting	See Section 10.7 on page 241 for more information about OSPF.
Area	Select the area in which this interface belongs. Select None to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.

Table 76 Configuration > Network > Interface > VLAN > Add / Edit (continued)

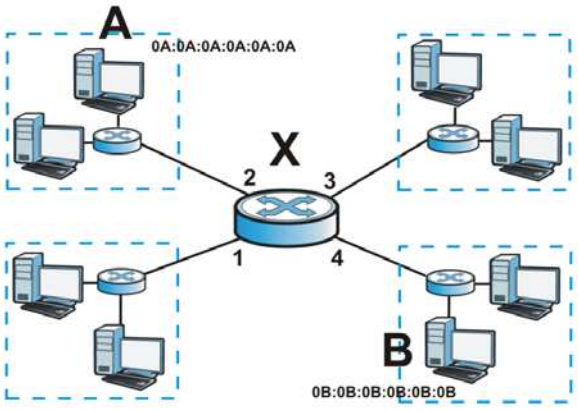
LABEL	DESCRIPTION
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: Same-as-Area - use the default authentication method in the area None - disable authentication Text - authenticate OSPF routing information using a plain-text password MD5 - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the Authentication is Text. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Related Setting	
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can set this VLAN to be part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the screen where you can manually configure a policy route to associate traffic with this VLAN.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

9.8 Bridge Interfaces

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

Bridge Overview

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



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

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

Table 77 Example: Bridge Table After Computer A Sends a Packet to Computer B

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

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

Table 78 Example: Bridge Table After Computer B Responds to Computer A

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

Bridge Interface Overview

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

Unlike the device-wide bridge mode in ZyNOS-based USGs, this USG can bridge traffic between some interfaces while it routes traffic for other interfaces. The bridge interfaces also support more functions, like interface bandwidth parameters, DHCP settings, and connectivity check. To use the whole USG as a transparent bridge, add all of the USG's interfaces to a bridge interface.

A bridge interface may consist of the following members:

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

When you create a bridge interface, the USG removes the members' entries from the routing table and adds the bridge interface's entries to the routing table. For example, this table shows the routing table before and after you create bridge interface br0 (250.250.250.0/23) between lan1 and vlan1.

Table 79 Example: Routing Table Before and After Bridge Interface br0 Is Created

IP ADDRESS(ES)	DESTINATION
210.210.210.0/24	lan1
210.211.1.0/24	lan1:1
221.221.221.0/24	vlan0
222.222.222.0/24	vlan1
230.230.230.192/26	wan2

IP ADDRESS(ES)	DESTINATION
221.221.221.0/24	vlan0
230.230.230.192/26	wan2
241.241.241.241/32	dmz
242.242.242.242/32	dmz
250.250.250.0/23	br0

Table 79 Example: Routing Table Before and After Bridge Interface br0 Is Created (continued)

IP ADDRESS(ES)	DESTINATION
241.241.241.241/32	dmz
242.242.242.242/32	dmz

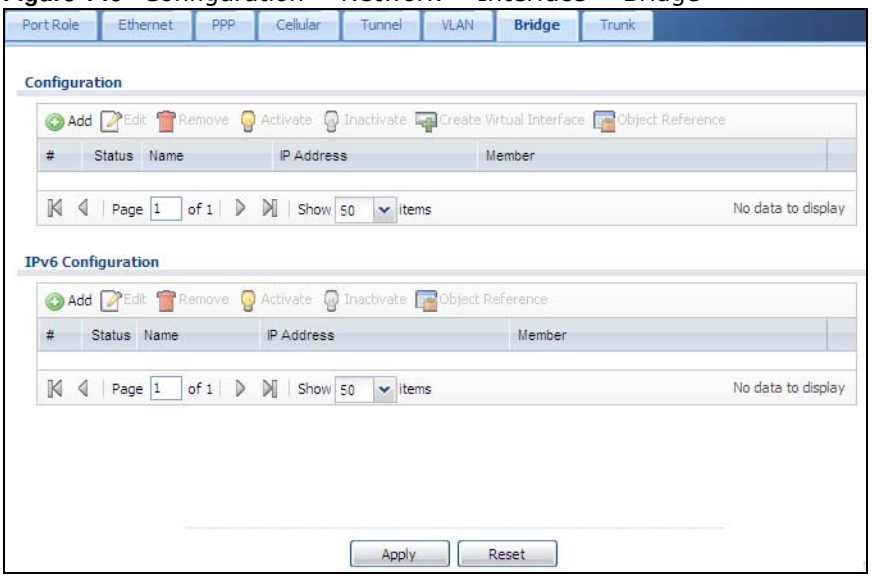
IP ADDRESS(ES)	DESTINATION

In this example, virtual Ethernet interface lan1:1 is also removed from the routing table when lan1 is added to br0. Virtual interfaces are automatically added to or remove from a bridge interface when the underlying interface is added or removed.

9.8.1 Bridge Summary

This screen lists every bridge interface and virtual interface created on top of bridge interfaces. If you enabled IPv6 in the Configuration > System > IPv6 screen, you can also configure bridge interfaces used for your IPv6 network on this screen. To access this screen, click Configuration > Network > Interface > Bridge.

Figure 140 Configuration > Network > Interface > Bridge



Each field is described in the following table.

Table 80 Configuration > Network > Interface > Bridge

LABEL	DESCRIPTION
Configuration / IPv6 Configuration	Use the Configuration section for IPv4 network settings. Use the IPv6 Configuration section for IPv6 network settings if you connect your USG to an IPv6 network. Both sections have similar fields as described below.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Create Virtual Interface	To open the screen where you can create a virtual interface, select an interface and click Create Virtual Interface.

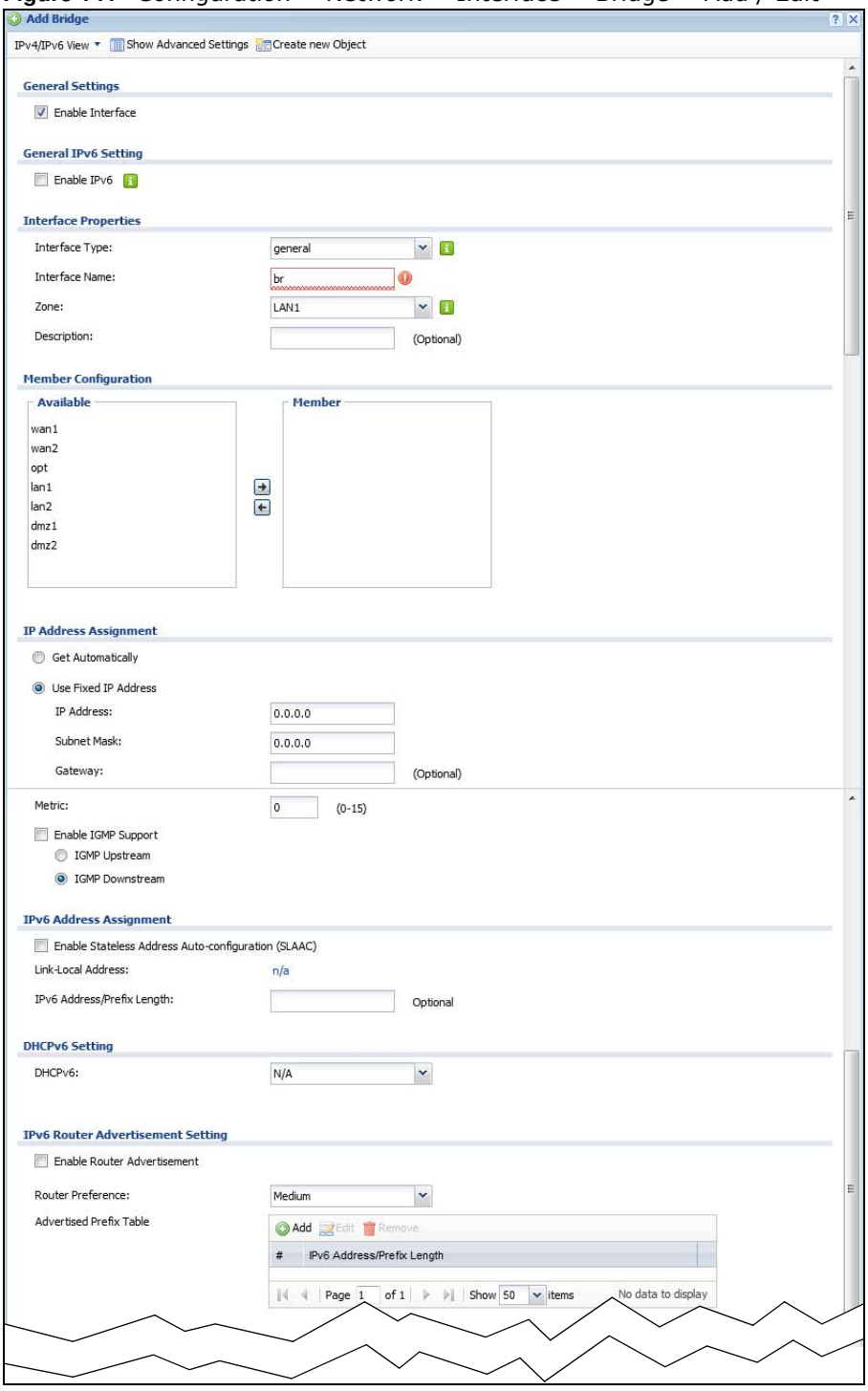
Table 80 Configuration > Network > Interface > Bridge (continued)

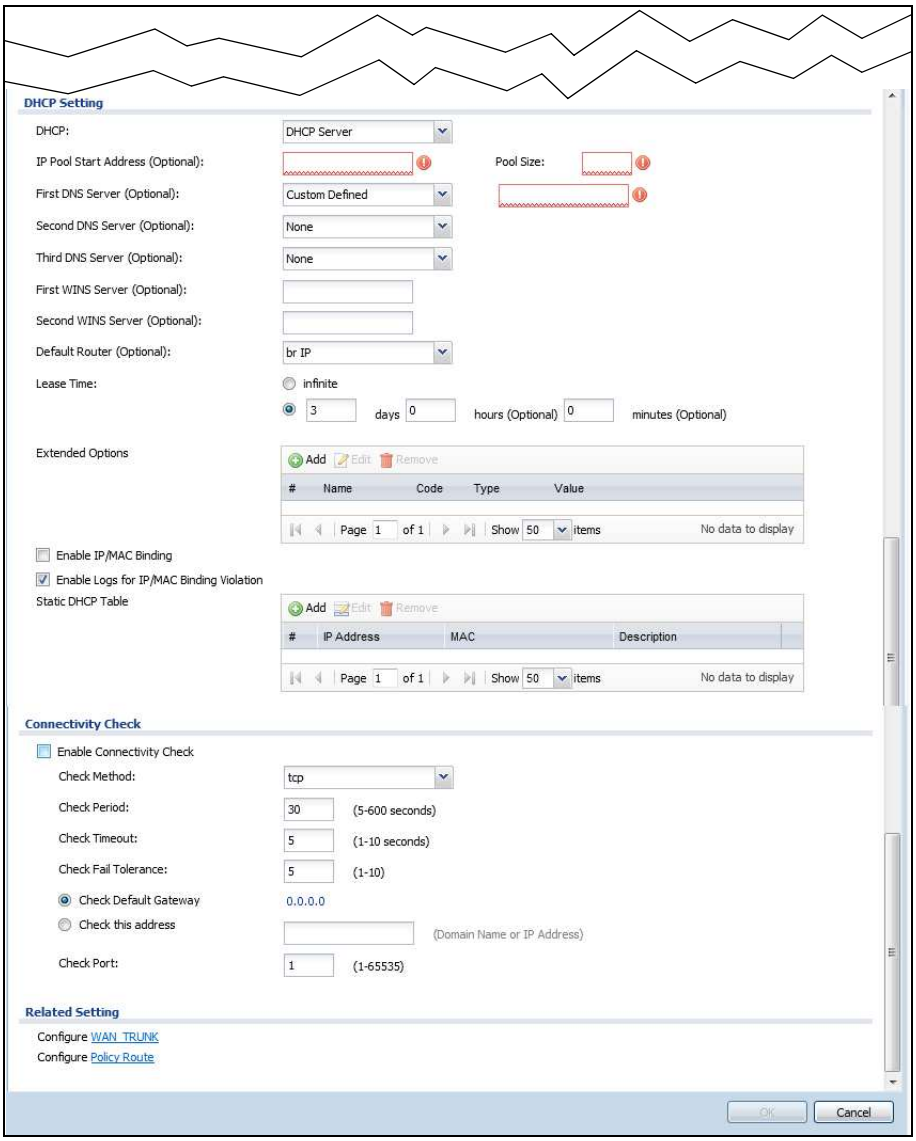
LABEL	DESCRIPTION
Object References	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (STATIC) or dynamically assigned (DHCP). IP addresses are always static in virtual interfaces.
Member	This field displays the Ethernet interfaces and VLAN interfaces in the bridge interface. It is blank for virtual interfaces.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

9.8.2 Bridge Add/Edit

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

Figure 141 Configuration > Network > Interface > Bridge > Add / Edit





Each field is described in the table below.

Table 81 Configuration > Network > Interface > Bridge > Add / Edit

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	

Table 81 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	Select one of the following option depending on the type of network to which the USG is connected or if you want to additionally manually configure some related settings. internal is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The USG automatically adds default SNAT settings for traffic flowing from this interface to an external interface. external is for connecting to an external network (like the Internet). The USG automatically adds this interface to the default WAN trunk. For general, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is br*x*, where *x* is 0 - 11. For example, br0, br3, and so on.
Zone	Select the zone to which the interface is to belong. You use zones to apply security settings such as security policy and remote management.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Member Configuration	
Available	This field displays Ethernet interfaces and VLAN interfaces that can become part of the bridge interface. An interface is not available in the following situations: • There is a virtual interface on top of it • It is already used in a different bridge interface Select one, and click the >> arrow to add it to the bridge interface. Each bridge interface can only have one VLAN interface.
Member	This field displays the interfaces that are part of the bridge interface. Select one, and click the << arrow to remove it from the bridge interface.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select Use Fixed IP Address. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select Use Fixed IP Address. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select Use Fixed IP Address. Enter the IP address of the gateway. The USG sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
Enable IGMP Support	Select this to allow the USG to act as an IGMP proxy for hosts connected on the IGMP downstream interface.

Table 81 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
IGMP Upstream	Enable IGMP Upstream on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable IGMP Downstream on the interface which connects to the multicast hosts.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Link-Local address	This displays the IPv6 link-local address and the network prefix that the USG generates itself for the interface.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the USG obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 145 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The USG will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 146 for more information.

Table 81 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 Client. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If the interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 9.3.3 on page 165 for more information.
Remove	Select an entry and click this to change the settings.
Object Reference	Select an entry and click this to delete it from this table.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the USG obtained from an uplink router (Server is selected) or will advertise to its clients (Client is selected).
Interface	When Relay is selected, select this check box and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When Relay is selected, select this check box and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 146 for more information.
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the USG indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the USG indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the USG indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the USG indicate to hosts that DNS information is not available in this network.

Table 81 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Router Preference	Select the router preference (Low, Medium or High) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the USG. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the USG divides it into smaller fragments.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the USG to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The USG will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.
Address	This is the final network prefix combined by the selected delegated prefix and the suffix. Note: This field displays the combined address after you click **OK** and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the USG can send through the interface to the network. Allowed values are 0 - 1048576.

Table 81 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the USG can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the USG divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
DHCP Setting	
DHCP	Select what type of DHCP service the USG provides to the network. Choices are: None - the USG does not provide any DHCP services. There is already a DHCP server on the network. DHCP Relay - the USG routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. DHCP Server - the USG assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The USG is the DHCP server for the network.
	These fields appear if the USG is a DHCP Relay.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the USG is a DHCP Server.
IP Pool Start Address	Enter the IP address from which the USG begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click Add Static DHCP. If this field is blank, the Pool Size must also be blank. In this case, the USG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the USG can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the IP Pool Start Address must also be blank. In this case, the USG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. Custom Defined - enter a static IP address. From ISP - select the DNS server that another interface received from its DHCP server. USG - the DHCP clients use the IP address of this interface and the USG works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to DHCP Server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select Custom Defined and enter the IP address.

Table 81 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: infinite - select this if IP addresses never expire days, hours, and minutes - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected DHCP server. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 9.3.4 on page 166.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the option's name.
Code	This is the option's code number.
Type	This is the option's type.
Value	This is the option's value.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the USG generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the USG assigns to computers connected to the interface. Otherwise, the USG assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC Address	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the USG stops routing to the gateway. The USG resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the USG regularly ping the gateway you specify to make sure it is still available. Select tcp to have the USG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.

Table 81 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the USG stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the screen where you can manually configure a policy route to associate traffic with this bridge interface.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

9.9 Virtual Interfaces

Use virtual interfaces to tell the USG where to route packets. Virtual interfaces can also be used in VPN gateways (see Chapter 21 on page 333).

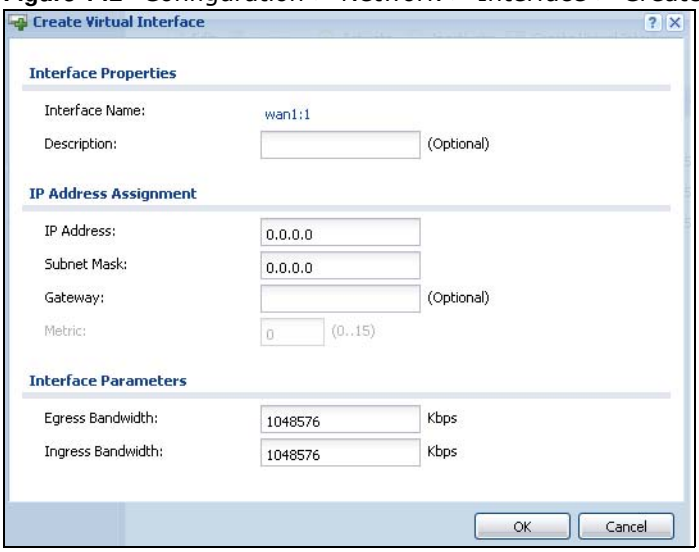
Virtual interfaces can be created on top of Ethernet interfaces, VLAN interfaces, or bridge interfaces. Virtual VLAN interfaces recognize and use the same VLAN ID. Otherwise, there is no difference between each type of virtual interface. Network policies (for example, security policies) that apply to the underlying interface automatically apply to the virtual interface as well.

Like other interfaces, virtual interfaces have an IP address, subnet mask, and gateway used to make routing decisions. However, you have to manually specify the IP address and subnet mask; virtual interfaces cannot be DHCP clients. Like other interfaces, you can restrict bandwidth through virtual interfaces, but you cannot change the MTU. The virtual interface uses the same MTU that the underlying interface uses. Unlike other interfaces, virtual interfaces do not provide DHCP services, and they do not verify that the gateway is available.

9.9.1 Virtual Interfaces Add/Edit

This screen lets you configure IP address assignment and interface parameters for virtual interfaces. To access this screen, click the Create Virtual Interface icon in the Ethernet, VLAN, or bridge interface summary screen.

Figure 142 Configuration > Network > Interface > Create Virtual Interface



Each field is described in the table below.

Table 82 Configuration > Network > Interface > Create Virtual Interface

LABEL	DESCRIPTION
Interface Properties	
Interface Name	This field is read-only. It displays the name of the virtual interface, which is automatically derived from the underlying Ethernet interface, VLAN interface, or bridge interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
IP Address Assignment	
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The USG sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The USG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the USG uses the one that was configured first.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the USG can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the USG can receive from the network through the interface. Allowed values are 0 - 1048576.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

9.10 Interface Technical Reference

Here is more detailed information about interfaces on the USG.

IP Address Assignment

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

Figure 143 Example: Entry in the Routing Table Derived from Interfaces

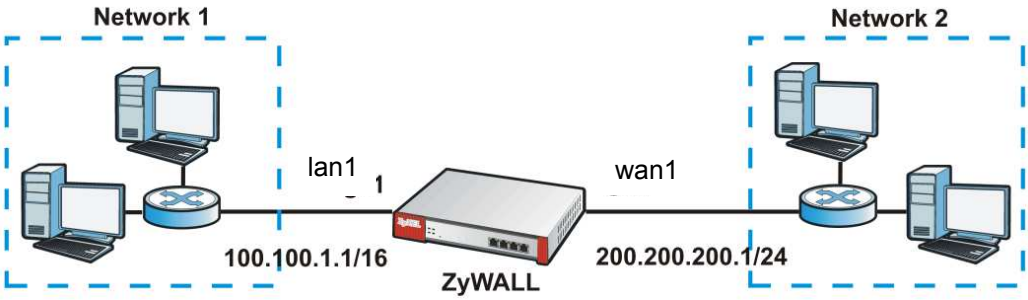


Table 83 Example: Routing Table Entries for Interfaces

IP ADDRESS(ES)	DESTINATION
100.100.1.1/16	lan1
200.200.200.1/24	wan1

For example, if the USG gets a packet with a destination address of 100.100.25.25, it routes the packet to interface lan1. If the USG gets a packet with a destination address of 200.200.200.200, it routes the packet to interface wan1.

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

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

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

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

Table 84 Example: Routing Table Entry for a Gateway

IP ADDRESS(ES)	DESTINATION
0.0.0.0/0	200.200.200.100

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

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

Interface Parameters

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

- Egress bandwidth sets the amount of traffic the USG sends out through the interface to the network.
- Ingress bandwidth sets the amount of traffic the USG allows in through the interface from the network.At the time of writing, the USG does not support ingress bandwidth management.

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

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

DHCP Settings

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

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

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

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

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

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

Table 85 Example: Assigning IP Addresses from a Pool

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

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

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

- Subnet mask - The interface provides the same subnet mask you specify for the interface. See IP Address Assignment on page 216.
- Gateway - The interface provides the same gateway you specify for the interface. See IP Address Assignment on page 216.
- DNS servers - The interface provides IP addresses for up to three DNS servers that provide DNS services for DHCP clients. You can specify each IP address manually (for example, a company's own DNS server), or you can refer to DNS servers that other interfaces received from DHCP servers (for example, a DNS server at an ISP). These other interfaces have to be DHCP clients.

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

WINS

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

PPPoE/PPTP Overview

Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) and Point-to-Point Tunneling Protocol (PPTP, RFC 2637) are usually used to connect two computers over phone lines or broadband connections. PPPoE is often used with cable modems and DSL connections. It provides the following advantages:

- The access and authentication method works with existing systems, including RADIUS.
- You can access one of several network services. This makes it easier for the service provider to offer the service

- PPPoE does not usually require any special configuration of the modem.

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

1 The first one runs on TCP port 1723. It is used to start and manage the second one.

2 The second one uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers.

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

9.11 Trunk Overview

Use trunks for WAN traffic load balancing to increase overall network throughput and reliability. Load balancing divides traffic loads between multiple interfaces. This allows you to improve quality of service and maximize bandwidth utilization for multiple ISP links.

Maybe you have two Internet connections with different bandwidths. You could set up a trunk that uses spillover or weighted round robin load balancing so time-sensitive traffic (like video) usually goes through the higher-bandwidth interface. For other traffic, you might want to use least load first load balancing to even out the distribution of the traffic load.

Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routes and trunks to have traffic for your European branch office primarily use ISP A and traffic for your Australian branch office primarily use ISP B.

Or maybe one of the USG's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You can use policy routing to send the VoIP traffic through a trunk with the interface connected to the VoIP service provider set to active and another interface (connected to another ISP) set to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface's connection is up.

- Use the Trunk summary screen (Section 9.12 on page 222) to view the list of configured trunks and which load balancing algorithm each trunk uses.
- Use the Add Trunk screen (Section 9.12.1 on page 223) to configure the member interfaces for a trunk and the load balancing algorithm the trunk uses.
- Use the Add System Default screen (Section 9.12.2 on page 225) to configure the load balancing algorithm for the system default trunk.

9.11.1 What You Need to Know

- Add WAN interfaces to trunks to have multiple connections share the traffic load.
- If one WAN interface's connection goes down, the USG sends traffic through another member of the trunk.
- For example, you connect one WAN interface to one ISP and connect a second WAN interface to a second ISP. The USG balances the WAN traffic load between the connections. If one interface's connection goes down, the USG can automatically send its traffic through another interface.

You can also use trunks with policy routing to send specific traffic types through the best WAN interface for that type of traffic.

- If that interface's connection goes down, the USG can still send its traffic through another interface.
- You can define multiple trunks for the same physical interfaces.

1 LAN user A logs into server B on the Internet. The USG uses wan1 to send the request to server B.

2 The USG is using active/active load balancing. So when LAN user A tries to access something on the server, the request goes out through wan2.

3 The server finds that the request comes from wan2's IP address instead of wan1's IP address and rejects the request.

If link sticking had been configured, the USG would have still used wan1 to send LAN user A's request to the server and server would have given the user A access.

Load Balancing Algorithms

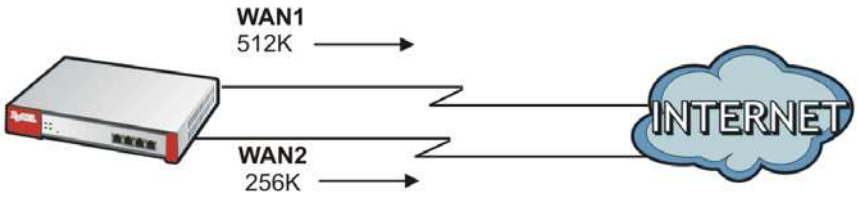
The following sections describe the load balancing algorithms the USG can use to decide which interface the traffic (from the LAN) should use for a session. In the load balancing section, a session may refer to normal connection-oriented, UDP or SNMP2 traffic. The available bandwidth you configure on the USG refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

Least Load First

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

Here the USG has two WAN interfaces connected to the Internet. The configured available outbound bandwidths for WAN 1 and WAN 2 are 512K and 256K respectively.

Figure 144 Least Load First Example



The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of WAN 1 is 412K and WAN 2 is 198K. The USG calculates the load balancing index as shown in the table below.

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

Table 86 Least Load First Example

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

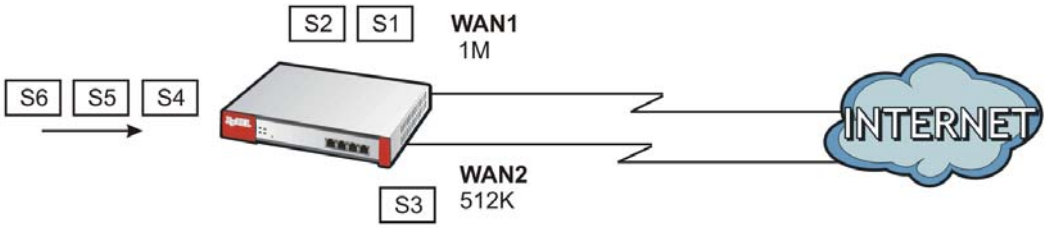
Weighted Round Robin

Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that interface. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

The Weighted Round Robin (WRR) algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different. Similar to the Round Robin (RR) algorithm, the Weighted Round Robin (WRR) algorithm sets the USG to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.

For example, in the figure below, the configured available bandwidth of WAN1 is 1M and WAN2 is 512K. You can set the USG to distribute the network traffic between the two interfaces by setting the weight of wan1 and wan2 to 2 and 1 respectively. The USG assigns the traffic of two sessions to wan1 and one session's traffic to wan2 in each round of 3 new sessions.

Figure 145 Weighted Round Robin Algorithm Example



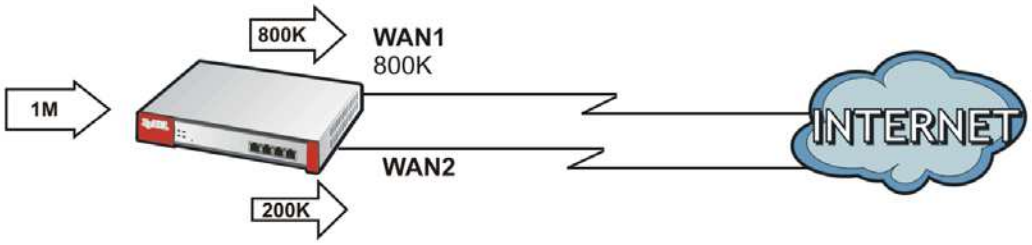
Spillover

The spillover load balancing algorithm sends network traffic to the first interface in the trunk member list until the interface’s maximum allowable load is reached, then sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

Suppose the first trunk member interface uses an unlimited access Internet connection and the second is billed by usage. Spillover load balancing only uses the second interface when the traffic load exceeds the threshold on the first interface. This fully utilizes the bandwidth of the first interface to reduce Internet usage fees and avoid overloading the interface.

In this example figure, the upper threshold of the first interface is set to 800K. The USG sends network traffic of new sessions that exceed this limit to the secondary WAN interface.

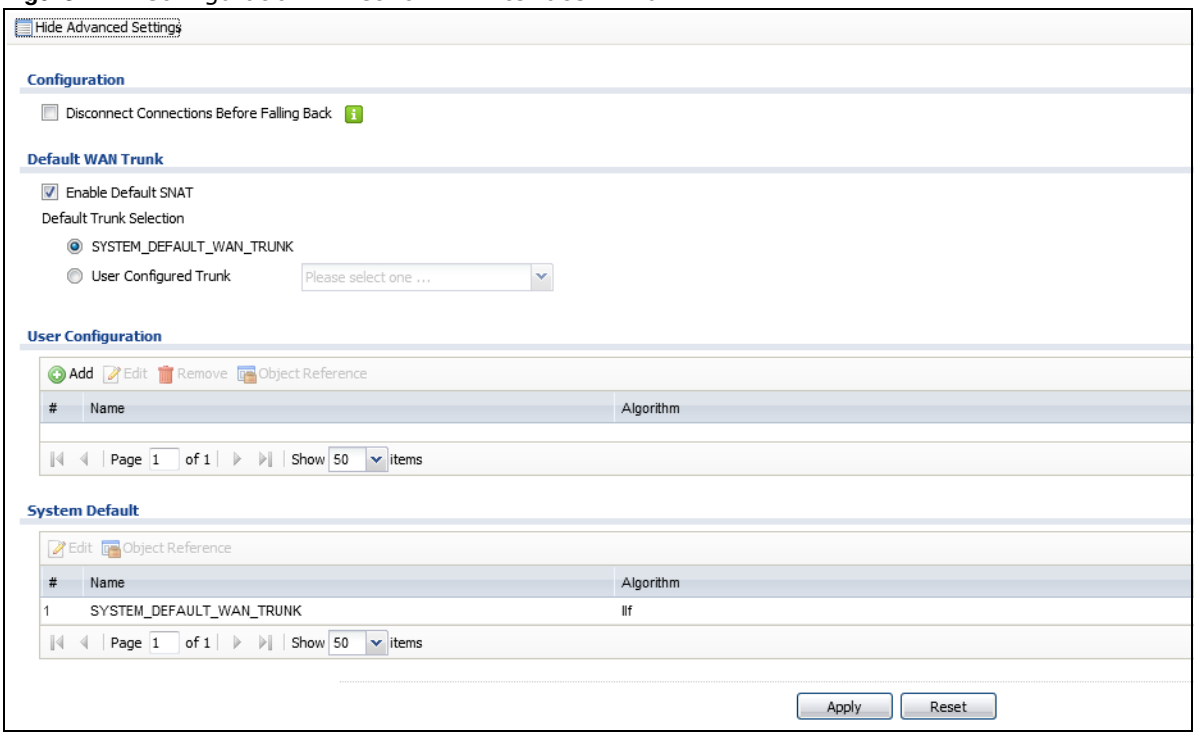
Figure 146 Spillover Algorithm Example



9.12 The Trunk Summary Screen

Click Configuration > Network > Interface > Trunk to open the Trunk screen. This screen lists the configured trunks and the load balancing algorithm that each is configured to use.

Figure 147 Configuration > Network > Interface > Trunk



The following table describes the items in this screen.

Table 87 Configuration > Network > Interface > Trunk

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Configuration	Configure what to do with existing passive mode interface connections when an interface set to active mode in the same trunk comes back up.
Disconnect Connections Before Falling Back	Select this to terminate existing connections on an interface which is set to passive mode when any interface set to active mode in the same trunk comes back up.

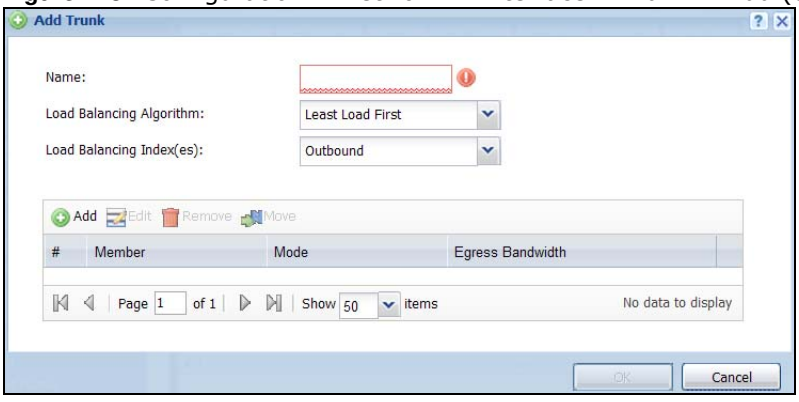
Table 87 Configuration > Network > Interface > Trunk (continued)

LABEL	DESCRIPTION
Enable Default SNAT	Select this to have the USG use the IP address of the outgoing interface as the source IP address of the packets it sends out through its WAN trunks. The USG automatically adds SNAT settings for traffic it routes from internal interfaces to external interfaces.
Default Trunk Selection	Select whether the USG is to use the default system WAN trunk or one of the user configured WAN trunks as the default trunk for routing traffic from internal interfaces to external interfaces.
User Configuration / System Default	The USG automatically adds all external interfaces into the pre-configured system default SYSTEM_DEFAULT_WAN_TRUNK. You cannot delete it. You can create your own User Configuration trunks and customize the algorithm, member interfaces and the active/passive mode.
Add	Click this to create a new user-configured trunk.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the label that you specified to identify the trunk.
Algorithm	This field displays the load balancing method the trunk is set to use.
Apply	Click this button to save your changes to the USG.
Reset	Click this button to return the screen to its last-saved settings.

9.12.1 Configuring a User-Defined Trunk

Click Configuration > Network > Interface > Trunk, in the User Configuration table click the Add (or Edit) icon to open the following screen. Use this screen to create or edit a WAN trunk entry.

Figure 148 Configuration > Network > Interface > Trunk > Add (or Edit)



Each field is described in the table below.

Table 88 Configuration > Network > Interface > Trunk > Add (or Edit)

LABEL	DESCRIPTION
Name	This is read-only if you are editing an existing trunk. When adding a new trunk, enter a descriptive name for this trunk. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box. Select Weighted Round Robin to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the USG chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. Select Least Load First to send new session traffic through the least utilized trunk member. Select Spillover to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).
Load Balancing Index(es)	This field is available if you selected to use the Least Load First or Spillover method. Select Outbound, Inbound, or Outbound + Inbound to set the traffic to which the USG applies the load balancing method. Outbound means the traffic traveling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound means the opposite.
	The table lists the trunk's member interfaces. You can add, edit, remove, or move entries for user configured trunks.
Add	Click this to add a member interface to the trunk. Select an interface and click Add to add a new member interface after the selected member interface.
Edit	Select an entry and click Edit to modify the entry's settings.
Remove	To remove a member interface, select it and click Remove. The USG confirms you want to remove it before doing so.
Move	To move an interface to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the interface.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	Click this table cell and select an interface to be a group member. If you select an interface that is part of another Ethernet interface, the USG does not send traffic through the interface as part of the trunk. For example, if you have physical port 5 in the ge2 representative interface, you must select interface ge2 in order to send traffic through port 5 as part of the trunk. If you select interface ge5 as a member here, the USG will not send traffic through port 5 as part of the trunk.
Mode	Click this table cell and select Active to have the USG always attempt to use this connection. Select Passive to have the USG only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the USG assigns to each member interface. The higher an interface's weight is (relative to the weights of the interfaces), the more sessions that interface should handle.

Table 88 Configuration > Network > Interface > Trunk > Add (or Edit) (continued)

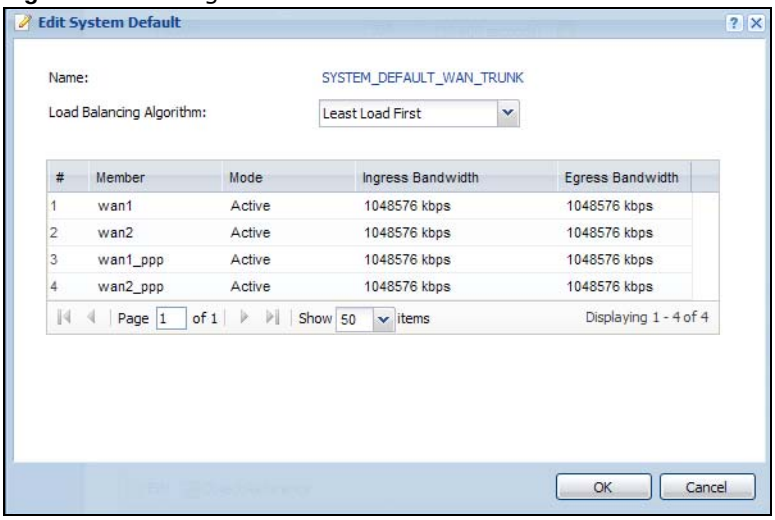
LABEL	DESCRIPTION
Ingress Bandwidth	This is reserved for future use. This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the USG is to allow to come in through the interface per second. Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the USG is to send out through the interface per second. Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the USG sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The USG uses the group member interfaces in the order that they are listed.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

9.12.2 Configuring the System Default Trunk

In the Configuration > Network > Interface > Trunk screen and the System Default section, select the default trunk entry and click Edit to open the following screen. Use this screen to change the load balancing algorithm and view the bandwidth allocations for each member interface.

Note: The available bandwidth is allocated to each member interface equally and is not allowed to be changed for the default trunk.

Figure 149 Configuration > Network > Interface > Trunk > Edit (System Default)



Each field is described in the table below.

Table 89 Configuration > Network > Interface > Trunk > Edit (System Default)

LABEL	DESCRIPTION
Name	This field displays the name of the selected system default trunk.
Load Balancing Algorithm	Select the load balancing method to use for the trunk. Select Weighted Round Robin to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the USG chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. Select Least Load First to send new session traffic through the least utilized trunk member. Select Spillover to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).
	The table lists the trunk's member interfaces. This table is read-only.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	This column displays the name of the member interfaces.
Mode	This field displays Active if the USG always attempt to use this connection. This field displays Passive if the USG only use this connection when all of the connections set to active are down. Only one of a group's interfaces can be set to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. s
Ingress Bandwidth	This is reserved for future use. This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the USG is to allow to come in through the interface per second.
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the USG is to send out through the interface per second.
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the USG sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The USG uses the group member interfaces in the order that they are listed.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

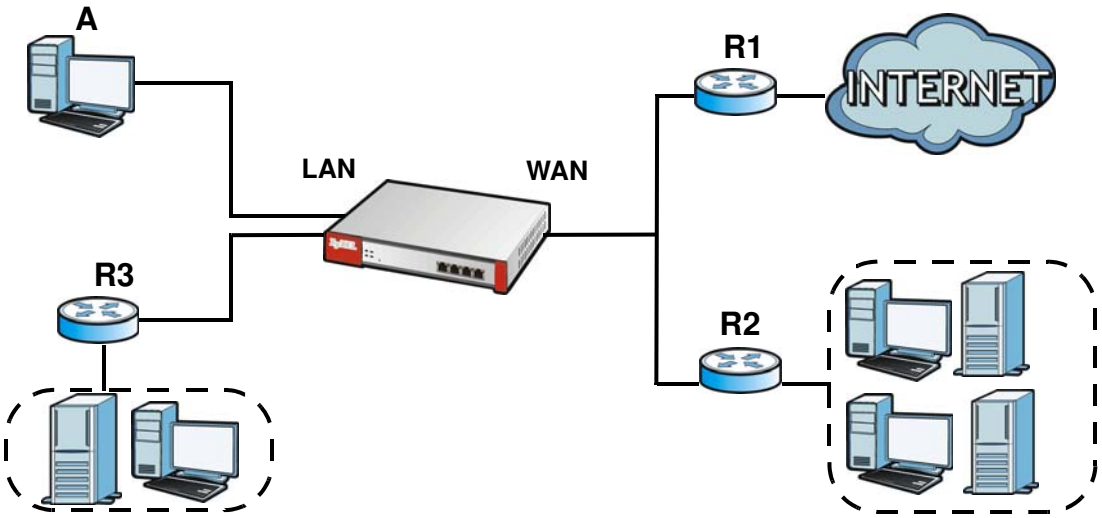
10 Routing

10.1 Policy and Static Routes Overview

Use policy routes and static routes to override the USG's default routing behavior in order to send packets through the appropriate interface or VPN tunnel.

For example, the next figure shows a computer (A) connected to the USG's LAN interface. The USG routes most traffic from A to the Internet through the USG's default gateway (R1). You create one policy route to connect to services offered by your ISP behind router R2. You create another policy route to communicate with a separate network behind another router (R3) connected to the LAN.

Figure 150 Example of Policy Routing Topology



Note: You can generally just use policy routes. You only need to use static routes if you have a large network with multiple routers where you use RIP or OSPF to propagate routing information to other routers.

10.1.1 What You Can Do in this Chapter

- Use the Policy Route screens (see Section 10.2 on page 229) to list and configure policy routes.
- Use the Static Route screens (see Section 10.3 on page 236) to list and configure static routes.

10.1.2 What You Need to Know

Policy Routing

Traditionally, routing is based on the destination address only and the USG 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.

How You Can Use Policy Routing

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Bandwidth Shaping – You can allocate bandwidth to traffic that matches routing policies and prioritize traffic. You can also use policy routes to manage other types of traffic (like ICMP traffic) and send traffic through VPN tunnels.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The USG performs NAT by default for traffic going to or from the WAN interfaces. A routing policy's SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.

Note: The USG automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic.

Static Routes

The USG usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the USG send data to devices not reachable through the default gateway, use static routes. Configure static routes if you need to use RIP or OSPF to propagate the routing information to other routers. See Chapter 10 on page 239 for more on RIP and OSPF.

Policy Routes Versus Static Routes

- Policy routes are more flexible than static routes. You can select more criteria for the traffic to match and can also use schedules, NAT, and bandwidth management.
- Policy routes are only used within the USG itself. Static routes can be propagated to other routers using RIP or OSPF.
- Policy routes take priority over static routes. If you need to use a routing policy on the USG and propagate it to other routers, you could configure a policy route and an equivalent static route.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP Marking and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP (6 bits)	Unused (2 bits)

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

10.2 Policy Route Screen

Click Configuration > Network > Routing to open the Policy Route screen. Use this screen to see the configured policy routes and turn policy routing based bandwidth management on or off.

A policy route defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

The actions that can be taken include:

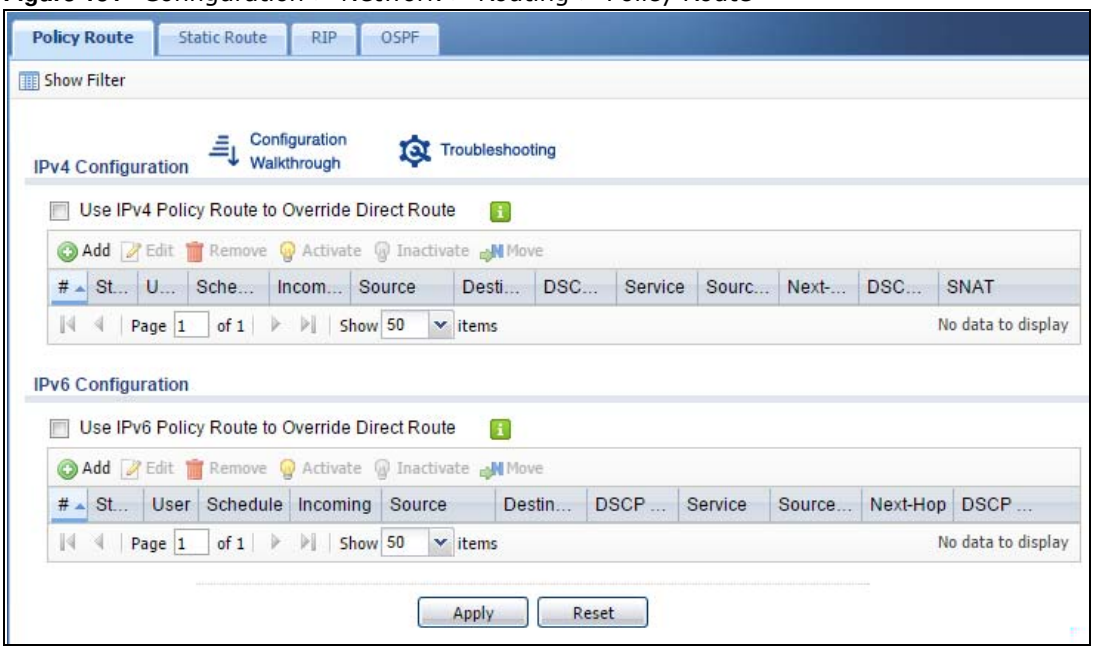
- Routing the packet to a different gateway, outgoing interface, VPN tunnel, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

If you enabled IPv6 in the Configuration > System > IPv6 screen, you can also configure policy routes used for your IPv6 networks on this screen.

Click on the icons to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting, and other information.

Figure 151 Configuration > Network > Routing > Policy Route



The following table describes the labels in this screen.

Table 90 Configuration > Network > Routing > Policy Route

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable BWM	This is a global setting for enabling or disabling bandwidth management on the USG. You must enable this setting to have individual policy routes apply bandwidth management.
IPv4 Configuration / IPv6 Configuration	Use the IPv4 Configuration section for IPv4 network settings. Use the IPv6 Configuration section for IPv6 network settings if you connect your USG to an IPv6 network. Both sections have similar fields as described below.
Use IPv4/IPv6 Policy Route to Override Direct Route	Select this to have the USG forward packets that match a policy route according to the policy route instead of sending the packets directly to a connected network.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This is the number of an individual policy route.

Table 90 Configuration > Network > Routing > Policy Route (continued)

LABEL	DESCRIPTION
Status	This icon is lit when the entry is active, red when the next hop's connection is down, and dimmed when the entry is inactive.
User	This is the name of the user (group) object from which the packets are sent. any means all users.
Schedule	This is the name of the schedule object. none means the route is active at all times if enabled.
Incoming	This is the interface on which the packets are received.
Source	This is the name of the source IP address (group) object. any means all IP addresses.
Destination	This is the name of the destination IP address (group) object. any means all IP addresses.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. any means all DSCP values or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic The "af" entries stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 238 for more details.
Service	This is the name of the service object. any means all services.
Source Port	This is the name of a service object. The USG applies the policy route to the packets sent from the corresponding service port. any means all service ports.
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, outgoing interface or trunk.
DSCP Marking	This is how the USG handles the DSCP value of the outgoing packets that match this route. If this field displays a DSCP value, the USG applies that DSCP value to the route's outgoing packets. preserve means the USG does not modify the DSCP value of the route's outgoing packets. default means the USG sets the DSCP value of the route's outgoing packets to 0. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 238 for more details.
SNAT	This is the source IP address that the route uses. It displays none if the USG does not perform NAT for this route.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

10.2.1 Policy Route Edit Screen

Click Configuration > Network > Routing to open the Policy Route screen. Then click the Add or Edit icon in the IPv4 Configuration or IPv6 Configuration section. The Add Policy Route or Policy Route Edit screen opens. Use this screen to configure or edit a policy route. Both IPv4 and IPv6 policy route have similar settings except the Address Translation (SNAT) settings.

Figure 152 Configuration > Network > Routing > Policy Route > Add/Edit (IPv4 Configuration)

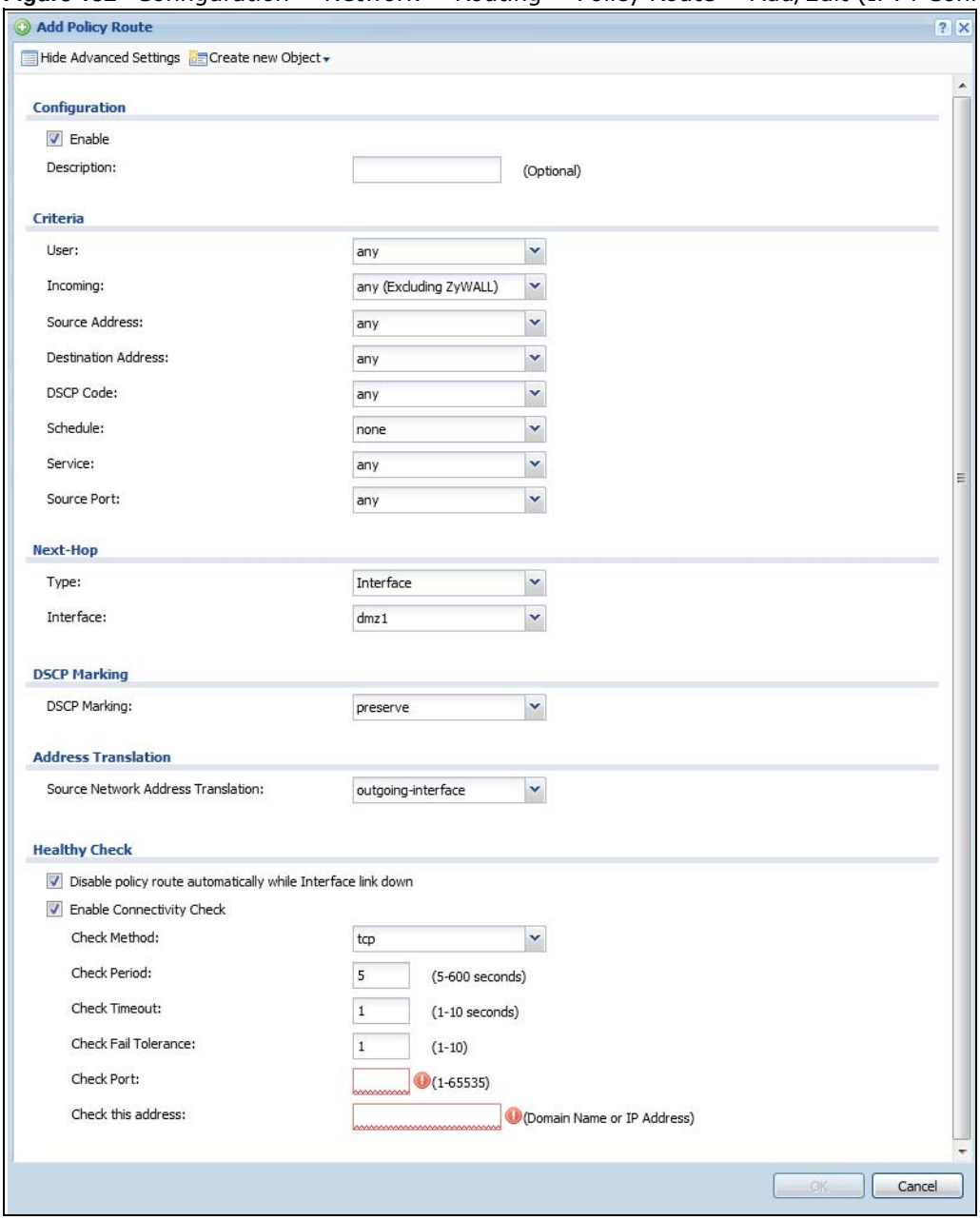
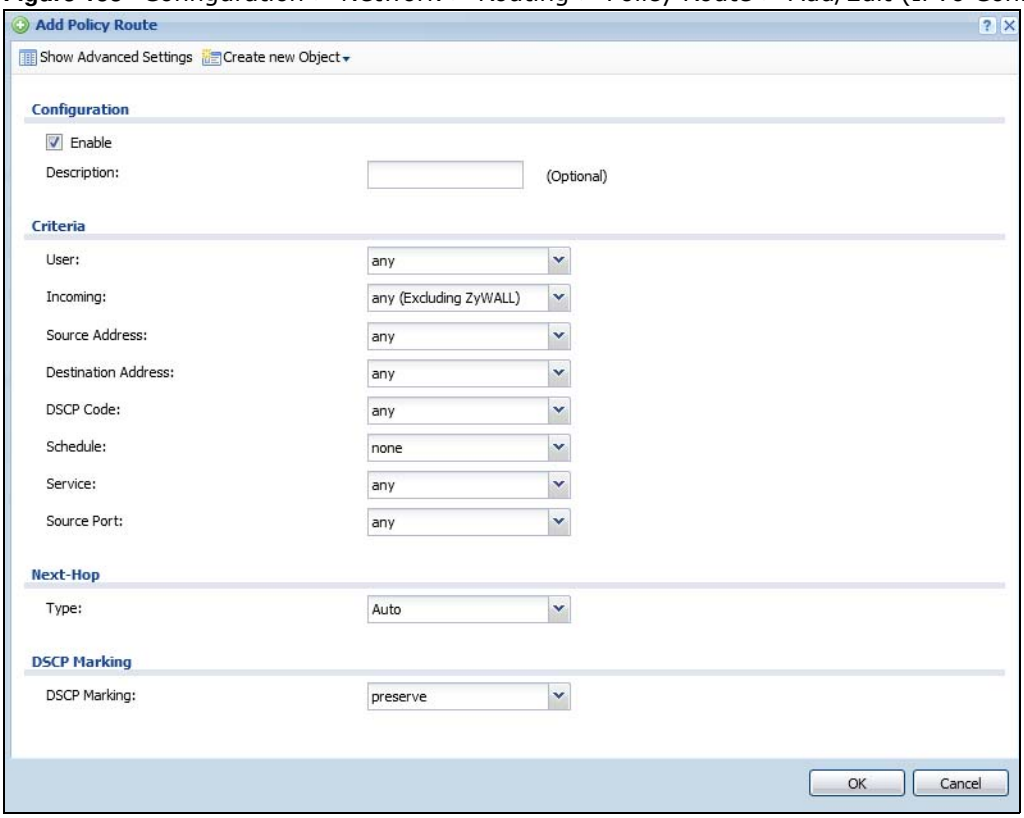


Figure 153 Configuration > Network > Routing > Policy Route > Add/Edit (IPv6 Configuration)



The following table describes the labels in this screen.

Table 91 Configuration > Network > Routing > Policy Route > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Configuration	
Enable	Select this to activate the policy.
Description	Enter a descriptive name of up to 31 printable ASCII characters for the policy.
Criteria	
User	Select a user name or user group from which the packets are sent.
Incoming	Select where the packets are coming from; any, an interface, a tunnel, an SSL VPN, or the USG itself. For an interface, a tunnel, or an SSL VPN, you also need to select the individual interface, VPN tunnel, or SSL VPN connection.
Source Address	Select a source IP address object from which the packets are sent.
Destination Address	Select a destination IP address object to which the traffic is being sent. If the next hop is a dynamic VPN tunnel and you enable Auto Destination Address, the USG uses the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of your configuration here.

Table 91 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select User Define to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. any means all DSCP value or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 238 for more details.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point when you select User Define in the previous field.
Schedule	Select a schedule to control when the policy route is active. none means the route is active at all times if enabled.
Service	Select a service or service group to identify the type of traffic to which this policy route applies.
Source Port	Select a service or service group to identify the source port of packets to which the policy route applies.
Next-Hop	
Type	Select Auto to have the USG use the routing table to find a next-hop and forward the matched packets automatically. Select Gateway to route the matched packets to the next-hop router or switch you specified in the Gateway field. You have to set up the next-hop router or switch as a HOST address object first. Select VPN Tunnel to route the matched packets via the specified VPN tunnel. Select Trunk to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm. Select Interface to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).
Gateway	This field displays when you select Gateway in the Type field. Select a HOST address object. The gateway is an immediate neighbor of your USG that will forward the packet to the destination. The gateway must be a router or switch on the same segment as your USG's interface(s).
VPN Tunnel	This field displays when you select VPN Tunnel in the Type field. Select a VPN tunnel through which the packets are sent to the remote network that is connected to the USG directly.
Auto Destination Address	This field displays when you select VPN Tunnel in the Type field. Select this to have the USG use the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy. Leave this cleared if you want to manually specify the destination address.
Trunk	This field displays when you select Trunk in the Type field. Select a trunk group to have the USG send the packets via the interfaces in the group.
Interface	This field displays when you select Interface in the Type field. Select an interface to have the USG send traffic that matches the policy route through the specified interface.

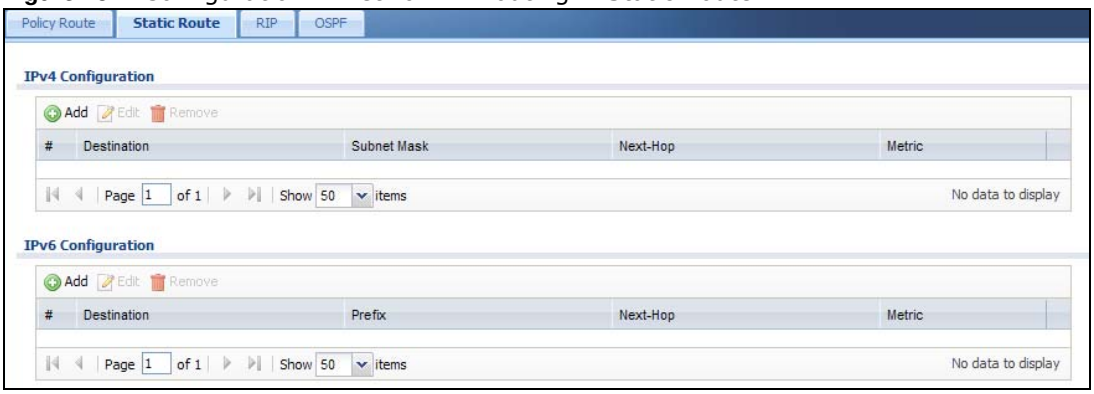
Table 91 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
DSCP Marking	Set how the USG handles the DSCP value of the outgoing packets that match this route. Select one of the pre-defined DSCP values to apply or select User Define to specify another DSCP value. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 238 for more details. Select preserve to have the USG keep the packets' original DSCP value. Select default to have the USG set the DSCP value of the packets to 0.
User-Defined DSCP Code	Use this field to specify a custom DSCP value.
Address Translation	Use this section to configure NAT for the policy route. This section does not apply to policy routes that use a VPN tunnel as the next hop.
Source Network Address Translation	Select none to not use NAT for the route. Select outgoing-interface to use the IP address of the outgoing interface as the source IP address of the packets that matches this route. To use SNAT for a virtual interface that is in the same WAN trunk as the physical interface to which the virtual interface is bound, the virtual interface and physical interface must be in different subnets. Otherwise, select a pre-defined address (group) to use as the source IP address(es) of the packets that match this route. Use Create new Object if you need to configure a new address (group) to use as the source IP address(es) of the packets that match this route.
Healthy Check	Use this part of the screen to configure a route connectivity check and disable the policy if the interface is down.
Disable policy route automatically while Interface link down	Select this to disable the policy if the interface is down or disabled. This is available for Interface and Trunk in the Type field above.
Enable Connectivity Check	Select this to turn on the connection check. This is available for Interface and Gateway in the Type field above.
Check Method:	Select the method that the gateway allows. Select icmp to have the USG regularly ping the gateway you specify to make sure it is still available. Select tcp to have the USG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period:	Enter the number of seconds between connection check attempts (5-600 seconds).
Check Timeout:	Enter the number of seconds to wait for a response before the attempt is a failure (1-10 seconds).
Check Fail Tolerance:	Enter the number of consecutive failures before the USG stops routing using this policy (1-10).
Check Port:	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check (1-65535).
Check this address:	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

10.3 IP Static Route Screen

Click Configuration > Network > Routing > Static Route to open the Static Route screen. This screen displays the configured static routes. Configure static routes to be able to use RIP or OSPF to propagate the routing information to other routers. If you enabled IPv6 in the Configuration > System > IPv6 screen, you can also configure static routes used for your IPv6 networks on this screen.

Figure 154 Configuration > Network > Routing > Static Route



The following table describes the labels in this screen.

Table 92 Configuration > Network > Routing > Static Route

LABEL	DESCRIPTION
IPv4 Configuration / IPv6 Configuration	Use the IPv4 Configuration section for IPv4 network settings. Use the IPv6 Configuration section for IPv6 network settings if you connect your USG to an IPv6 network. Both sections have similar fields as described below.
Add	Click this to create a new static route.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
#	This is the number of an individual static route.
Destination	This is the destination IP address.
Subnet Mask	This is the IP subnet mask.
Prefix	This is the IPv6 prefix for the destination IP address.
Next-Hop	This is the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or switch on the same segment as your USG's interface(s). The gateway helps forward packets to their destinations.
Metric	This is the route's priority among the USG's routes. The smaller the number, the higher priority the route has.

10.3.1 Static Route Add/Edit Screen

Select a static route index number and click Add or Edit. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 155 Configuration > Network > Routing > Static Route > Add (IPv4 Configuration)

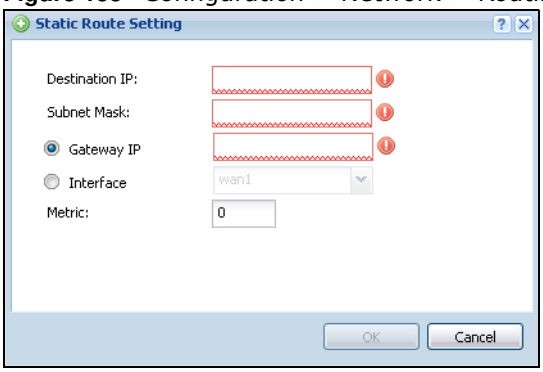
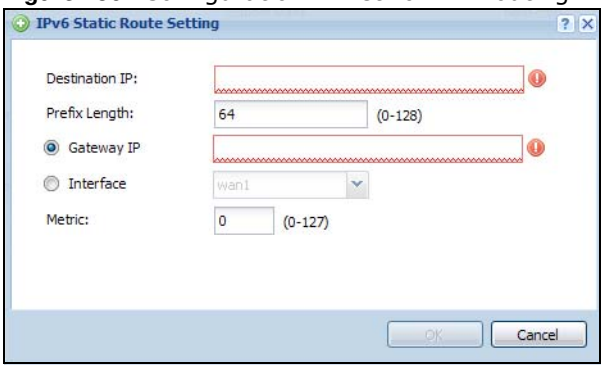


Figure 156 Configuration > Network > Routing > Static Route > Add (IPv6 Configuration)



The following table describes the labels in this screen.

Table 93 Configuration > Network > Routing > Static Route > Add

LABEL	DESCRIPTION
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, enter the specific IP address here and use a subnet mask of 255.255.255.255 (for IPv4) in the Subnet Mask field or a prefix of 128 (for IPv6) in the Prefix Length field to force the network number to be identical to the host ID. For IPv6, if you want to send all traffic to the gateway or interface specified in the Gateway IP or Interface field, enter :: in this field and 0 in the Prefix Length field.
Subnet Mask	Enter the IP subnet mask here.
Prefix Length	Enter the number of left-most digits in the destination IP address, which indicates the network prefix. Enter :: in the Destination IP field and 0 in this field if you want to send all traffic to the gateway or interface specified in the Gateway IP or Interface field.
Gateway IP	Select the radio button and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your USG's interface(s). The gateway helps forward packets to their destinations.
Interface	Select the radio button and a predefined interface through which the traffic is sent.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be 0~127. In practice, 2 or 3 is usually a good number.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

10.4 Policy Routing Technical Reference

Here is more detailed information about some of the features you can configure in policy routing.

NAT and SNAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address in a packet in one network to a different IP address in another network. Use SNAT (Source NAT) to change the source IP address in one network to a different IP address in another network.

Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers in the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

Table 94 Assured Forwarding (AF) Behavior Group

	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low Drop Precedence	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Medium Drop Precedence	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
High Drop Precedence	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

Maximize Bandwidth Usage

The maximize bandwidth usage option allows the USG to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a policy route is not using) among the policy routes that require more bandwidth.

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

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

10.5 Routing Protocols Overview

Routing protocols give the USG routing information about the network from other routers. The USG stores this routing information in the routing table it uses to make routing decisions. In turn, the USG can also use routing protocols to propagate routing information to other routers.

Routing protocols are usually only used in networks using multiple routers like campuses or large enterprises.

- Use the RIP screen (see Section 10.6 on page 239) to configure the USG to use RIP to receive and/or send routing information.
- Use the OSPF screen (see Section 10.7 on page 241) to configure general OSPF settings and manage OSPF areas.
- Use the OSPF Area Add/ Edit screen (see Section 10.7.2 on page 245) to create or edit an OSPF area.

10.5.1 What You Need to Know

The USG supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared here and discussed further in the rest of the chapter.

Table 95 RIP vs. OSPF

	RIP	OSPF
Network Size	Small (with up to 15 routers)	Large
Metric	Hop count	Bandwidth, hop count, throughput, round trip time and reliability.
Convergence	Slow	Fast

Finding Out More

See Section 10.8 on page 248 for background information on routing protocols.

10.6 The RIP Screen

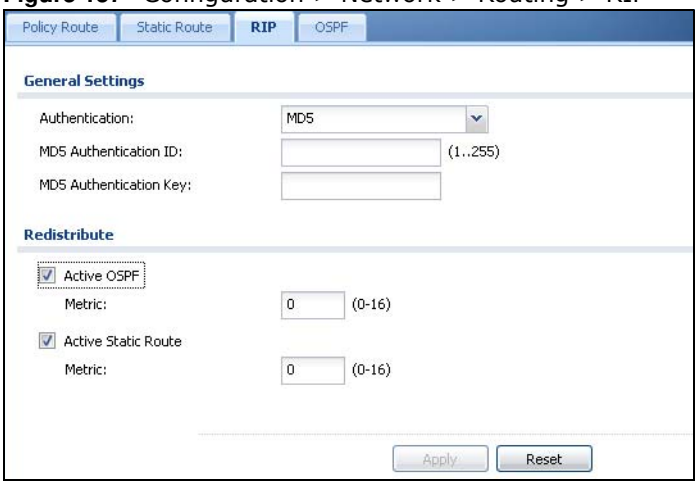
RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers. RIP is a vector-space routing protocol, and, like most such protocols, it uses hop count to decide which route is the shortest. Unfortunately, it also broadcasts its routes asynchronously to the network and converges slowly. Therefore, RIP is more suitable for small networks (up to 15 routers).

- In the USG, you can configure two sets of RIP settings before you can use it in an interface.
- First, the Authentication field specifies how to verify that the routing information that is received is the same routing information that is sent. This is discussed in more detail in Authentication Types on page 248.
- Second, the USG can also redistribute routing information from non-RIP networks, specifically OSPF networks and static routes, to the RIP network. Costs might be calculated differently, however, so you use the Metric field to specify the cost in RIP terms.
- RIP uses UDP port 520.

Use the RIP screen to specify the authentication method and maintain the policies for redistribution.

Click Configuration > Network > Routing > RIP to open the following screen.

Figure 157 Configuration > Network > Routing > RIP



The following table describes the labels in this screen.

Table 96 Configuration > Network > Routing Protocol > RIP

LABEL	DESCRIPTION
Authentication	
Authentication	Select the authentication method used in the RIP network. This authentication protects the integrity, but not the confidentiality, of routing updates. None uses no authentication. Text uses a plain text password that is sent over the network (not very secure). MD5 uses an MD5 password and authentication ID (most secure).
Text Authentication Key	This field is available if the Authentication is Text. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Redistribute	
Active OSPF	Select this to use RIP to advertise routes that were learned through OSPF.
Metric	Type the cost for routes provided by OSPF. The metric represents the "cost" of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used.
Active Static Route	Select this to use RIP to advertise routes that were learned through the static route configuration.

Table 96 Configuration > Network > Routing Protocol > RIP (continued)

LABEL	DESCRIPTION
Metric	Type the cost for routes provided by the static route configuration. The metric represents the "cost" of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used.
Apply	Click this button to save your changes to the USG.
Reset	Click this button to return the screen to its last-saved settings.

10.7 The OSPF Screen

OSPF (Open Shortest Path First, RFC 2328) is a link-state protocol designed to distribute routing information within a group of networks, called an Autonomous System (AS). OSPF offers some advantages over vector-space routing protocols like RIP.

- OSPF supports variable-length subnet masks, which can be set up to use available IP addresses more efficiently.
- OSPF filters and summarizes routing information, which reduces the size of routing tables throughout the network.
- OSPF responds to changes in the network, such as the loss of a router, more quickly.
- OSPF considers several factors, including bandwidth, hop count, throughput, round trip time, and reliability, when it calculates the shortest path.
- OSPF converges more quickly than RIP.

Naturally, OSPF is also more complicated than RIP, so OSPF is usually more suitable for large networks.

OSPF uses IP protocol 89.

OSPF Areas

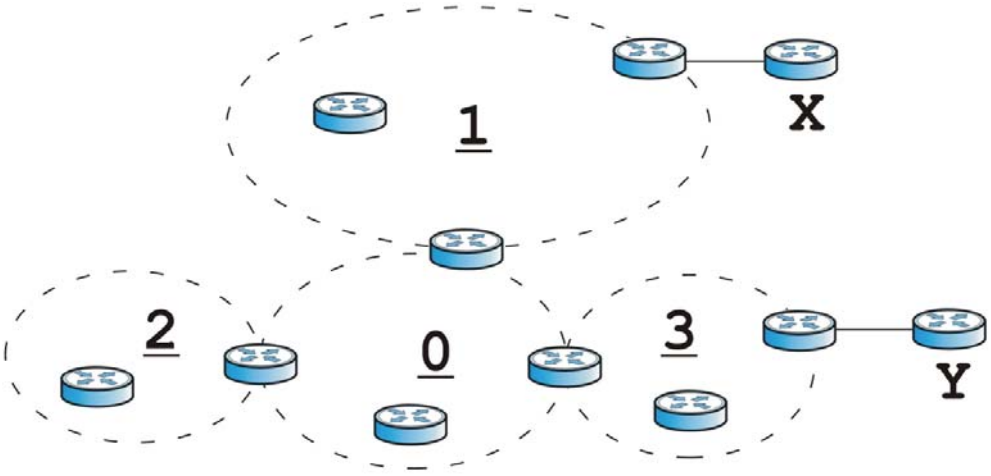
An OSPF Autonomous System (AS) is divided into one or more areas. Each area represents a group of adjacent networks and is identified by a 32-bit ID. In OSPF, this number may be expressed as an integer or as an IP address.

There are several types of areas.

- The backbone is the transit area that routes packets between other areas. All other areas are connected to the backbone.
- A normal area is a group of adjacent networks. A normal area has routing information about the OSPF AS, any networks outside the OSPF AS to which it is directly connected, and any networks outside the OSPF AS that provide routing information to any area in the OSPF AS.
- A stub area has routing information about the OSPF AS. It does not have any routing information about any networks outside the OSPF AS, including networks to which it is directly connected. It relies on a default route to send information outside the OSPF AS.
- A Not So Stubby Area (NSSA, RFC 1587) has routing information about the OSPF AS and networks outside the OSPF AS to which the NSSA is directly connected. It does not have any routing information about other networks outside the OSPF AS.

Each type of area is illustrated in the following figure.

Figure 158 OSPF: Types of Areas



This OSPF AS consists of four areas, areas 0-3. Area 0 is always the backbone. In this example, areas 1, 2, and 3 are all connected to it. Area 1 is a normal area. It has routing information about the OSPF AS and networks X and Y. Area 2 is a stub area. It has routing information about the OSPF AS, but it depends on a default route to send information to networks X and Y. Area 3 is a NSSA. It has routing information about the OSPF AS and network Y but not about network X.

OSPF Routers

Every router in the same area has the same routing information. They do this by exchanging Hello messages to confirm which neighbor (layer-3) devices exist, and then they exchange database descriptions (DDs) to create a synchronized link-state database. The link-state database contains records of router IDs, their associated links and path costs. The link-state database is then constantly updated through Link State Advertisements (LSA). Each router uses the link state database and the Dijkstra algorithm to compute the least cost paths to network destinations.

Like areas, each router has a unique 32-bit ID in the OSPF AS, and there are several types of routers. Each type is really just a different role, and it is possible for one router to play multiple roles at one time.

- An internal router (IR) only exchanges routing information with other routers in the same area.
- An Area Border Router (ABR) connects two or more areas. It is a member of all the areas to which it is connected, and it filters, summarizes, and exchanges routing information between them.
- An Autonomous System Boundary Router (ASBR) exchanges routing information with routers in networks outside the OSPF AS. This is called redistribution in OSPF.

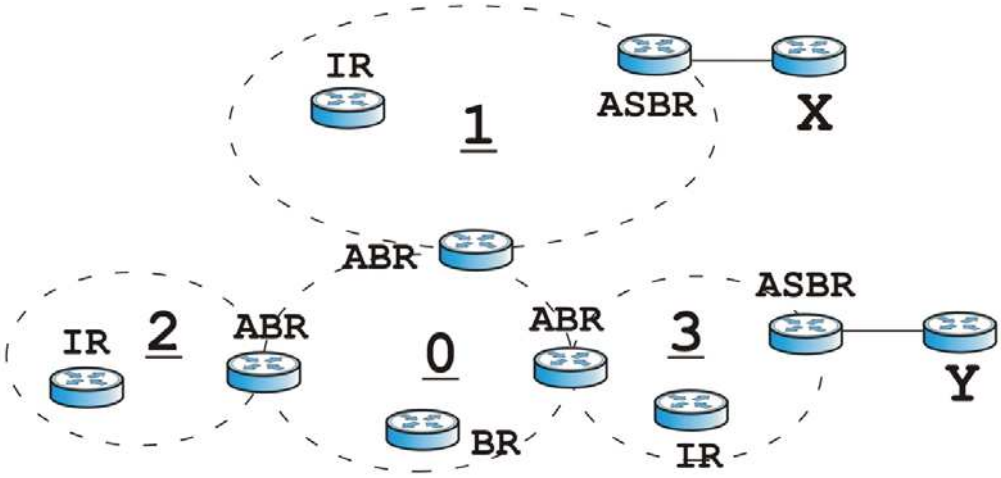
Table 97 OSPF: Redistribution from Other Sources to Each Type of Area

SOURCE \ TYPE OF AREA	NORMAL	NSSA	STUB
Static routes	Yes	Yes	No
RIP	Yes	Yes	Yes

- A backbone router (BR) has at least one interface with area 0. By default, every router in area 0 is a backbone router, and so is every ABR.

Each type of router is illustrated in the following example.

Figure 159 OSPF: Types of Routers



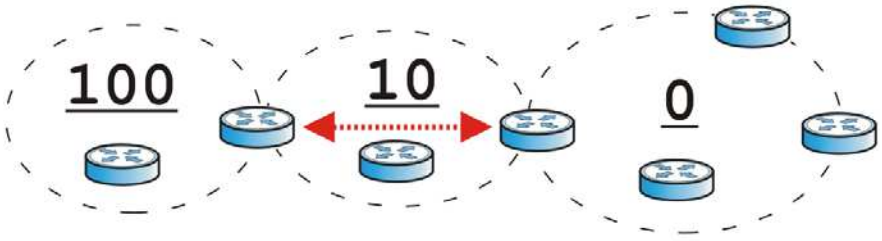
In order to reduce the amount of traffic between routers, a group of routers that are directly connected to each other selects a designated router (DR) and a backup designated router (BDR). All of the routers only exchange information with the DR and the BDR, instead of exchanging information with all of the other routers in the group. The DR and BDR are selected by priority; if two routers have the same priority, the highest router ID is used.

The DR and BDR are selected in each group of routers that are directly connected to each other. If a router is directly connected to several groups, it might be a DR in one group, a BDR in another group, and neither in a third group all at the same time.

Virtual Links

In some OSPF AS, it is not possible for an area to be directly connected to the backbone. In this case, you can create a virtual link through an intermediate area to logically connect the area to the backbone. This is illustrated in the following example.

Figure 160 OSPF: Virtual Link



In this example, area 100 does not have a direct connection to the backbone. As a result, you should set up a virtual link on both ABR in area 10. The virtual link becomes the connection between area 100 and the backbone.

You cannot create a virtual link to a router in a different area.

OSPF Configuration

Follow these steps when you configure OSPF on the USG.

1 Enable OSPF.

2 Set up the OSPF areas.

3 Configure the appropriate interfaces. See Section 9.3.1 on page 149.

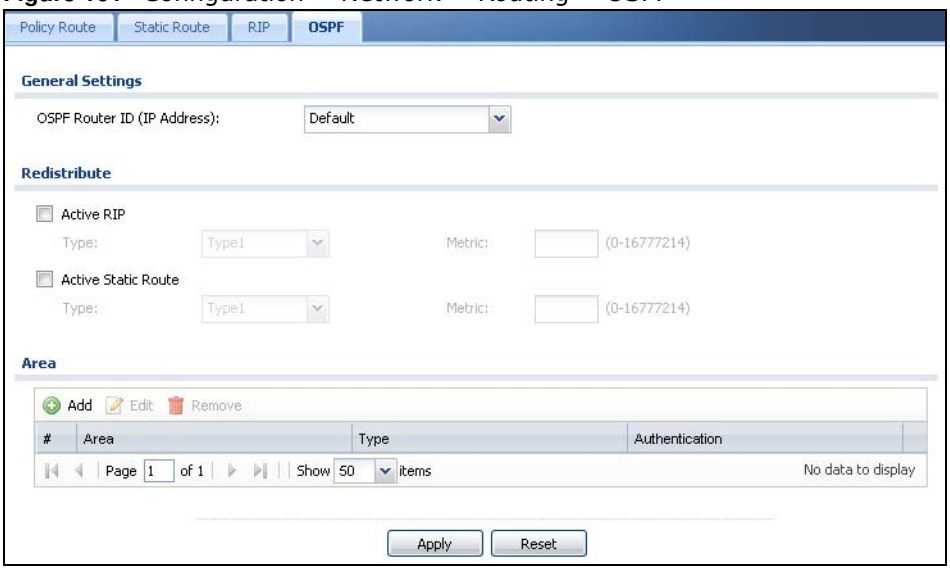
4 Set up virtual links, as needed.

10.7.1 Configuring the OSPF Screen

Use the first OSPF screen to specify the OSPF router the USG uses in the OSPF AS and maintain the policies for redistribution. In addition, it provides a summary of OSPF areas, allows you to remove them, and opens the OSPF Add/ Edit screen to add or edit them.

Click Configuration > Network > Routing > OSPF to open the following screen.

Figure 161 Configuration > Network > Routing > OSPF



The following table describes the labels in this screen. See Section 10.7.2 on page 245 for more information as well.

Table 98 Configuration > Network > Routing Protocol > OSPF

LABEL	DESCRIPTION
OSPF Router ID	Select the 32-bit ID the USG uses in the OSPF AS. Default - the first available interface IP address is the USG's ID. User Defined - enter the ID (in IP address format) in the field that appears when you select User Define.
Redistribute	
Active RIP	Select this to advertise routes that were learned from RIP. The USG advertises routes learned from RIP to Normal and NSSA areas but not to Stub areas.

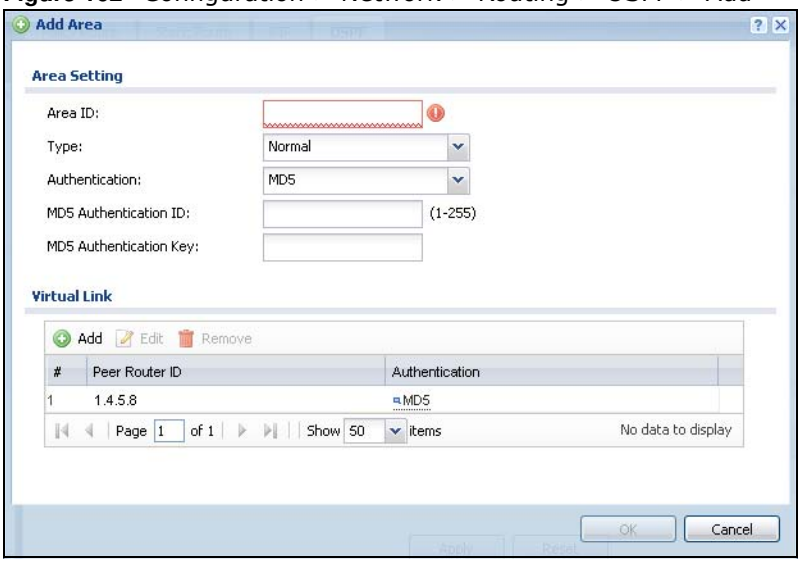
Table 98 Configuration > Network > Routing Protocol > OSPF (continued)

LABEL	DESCRIPTION
Type	Select how OSPF calculates the cost associated with routing information from RIP. Choices are: Type 1 and Type 2. Type 1 - cost = OSPF AS cost + external cost (Metric) Type 2 - cost = external cost (Metric); the OSPF AS cost is ignored.
Metric	Type the external cost for routes provided by RIP. The metric represents the "cost" of transmission for routing purposes. The way this is used depends on the Type field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214.
Active Static Route	Select this to advertise routes that were learned from static routes. The USG advertises routes learned from static routes to all types of areas.
Type	Select how OSPF calculates the cost associated with routing information from static routes. Choices are: Type 1 and Type 2. Type 1 - cost = OSPF AS cost + external cost (Metric) Type 2 - cost = external cost (Metric); the OSPF AS cost is ignored.
Metric	Type the external cost for routes provided by static routes. The metric represents the "cost" of transmission for routing purposes. The way this is used depends on the Type field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214.
Area	This section displays information about OSPF areas in the USG.
Add	Click this to create a new OSPF area.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
Area	This field displays the 32-bit ID for each area in IP address format.
Type	This field displays the type of area. This type is different from the Type field above.
Authentication	This field displays the default authentication method in the area.
Apply	Click this button to save your changes to the USG.
Reset	Click this button to return the screen to its last-saved settings.

10.7.2 OSPF Area Add/Edit Screen

The OSPF Area Add/ Edit screen allows you to create a new area or edit an existing one. To access this screen, go to the OSPF summary screen (see Section 10.7 on page 241), and click either the Add icon or an Edit icon.

Figure 162 Configuration > Network > Routing > OSPF > Add



The following table describes the labels in this screen.

Table 99 Configuration > Network > Routing > OSPF > Add

LABEL	DESCRIPTION
Area ID	Type the unique, 32-bit identifier for the area in IP address format.
Type	Select the type of OSPF area. Normal - This area is a normal area. It has routing information about the OSPF AS and about networks outside the OSPF AS. Stub - This area is an stub area. It has routing information about the OSPF AS but not about networks outside the OSPF AS. It depends on a default route to send information outside the OSPF AS. NSSA - This area is a Not So Stubby Area (NSSA), per RFC 1587. It has routing information about the OSPF AS and networks that are outside the OSPF AS and are directly connected to the NSSA. It does not have information about other networks outside the OSPF AS.
Authentication	Select the default authentication method used in the area. This authentication protects the integrity, but not the confidentiality, of routing updates. None uses no authentication. Text uses a plain text password that is sent over the network (not very secure). MD5 uses an MD5 password and authentication ID (most secure).
Text Authentication Key	This field is available if the Authentication is Text. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Virtual Link	This section is displayed if the Type is Normal. Create a virtual link if you want to connect a different area (that does not have a direct connection to the backbone) to the backbone. You should set up the virtual link on the ABR that is connected to the other area and on the ABR that is connected to the backbone.
Add	Click this to create a new virtual link.

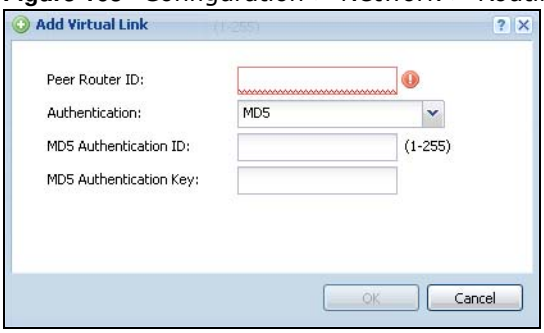
Table 99 Configuration > Network > Routing > OSPF > Add (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
Peer Router ID	This is the 32-bit ID (in IP address format) of the other ABR in the virtual link.
Authentication	This is the authentication method the virtual link uses. This authentication protects the integrity, but not the confidentiality, of routing updates. None uses no authentication. Text uses a plain text password that is sent over the network (not very secure). Hover your cursor over this label to display the password. MD5 uses an MD5 password and authentication ID (most secure). Hover your cursor over this label to display the authentication ID and key. Same as Area has the virtual link also use the Authentication settings above.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

10.7.3 Virtual Link Add/Edit Screen

The Virtual Link Add/ Edit screen allows you to create a new virtual link or edit an existing one. When the OSPF add or edit screen (see Section 10.7.2 on page 245) has the Type set to Normal, a Virtual Link table displays. Click either the Add icon or an entry and the Edit icon to display a screen like the following.

Figure 163 Configuration > Network > Routing > OSPF > Add > Add



The following table describes the labels in this screen.

Table 100 Configuration > Network > Routing > OSPF > Add > Add

LABEL	DESCRIPTION
Peer Router ID	Enter the 32-bit ID (in IP address format) of the other ABR in the virtual link.
Authentication	Select the authentication method the virtual link uses. This authentication protects the integrity, but not the confidentiality, of routing updates. None uses no authentication. Text uses a plain text password that is sent over the network (not very secure). MD5 uses an MD5 password and authentication ID (most secure). Same as Area has the virtual link also use the Authentication settings above.
Text Authentication Key	This field is available if the Authentication is Text. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

10.8 Routing Protocol Technical Reference

Here is more detailed information about RIP and OSPF.

Authentication Types

Authentication is used to guarantee the integrity, but not the confidentiality, of routing updates. The transmitting router uses its key to encrypt the original message into a smaller message, and the smaller message is transmitted with the original message. The receiving router uses its key to encrypt the received message and then verifies that it matches the smaller message sent with it. If the received message is verified, then the receiving router accepts the updated routing information. The transmitting and receiving routers must have the same key.

The USG supports three types of authentication for RIP and OSPF routing protocols:

- None - no authentication is used.
- Text – authentication using a plain text password, and the (unencrypted) password is sent over the network. This method is usually used temporarily to prevent network problems.
- MD5 – authentication using an MD5 password and authentication ID.

MD5 is an authentication method that produces a 128-bit checksum, called a message-digest, for each packet. It also includes an authentication ID, which can be set to any value between 1 and 255. The USG only accepts packets if these conditions are satisfied.

- The packet's authentication ID is the same as the authentication ID of the interface that received it.

- The packet's message-digest is the same as the one the USG calculates using the MD5 password.

For RIP, authentication is not available in RIP version 1. In RIP version 2, you can only select one authentication type for all interfaces. For OSPF, the USG supports a default authentication type by area. If you want to use this default in an interface or virtual link, you set the associated Authentication Type field to Same as Area. As a result, you only have to update the authentication information for the area to update the authentication type used by these interfaces and virtual links. Alternatively, you can override the default in any interface or virtual link by selecting a specific authentication method. Please see the respective interface sections for more information.

11

DDNS

11.1 DDNS Overview

Dynamic DNS (DDNS) services let you use a domain name with a dynamic IP address.

11.1.1 What You Can Do in this Chapter

- Use the DDNS screen (see Section 11.2 on page 251) to view a list of the configured DDNS domain names and their details.
- Use the DDNS Add/ Edit screen (see Section 11.2.1 on page 252) to add a domain name to the USG or to edit the configuration of an existing domain name.

11.1.2 What You Need to Know

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, Dynamic DNS (DDNS) maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current (dynamic) IP address.

Note: You must have a public WAN IP address to use Dynamic DNS.

You must set up a dynamic DNS account with a supported DNS service provider before you can use Dynamic DNS services with the USG. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the USG supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

Table 101 DDNS Service Providers

PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE
DynDNS	Dynamic DNS, Static DNS, and Custom DNS	www.dyndns.com
Dynu	Basic, Premium	www.dynu.com
No-IP	No-IP	www.no-ip.com
Peanut Hull	Peanut Hull	www.oray.cn
3322	3322 Dynamic DNS, 3322 Static DNS	www.3322.org
Selfhost	Selfhost	selfhost.de

Note: Record your DDNS account's user name, password, and domain name to use to configure the USG.

After you configure the USG, it automatically sends updated IP addresses to the DDNS service provider, which helps redirect traffic accordingly.

11.2 The DDNS Screen

The DDNS screen provides a summary of all DDNS domain names and their configuration. In addition, this screen allows you to add new domain names, edit the configuration for existing domain names, and delete domain names. Click Configuration > Network > DDNS to open the following screen.

Figure 164 Configuration > Network > DDNS



The following table describes the labels in this screen.

Table 102 Configuration > Network > DDNS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This is the number of an individual DDNS profile.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field displays the descriptive profile name for this entry.
DDNS Type	This field displays which DDNS service you are using.
Domain Name	This field displays each domain name the USG can route.
Primary Interface/IP	This field displays the interface to use for updating the IP address mapped to the domain name followed by how the USG determines the IP address for the domain name. from interface - The IP address comes from the specified interface. auto detected -The DDNS server checks the source IP address of the packets from the USG for the IP address to use for the domain name. custom - The IP address is static.
Backup Interface/IP	This field displays the alternate interface to use for updating the IP address mapped to the domain name followed by how the USG determines the IP address for the domain name. The USG uses the backup interface and IP address when the primary interface is disabled, its link is down or its connectivity check fails. from interface - The IP address comes from the specified interface. auto detected -The DDNS server checks the source IP address of the packets from the USG for the IP address to use for the domain name. custom - The IP address is static.

Table 102 Configuration > Network > DDNS (continued)

LABEL	DESCRIPTION
Apply	Click this button to save your changes to the USG.
Reset	Click this button to return the screen to its last-saved settings.

11.2.1 The Dynamic DNS Add/Edit Screen

The DDNS Add/ Edit screen allows you to add a domain name to the USG or to edit the configuration of an existing domain name. Click Configuration > Network > DDNS and then an Add or Edit icon to open this screen.

Figure 165 Configuration > Network > DDNS > Add

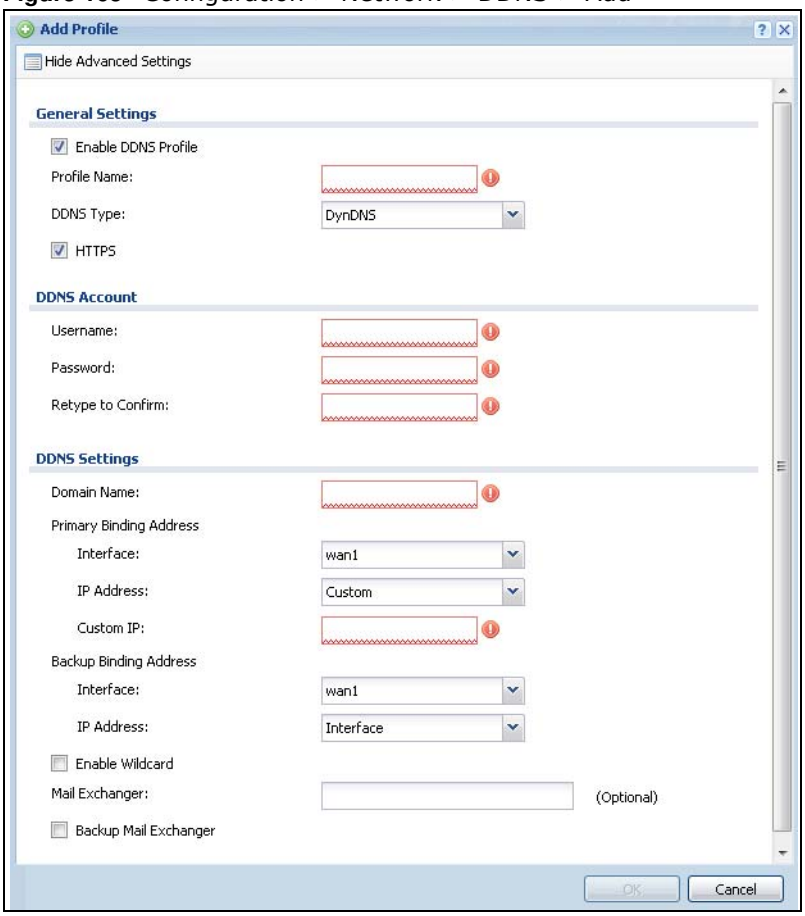
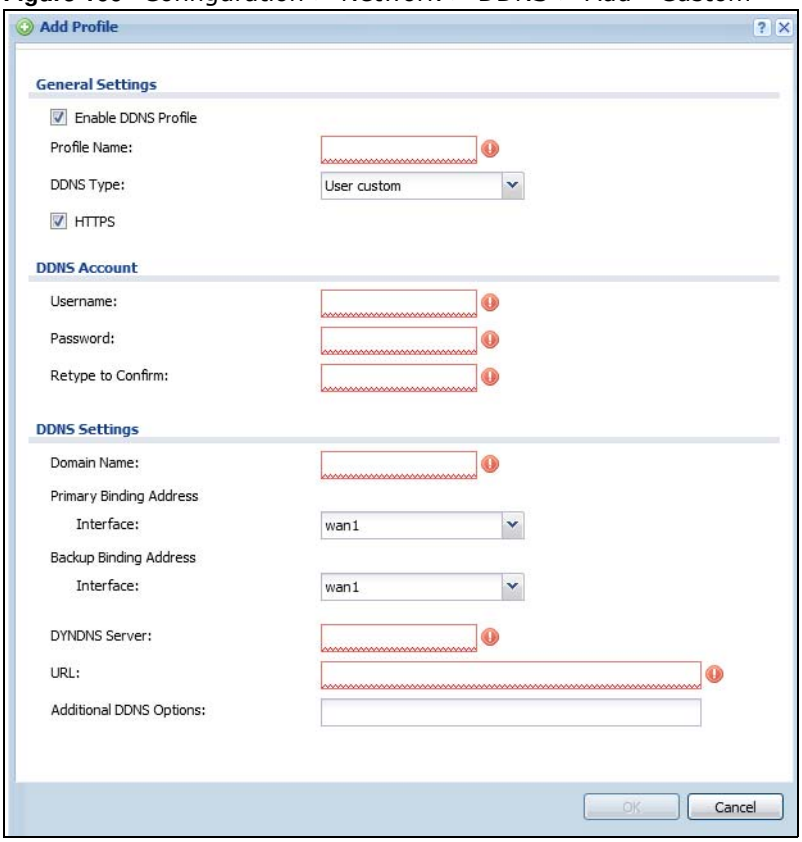


Figure 166 Configuration > Network > DDNS > Add - Custom



The following table describes the labels in this screen.

Table 103 Configuration > Network > DDNS > Add

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable DDNS Profile	Select this check box to use this DDNS entry.
Profile Name	When you are adding a DDNS entry, type a descriptive name for this DDNS entry in the USG. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is read-only when you are editing an entry.
DDNS Type	Select the type of DDNS service you are using. Select User custom to create your own DDNS service and configure the DYNDNS Server, URL, and Additional DDNS Options fields below.
HTTPS	Select this to encrypt traffic using SSL (port 443), including traffic with username and password, to the DDNS server. Not all DDNS providers support this option.
Username	Type the user name used when you registered your domain name. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed. For a Dynu DDNS entry, this user name is the one you use for logging into the service, not the name recorded in your personal information in the Dynu website.
Password	Type the password provided by the DDNS provider. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed.
Retype to Confirm	Type the password again to confirm it.

Table 103 Configuration > Network > DDNS > Add (continued)

LABEL	DESCRIPTION
DDNS Settings	
Domain name	Type the domain name you registered. You can use up to 255 characters.
Primary Binding Address	Use these fields to set how the USG determines the IP address that is mapped to your domain name in the DDNS server. The USG uses the Backup Binding Address if the interface specified by these settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select Any to let the domain name be used with any interface.
IP Address	The options available in this field vary by DDNS provider. Interface -The USG uses the IP address of the specified interface. This option appears when you select a specific interface in the Primary Binding Address Interface field. Auto - If the interface has a dynamic IP address, the DDNS server checks the source IP address of the packets from the USG for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the USG and the DDNS server. Note: The USG may not determine the proper IP address if there is an HTTP proxy server between the USG and the DDNS server. Custom - If you have a static IP address, you can select this to use it for the domain name. The USG still sends the static IP address to the DDNS server.
Custom IP	This field is only available when the IP Address is Custom. Type the IP address to use for the domain name.
Backup Binding Address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the Primary Binding Interface settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select Any to let the domain name be used with any interface. Select None to not use a backup address.
IP Address	The options available in this field vary by DDNS provider. Interface -The USG uses the IP address of the specified interface. This option appears when you select a specific interface in the Backup Binding Address Interface field. Auto -The DDNS server checks the source IP address of the packets from the USG for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the USG and the DDNS server. Note: The USG may not determine the proper IP address if there is an HTTP proxy server between the USG and the DDNS server. Custom - If you have a static IP address, you can select this to use it for the domain name. The USG still sends the static IP address to the DDNS server.
Custom IP	This field is only available when the IP Address is Custom. Type the IP address to use for the domain name.
Enable Wildcard	This option is only available with a DynDNS account. Enable the wildcard feature to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Table 103 Configuration > Network > DDNS > Add (continued)

LABEL	DESCRIPTION
Mail Exchanger	This option is only available with a DynDNS account. DynDNS can route e-mail for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes e-mail for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger. If you are using this service, type the host record of your mail server here. Otherwise leave the field blank. See www.dyndns.org for more information about mail exchangers.
Backup Mail Exchanger	This option is only available with a DynDNS account. Select this check box if you are using DynDNS's backup service for e-mail. With this service, DynDNS holds onto your e-mail if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. See www.dyndns.org for more information about this service.
DYNDNS Server	This field displays when you select User custom from the DDNS Type field above. Type the IP address of the server that will host the DDSN service.
URL	This field displays when you select User custom from the DDNS Type field above. Type the URL that can be used to access the server that will host the DDSN service.
Additional DDNS Options	This field displays when you select User custom from the DDNS Type field above. These are the options supported at the time of writing: • dyndns_system to specify the DYNDNS Server type - for example, dyndns@dyndns.org • ip_server_name which should be the URL to get the server's public IP address - for example, http://myip.easylife.tw/
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

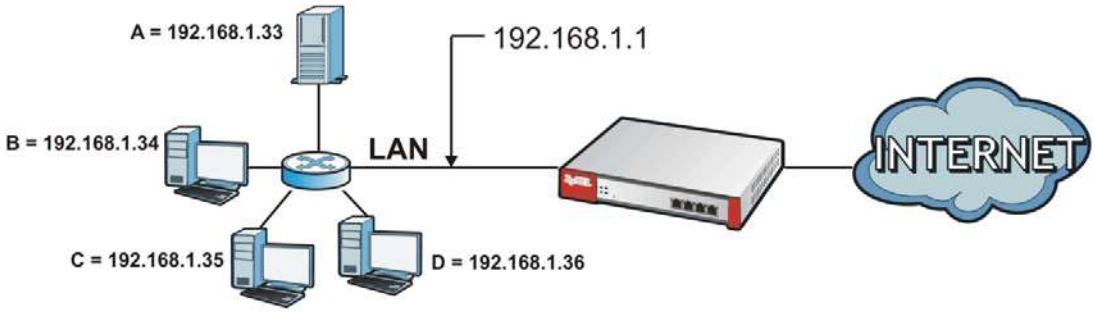
12 NAT

12.1 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. Use Network Address Translation (NAT) to make computers on a private network behind the USG available outside the private network. If the USG has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 167 Multiple Servers Behind NAT Example



12.1.1 What You Can Do in this Chapter

Use the NAT screens (see Section 12.2 on page 256) to view and manage the list of NAT rules and see their configuration details. You can also create new NAT rules and edit or delete existing ones.

12.1.2 What You Need to Know

NAT is also known as virtual server, port forwarding, or port translation.

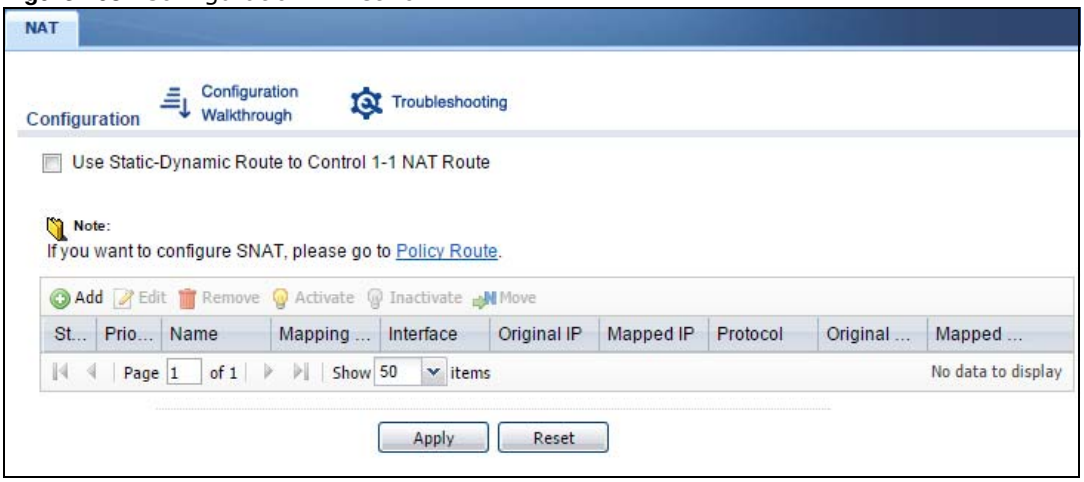
12.2 The NAT Screen

The NAT summary screen provides a summary of all NAT rules and their configuration. In addition, this screen allows you to create new NAT rules and edit and delete existing NAT rules. To access this

screen, login to the Web Configurator and click Configuration > Network > NAT. The following screen appears, providing a summary of the existing NAT rules.

Click on the icons to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting, and other information.

Figure 168 Configuration > Network > NAT



The following table describes the labels in this screen.

Table 104 Configuration > Network > NAT

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the entry.
Mapping Type	This field displays what kind of NAT this entry performs: Virtual Server, 1:1 NAT, or Many 1:1 NAT.
Interface	This field displays the interface on which packets for the NAT entry are received.
Original IP	This field displays the original destination IP address (or address object) of traffic that matches this NAT entry. It displays any if there is no restriction on the original destination IP address.
Mapped IP	This field displays the new destination IP address for the packet.
Protocol	This field displays the service used by the packets for this NAT entry. It displays any if there is no restriction on the services.
Original Port	This field displays the original destination port(s) of packets for the NAT entry. This field is blank if there is no restriction on the original destination port.
Mapped Port	This field displays the new destination port(s) for the packet. This field is blank if there is no restriction on the original destination port.

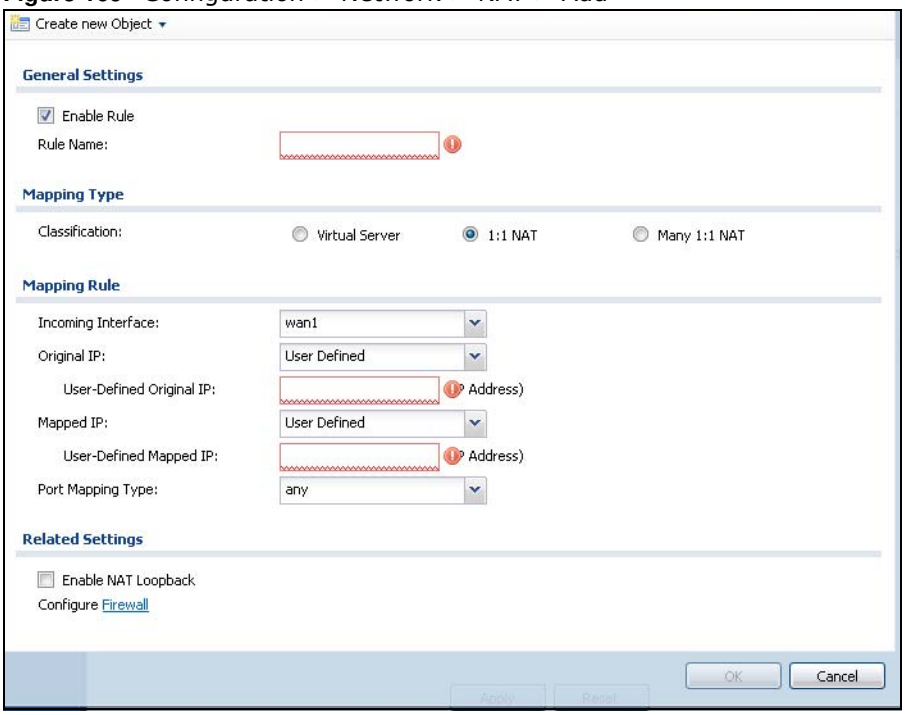
Table 104 Configuration > Network > NAT (continued)

LABEL	DESCRIPTION
Apply	Click this button to save your changes to the USG.
Reset	Click this button to return the screen to its last-saved settings.

12.2.1 The NAT Add/Edit Screen

The NAT Add/ Edit screen lets you create new NAT rules and edit existing ones. To open this window, open the NAT summary screen. (See Section 12.2 on page 256.) Then, click on an Add icon or Edit icon to open the following screen.

Figure 169 Configuration > Network > NAT > Add



The following table describes the labels in this screen.

Table 105 Configuration > Network > NAT > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Rule	Use this option to turn the NAT rule on or off.
Rule Name	Type in the name of the NAT rule. The name is used to refer to the NAT rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Table 105 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Classification	Select what kind of NAT this rule is to perform. Virtual Server - This makes computers on a private network behind the USG available to a public network outside the USG (like the Internet). 1:1 NAT - If the private network server will initiate sessions to the outside clients, select this to have the USG translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server. Many 1:1 NAT - If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, select this to have the USG translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses. One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases configuration effort since you only create one rule.
Incoming Interface	Select the interface on which packets for the NAT rule must be received. It can be an Ethernet, VLAN, bridge, or PPPoE/PPTP interface.
Original IP	Specify the destination IP address of the packets received by this NAT rule's specified incoming interface. any - Select this to use all of the incoming interface's IP addresses including dynamic addresses or those of any virtual interfaces built upon the selected incoming interface. User Defined - Select this to manually enter an IP address in the User Defined field. For example, you could enter a static public IP assigned by the ISP without having to create a virtual interface for it. Host address - select a host address object to use the IP address it specifies. The list also includes address objects based on interface IPs. So for example you could select an address object based on a WAN interface even if it has a dynamic IP address.
User Defined Original IP	This field is available if Original IP is User Defined. Type the destination IP address that this NAT rule supports.
Original IP Subnet/ Range	This field displays for Many 1:1 NAT. Select the destination IP address subnet or IP address range that this NAT rule supports. The original and mapped IP address subnets or ranges must have the same number of IP addresses.
Mapped IP	Select to which translated destination IP address this NAT rule forwards packets. User Defined - this NAT rule supports a specific IP address, specified in the User Defined field. HOST address - the drop-down box lists all the HOST address objects in the USG. If you select one of them, this NAT rule supports the IP address specified by the address object.
User Defined Original IP	This field is available if Mapped IP is User Defined. Type the translated destination IP address that this NAT rule supports.
Mapped IP Subnet/ Range	This field displays for Many 1:1 NAT. Select to which translated destination IP address subnet or IP address range this NAT rule forwards packets. The original and mapped IP address subnets or ranges must have the same number of IP addresses.

Table 105 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Port Mapping Type	Use the drop-down list box to select how many original destination ports this NAT rule supports for the selected destination IP address (Original IP). Choices are: Any - this NAT rule supports all the destination ports. Port - this NAT rule supports one destination port. Ports - this NAT rule supports a range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service. Service - this NAT rule supports a service such as FTP (see Object > Service > Service) Service-Group - this NAT rule supports a group of services such as all service objects related to DNS (see Object > Service > Service Group)
Protocol Type	This field is available if Mapping Type is Port or Ports. Select the protocol (TCP, UDP, or Any) used by the service requesting the connection.
Original Port	This field is available if Mapping Type is Port. Enter the original destination port this NAT rule supports.
Mapped Port	This field is available if Mapping Type is Port. Enter the translated destination port if this NAT rule forwards the packet.
Original Start Port	This field is available if Mapping Type is Ports. Enter the beginning of the range of original destination ports this NAT rule supports.
Original End Port	This field is available if Mapping Type is Ports. Enter the end of the range of original destination ports this NAT rule supports.
Mapped Start Port	This field is available if Mapping Type is Ports. Enter the beginning of the range of translated destination ports if this NAT rule forwards the packet.
Mapped End Port	This field is available if Mapping Type is Ports. Enter the end of the range of translated destination ports if this NAT rule forwards the packet. The original port range and the mapped port range must be the same size.
Enable NAT Loopback	Enable NAT loopback to allow users connected to any interface (instead of just the specified Incoming Interface) to use the NAT rule's specified Original IP address to access the Mapped IP device. For users connected to the same interface as the Mapped IP device, the USG uses that interface's IP address as the source address for the traffic it sends from the users to the Mapped IP device. For example, if you configure a NAT rule to forward traffic from the WAN to a LAN server, enabling NAT loopback allows users connected to other interfaces to also access the server. For LAN users, the USG uses the LAN interface's IP address as the source address for the traffic it sends to the LAN server. See NAT Loopback on page 261 for more details. If you do not enable NAT loopback, this NAT rule only applies to packets received on the rule's specified incoming interface.
Security Policy	By default the security policy blocks incoming connections from external addresses. After you configure your NAT rule settings, click the Security Policy link to configure a security policy to allow the NAT rule's traffic to come in. The USG checks NAT rules before it applies To-USG security policies, so To-USG security policies, do not apply to traffic that is forwarded by NAT rules. The USG still checks other security policies, according to the source IP address and mapped IP address.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to return to the NAT summary screen without creating the NAT rule (if it is new) or saving any changes (if it already exists).

12.3 NAT Technical Reference

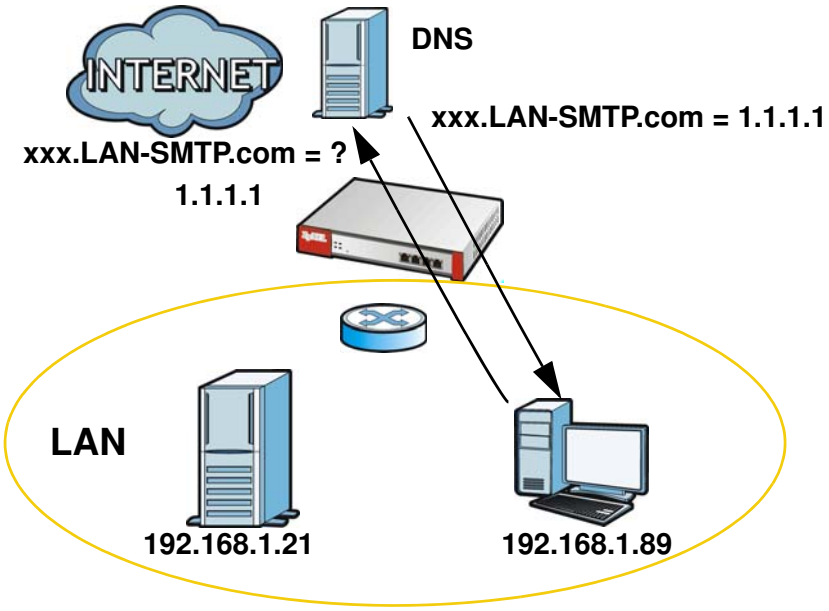
Here is more detailed information about NAT on the USG.

NAT Loopback

Suppose an NAT 1:1 rule maps a public IP address to the private IP address of a LAN SMTP e-mail server to give WAN users access. NAT loopback allows other users to also use the rule's original IP to access the mail server.

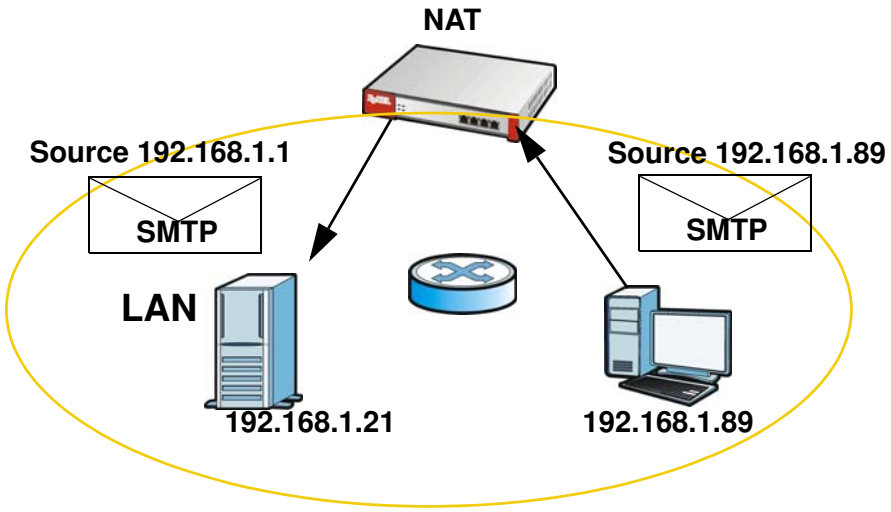
For example, a LAN user's computer at IP address 192.168.1.89 queries a public DNS server to resolve the SMTP server's domain name (xxx.LAN-SMTP.com in this example) and gets the SMTP server's mapped public IP address of 1.1.1.1.

Figure 170 LAN Computer Queries a Public DNS Server



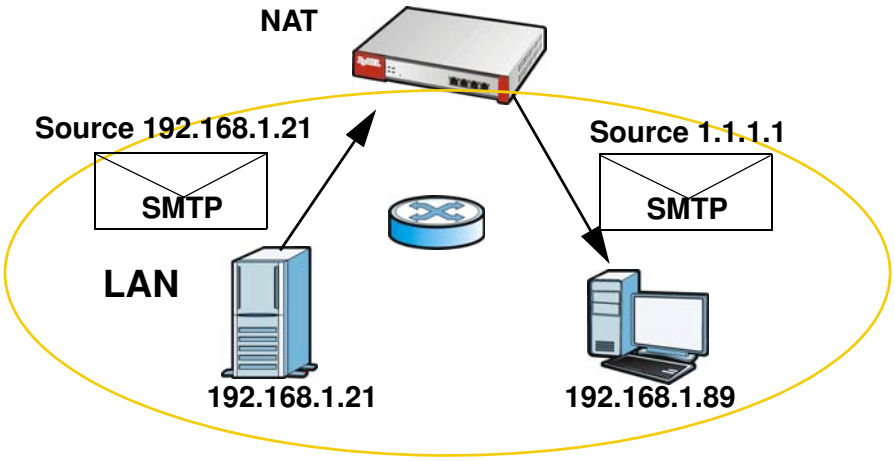
The LAN user's computer then sends traffic to IP address 1.1.1.1. NAT loopback uses the IP address of the USG's LAN interface (192.168.1.1) as the source address of the traffic going from the LAN users to the LAN SMTP server.

Figure 171 LAN to LAN Traffic



The LAN SMTP server replies to the USG's LAN IP address and the USG changes the source address to 1.1.1.1 before sending it to the LAN user. The return traffic's source matches the original destination address (1.1.1.1). If the SMTP server replied directly to the LAN user without the traffic going through NAT, the source would not match the original destination address which would cause the LAN user's computer to shut down the session.

Figure 172 LAN to LAN Return Traffic

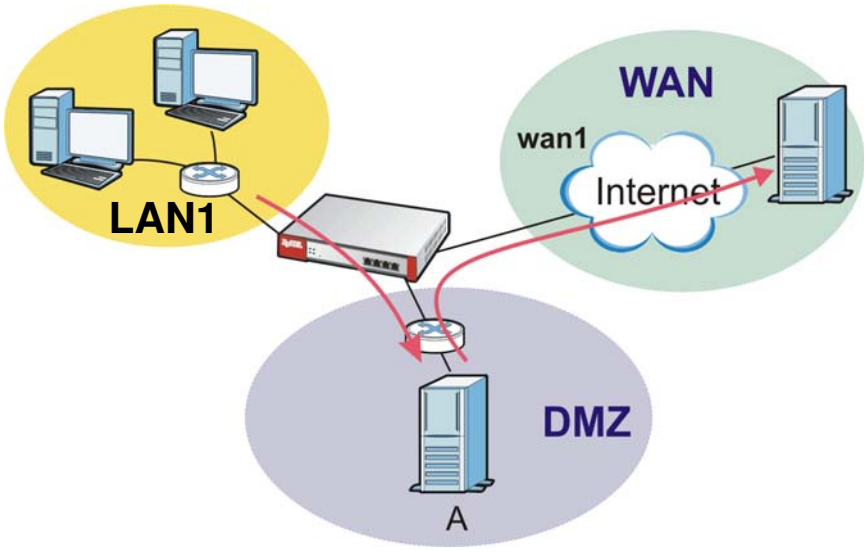


13 HTTP Redirect

13.1 Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the USG) to a web proxy server. In the following example, proxy server A is connected to the DMZ interface. When a client connected to the LAN1 zone wants to open a web page, its HTTP request is redirected to proxy server A first. If proxy server A cannot find the web page in its cache, a policy route allows it to access the Internet to get them from a server. Proxy server A then forwards the response to the client.

Figure 173 HTTP Redirect Example



13.1.1 What You Can Do in this Chapter

Use the HTTP Redirect screens (see Section 13.2 on page 264) to display and edit the HTTP redirect rules.

13.1.2 What You Need to Know

Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a security policy or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

A client connects to a web proxy server each time he/she wants to access the Internet. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

HTTP Redirect, Security Policy and Policy Route

With HTTP redirect, the relevant packet flow for HTTP traffic is:

1. Security Policy
2. HTTP Redirect
3. Policy Route

Even if you set a policy route to the same incoming interface and service as a HTTP redirect rule, the USG checks the HTTP redirect rules first and forwards HTTP traffic to a proxy server if matched. You need to make sure there is no security policy(s) blocking the HTTP requests from the client to the proxy server.

You also need to manually configure a policy route to forward the HTTP traffic from the proxy server to the Internet. To make the example in Figure 173 on page 263 work, make sure you have the following settings.

For HTTP traffic between lan1 and dmz:

- a from LAN1 to DMZ security policy (default) to allow HTTP requests from lan1 to dmz. Responses to this request are allowed automatically.
- a HTTP redirect rule to forward HTTP traffic from lan1 to proxy server A.

For HTTP traffic between dmz and wan1:

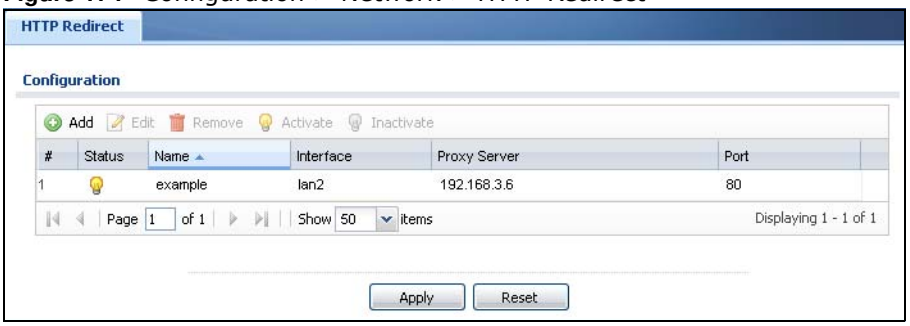
- a from DMZ to WAN security policy (default) to allow HTTP requests from dmz to wan1. Responses to these requests are allowed automatically.
- a policy route to forward HTTP traffic from proxy server A to the Internet.

13.2 The HTTP Redirect Screen

To configure redirection of a HTTP request to a proxy server, click Configuration > Network > HTTP Redirect. This screen displays the summary of the HTTP redirect rules.

Note: You can configure up to one HTTP redirect rule for each (incoming) interface.

Figure 174 Configuration > Network > HTTP Redirect



The following table describes the labels in this screen.

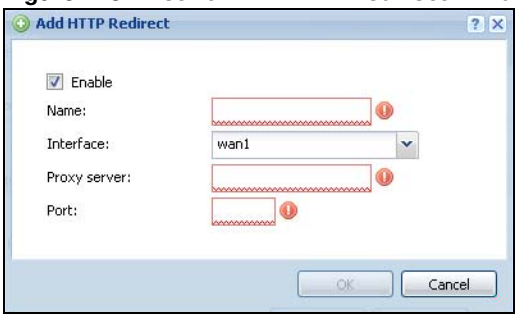
Table 106 Configuration > Network > HTTP Redirect

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the descriptive name of a rule.
Interface	This is the interface on which the request must be received.
Proxy Server	This is the IP address of the proxy server.
Port	This is the service port number used by the proxy server.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

13.2.1 The HTTP Redirect Edit Screen

Click Network > HTTP Redirect to open the HTTP Redirect screen. Then click the Add or Edit icon to open the HTTP Redirect Edit screen where you can configure the rule.

Figure 175 Network > HTTP Redirect > Edit



The following table describes the labels in this screen.

Table 107 Network > HTTP Redirect > Edit

LABEL	DESCRIPTION
Enable	Use this option to turn the HTTP redirect rule on or off.
Name	Enter a name to identify this rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Interface	Select the interface on which the HTTP request must be received for the USG to forward it to the specified proxy server.
Proxy Server	Enter the IP address of the proxy server.
Port	Enter the port number that the proxy server uses.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

14 ALG

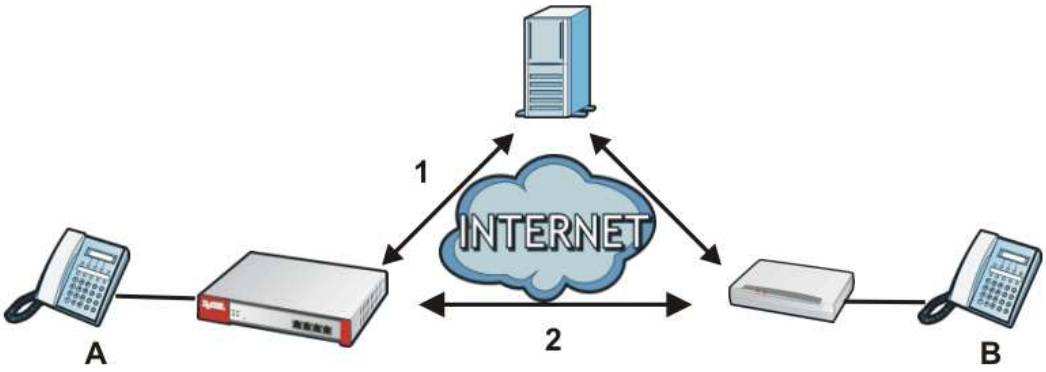
14.1 ALG Overview

Application Layer Gateway (ALG) allows the following applications to operate properly through the USG's NAT.

- SIP - Session Initiation Protocol (SIP) - An application-layer protocol that can be used to create voice and multimedia sessions over Internet.
- H.323 - A teleconferencing protocol suite that provides audio, data and video conferencing.
- FTP - File Transfer Protocol - an Internet file transfer service.

The following example shows SIP signaling (1) and audio (2) sessions between SIP clients A and B and the SIP server.

Figure 176 SIP ALG Example



The ALG feature is only needed for traffic that goes through the USG's NAT.

14.1.1 What You Need to Know

Application Layer Gateway (ALG), NAT and Security Policy

The USG can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the USG's NAT and security policy. The USG dynamically creates an implicit NAT session and security policy session for the application's traffic from the WAN to the LAN. The ALG on the USG supports all of the USG's NAT mapping types.

FTP ALG

The FTP ALG allows TCP packets with a specified port destination to pass through. If the FTP server is located on the LAN, you must also configure NAT (port forwarding) and security policies if you

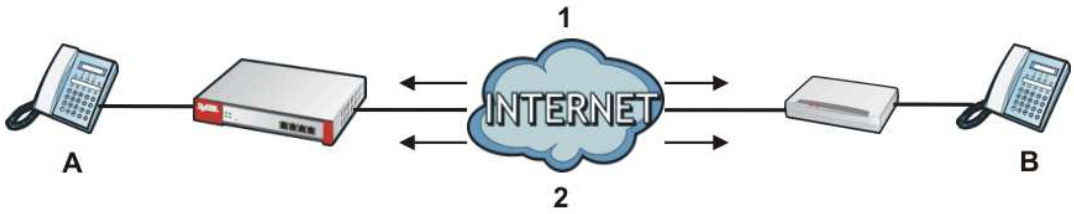
want to allow access to the server from the WAN. Bandwidth management can be applied to FTP ALG traffic.

H.323 ALG

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the USG routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- The H.323 ALG operates on TCP packets with a specified port destination.
- Bandwidth management can be applied to H.323 ALG traffic.
- The USG allows H.323 audio connections.
- The USG can also apply bandwidth management to traffic that goes through the H.323 ALG.

The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

Figure 177 H.323 ALG Example



SIP ALG

- SIP phones can be in any zone (including LAN, DMZ, WAN), and the SIP server and SIP clients can be in the same network or different networks. The SIP server cannot be on the LAN. It must be on the WAN or the DMZ.
- There should be only one SIP server (total) on the USG's private networks. Any other SIP servers must be on the WAN. So for example you could have a Back-to-Back User Agent such as the IPPBX x6004 or an asterisk PBX on the DMZ or on the LAN but not on both.
- Using the SIP ALG allows you to use bandwidth management on SIP traffic. Bandwidth management can be applied to FTP ALG traffic. Use the option in the Configuration > BWM screen to configure the highest bandwidth available for SIP traffic.
- The SIP ALG handles SIP calls that go through NAT or that the USG routes. You can also make other SIP calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The SIP ALG supports peer-to-peer SIP calls. The security policy (by default) allows peer to peer calls from the LAN zone to go to the WAN zone and blocks peer to peer calls from the WAN zone to the LAN zone.
- The SIP ALG allows UDP packets with a specified port destination to pass through.
- The USG allows SIP audio connections.
- You do not need to use TURN (Traversal Using Relay NAT) for VoIP devices behind the USG when you enable the SIP ALG.

Peer-to-Peer Calls and the USG

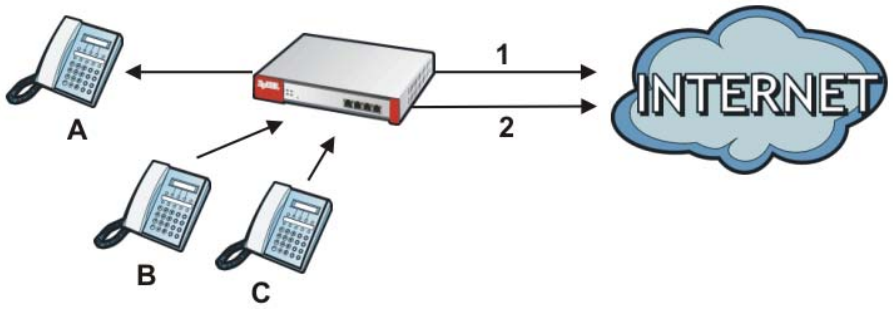
The USG ALG can allow peer-to-peer VoIP calls for both H.323 and SIP. You must configure the security policy and NAT (port forwarding) to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN (or DMZ).

VoIP Calls from the WAN with Multiple Outgoing Calls

When you configure the security policy and NAT (port forwarding) to allow calls from the WAN to a specific IP address on the LAN, you can also use policy routing to have H.323 (or SIP) calls from other LAN or DMZ IP addresses go out through a different WAN IP address. The policy routing lets the USG correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure the security policy and NAT to allow LAN IP address A to receive calls from the Internet through WAN IP address 1. You also use a policy route to have LAN IP address A make calls out through WAN IP address 1. Configure another policy route to have H.323 (or SIP) calls from LAN IP addresses B and C go out through WAN IP address 2. Even though only LAN IP address A can receive incoming calls from the Internet, LAN IP addresses B and C can still make calls out to the Internet.

Figure 178 VoIP Calls from the WAN with Multiple Outgoing Calls

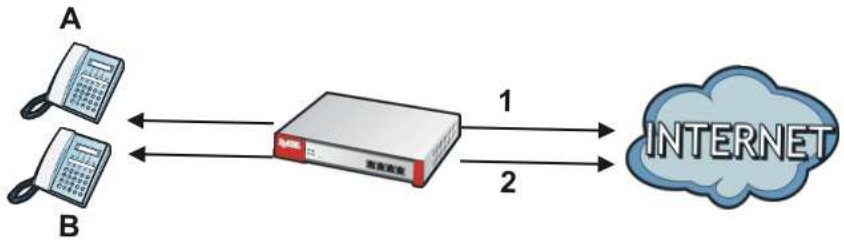


VoIP with Multiple WAN IP Addresses

With multiple WAN IP addresses on the USG, you can configure different security policy and NAT (port forwarding) rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN (or DMZ). Use policy routing to have the H.323 (or SIP) calls from each of those LAN or DMZ IP addresses go out through the same WAN IP address that calls come in on. The policy routing lets the USG correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure security policy and NAT rules to allow LAN IP address A to receive calls through public WAN IP address 1. You configure different security policy and port forwarding rules to allow LAN IP address B to receive calls through public WAN IP address 2. You configure corresponding policy routes to have calls from LAN IP address A go out through WAN IP address **1** and calls from LAN IP address B go out through WAN IP address 2.

Figure 179 VoIP with Multiple WAN IP Addresses



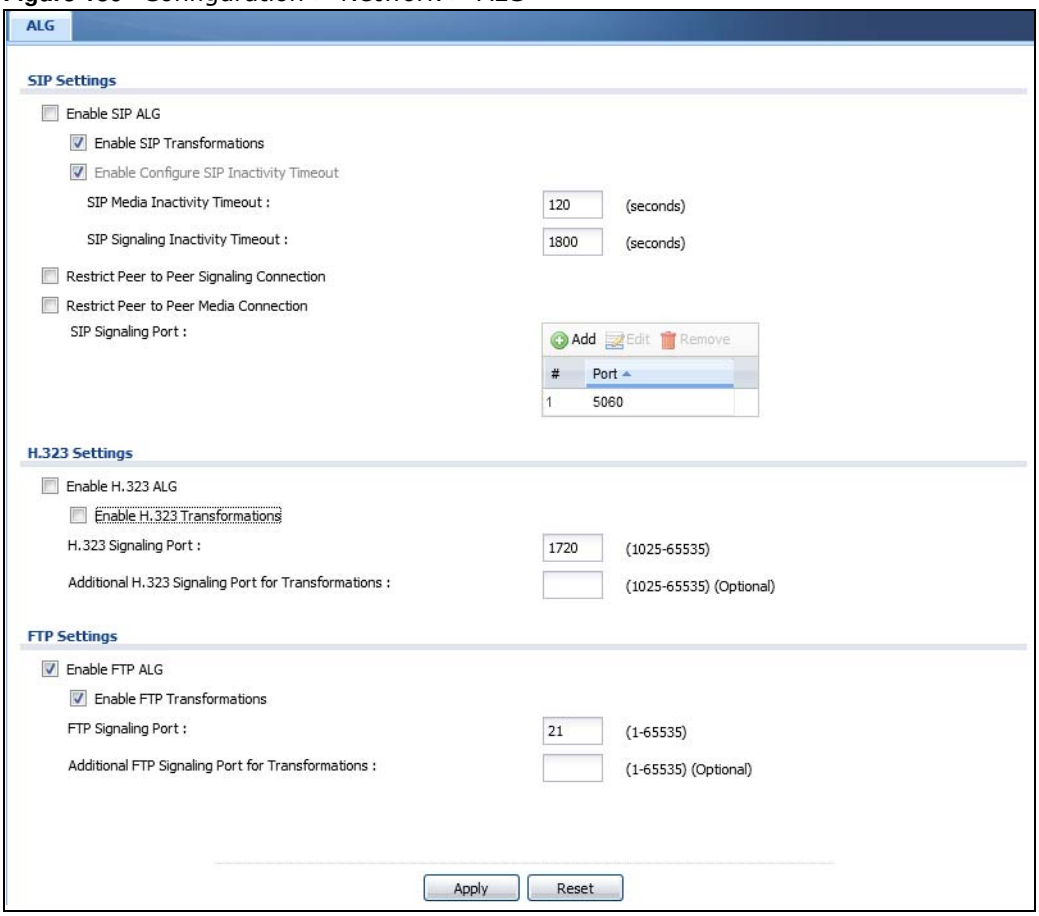
14.1.2 Before You Begin

You must also configure the security policy and enable NAT in the USG to allow sessions initiated from the WAN.

14.2 The ALG Screen

Click Configuration > Network > ALG to open the ALG screen. Use this screen to turn ALGs off or on, configure the port numbers to which they apply, and configure SIP ALG time outs.

Figure 180 Configuration > Network > ALG



The following table describes the labels in this screen.

Table 108 Configuration > Network > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Turn on the SIP ALG to detect SIP traffic and help build SIP sessions through the USG's NAT.
Enable SIP Transformations	Select this to have the USG modify IP addresses and port numbers embedded in the SIP data payload. You do not need to use this if you have a SIP device or server that will modify IP addresses and port numbers embedded in the SIP data payload.
Enable Configure SIP Inactivity Timeout	Select this option to have the USG apply SIP media and signaling inactivity time out limits.
SIP Media Inactivity Timeout	Use this field to set how many seconds (1~86400) the USG will allow a SIP session to remain idle (without voice traffic) before dropping it. If no voice packets go through the SIP ALG before the timeout period expires, the USG deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.
SIP Signaling Inactivity Timeout	Most SIP clients have an "expire" mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the USG. If the SIP client does not have this mechanism and makes no calls during the USG SIP timeout, the USG deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (1~86400).
Restrict Peer to Peer Signaling Connection	A signaling connection is used to set up the SIP connection. Enable this if you want signaling connections to only arrive from the IP address(es) you registered with. Signaling connections from other IP addresses will be dropped.
Restrict Peer to Peer Media Connection	A media connection is the audio transfer in a SIP connection. Enable this if you want media connections to only arrive from the IP address(es) you registered with. Media connections from other IP addresses will be dropped.
SIP Signaling Port	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here. Use the Add icon to add fields if you are also using SIP on additional UDP port numbers.
Additional SIP Signaling Port (UDP) for Transformations	If you are also using SIP on an additional UDP port number, enter it here.
Enable H.323 ALG	Turn on the H.323 ALG to detect H.323 traffic (used for audio communications) and help build H.323 sessions through the USG's NAT.
Enable H.323 Transformations	Select this to have the USG modify IP addresses and port numbers embedded in the H.323 data payload. You do not need to use this if you have a H.323 device or server that will modify IP addresses and port numbers embedded in the H.323 data payload.
H.323 Signaling Port	If you are using a custom TCP port number (not 1720) for H.323 traffic, enter it here.
Additional H.323 Signaling Port for Transformations	If you are also using H.323 on an additional TCP port number, enter it here.
Enable FTP ALG	Turn on the FTP ALG to detect FTP (File Transfer Program) traffic and help build FTP sessions through the USG's NAT.

Table 108 Configuration > Network > ALG (continued)

LABEL	DESCRIPTION
Enable FTP Transformations	Select this option to have the USG modify IP addresses and port numbers embedded in the FTP data payload to match the USG's NAT environment. Clear this option if you have an FTP device or server that will modify IP addresses and port numbers embedded in the FTP data payload to match the USG's NAT environment.
FTP Signaling Port	If you are using a custom TCP port number (not 21) for FTP traffic, enter it here.
Additional FTP Signaling Port for Transformations	If you are also using FTP on an additional TCP port number, enter it here.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

14.3 ALG Technical Reference

Here is more detailed information about the Application Layer Gateway.

ALG

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The USG examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the USG uses an application for which the USG has VoIP pass through enabled, the USG translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the security policy so the application's traffic can come in from the WAN to the LAN.

ALG and Trunks

If you send your ALG-managed traffic through an interface trunk and all of the interfaces are set to active, you can configure routing policies to specify which interface the ALG-managed traffic uses.

You could also have a trunk with one interface set to active and a second interface set to passive. The USG does not automatically change ALG-managed connections to the second (passive) interface when the active interface's connection goes down. When the active interface's connection fails, the client needs to re-initialize the connection through the second interface (that was set to passive) in order to have the connection go through the second interface. VoIP clients usually re-register automatically at set intervals or the users can manually force them to re-register.

FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files.

H.323

H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

RTP

When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

15

UPnP

15.1 UPnP and NAT-PMP Overview

The USG supports both UPnP and NAT-PMP to permit networking devices to discover each other and connect seamlessly.

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. A gateway that supports UPnP is called Internet Gateway Device (IGD). The standardized Device Control Protocol (DCP) is defined by the UPnP Forum for IGDs to configure port mapping automatically.

NAT Port Mapping Protocol (NAT-PMP), introduced by Apple and implemented in current Apple products, is used as an alternative NAT traversal solution to the UPnP IGD protocol. NAT-PMP runs over UDP port 5351. NAT-PMP is much simpler than UPnP IGD and mainly designed for small home networks. It allows a client behind a NAT router to retrieve the router's public IP address and port number and make them known to the peer device with which it wants to communicate. The client can automatically configure the NAT router to create a port mapping to allow the peer to contact it.

15.2 What You Need to Know

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.

15.2.1 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 NAT chapter for more information on NAT.

15.2.2 Cautions with UPnP and NAT-PMP

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

When a UPnP or NAT-PMP device joins a network, it announces its presence with a multicast message. For security reasons, the USG allows multicast messages on the LAN only.

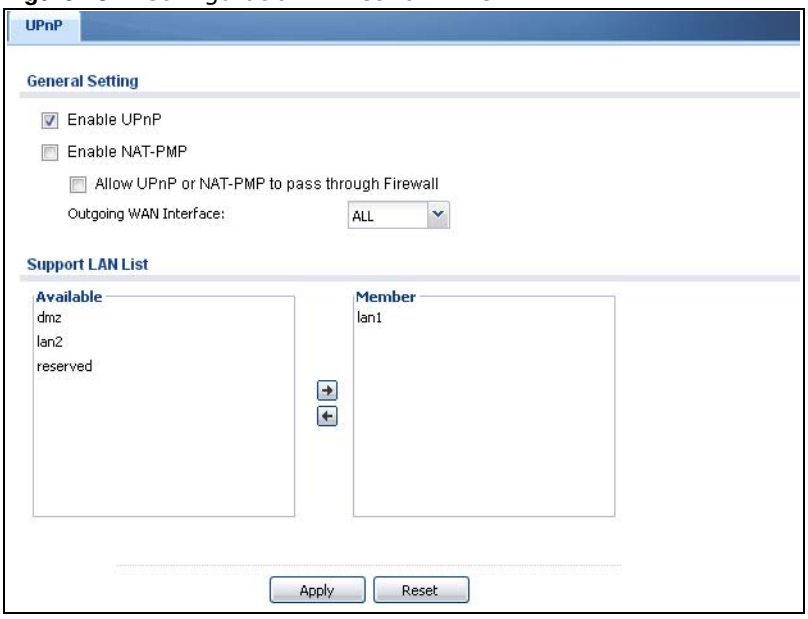
All UPnP-enabled or NAT-PMP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP or NAT-PMP if this is not your intention.

15.3 UPnP Screen

Use this screen to enable UPnP and NAT-PMP on your USG.

Click Configuration > Network > UPnP to display the screen shown next.

Figure 181 Configuration > Network > UPnP



The following table describes the fields in this screen.

Table 109 Configuration > Network > UPnP

LABEL	DESCRIPTION
Enable UPnP	Select this check box to activate UPnP on the USG. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the USG's IP address (although you must still enter the password to access the web configurator).
Enable NAT-PMP	NAT Port Mapping Protocol (NAT-PMP) automates port forwarding to allow a computer in a private network (behind the USG) to automatically configure the USG to allow computers outside the private network to contact it. Select this check box to activate NAT-PMP on the USG. Be aware that anyone could use a NAT-PMP application to open the web configurator's login screen without entering the USG's IP address (although you must still enter the password to access the web configurator).
Allow UPnP or NAT-PMP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled or NAT-PMP-enabled applications to bypass the security policy. Clear this check box to have the security policy block all UPnP or NAT-PMP application packets (for example, MSN packets).
Outgoing WAN Interface	Select through which WAN interface(s) you want to send out traffic from UPnP-enabled or NAT-PMP-enabled applications. If the WAN interface you select loses its connection, the USG attempts to use the other WAN interface. If the other WAN interface also does not work, the USG drops outgoing packets from UPnP-enabled or NAT-PMP-enabled applications.
Support LAN List	The Available list displays the name(s) of the internal interface(s) on which the USG supports UPnP and/or NAT-PMP. To enable UPnP and/or NAT-PMP on an interface, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entriess and click the right arrow button to add to the Member list. To remove an interface, select the name(s) in the Member list and click the left arrow button.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

15.4 Technical Reference

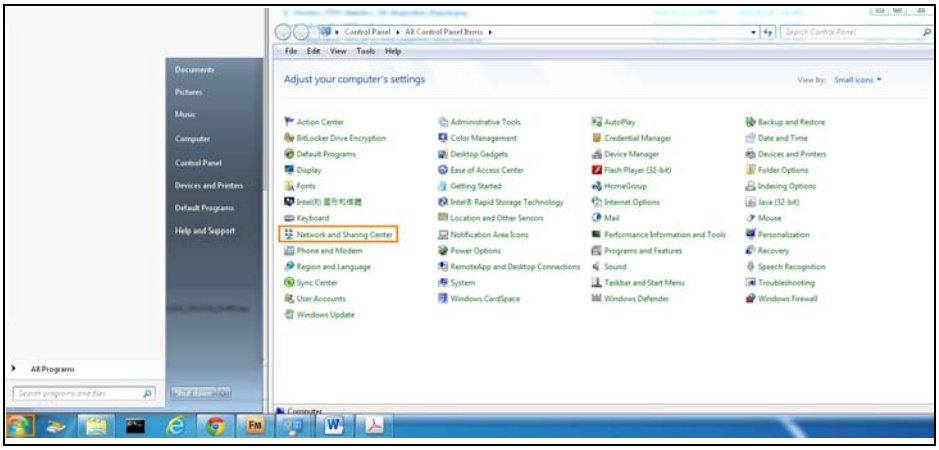
The sections show examples of using UPnP.

15.4.1 Turning on UPnP in Windows 7 Example

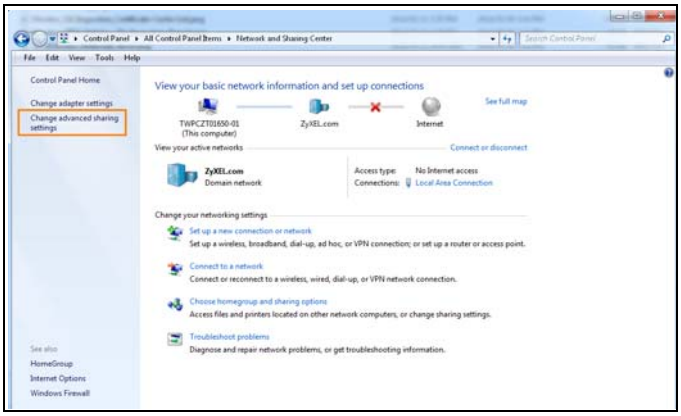
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the USG.

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

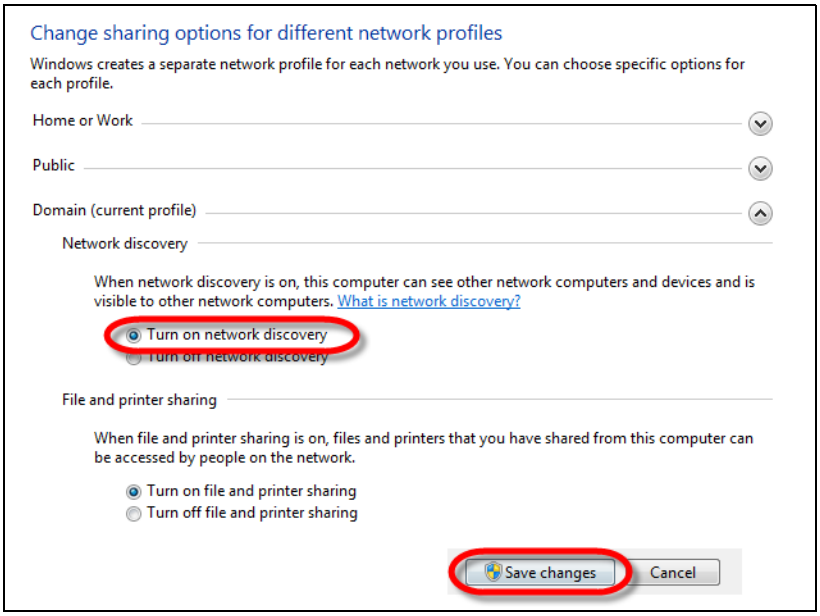
1 Click the start icon, Control Panel and then the Network and Sharing Center.



2 Click Change Advanced Sharing Settings.



3 Select Turn on network discovery and click Save Changes. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



15.4.2 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 USG.

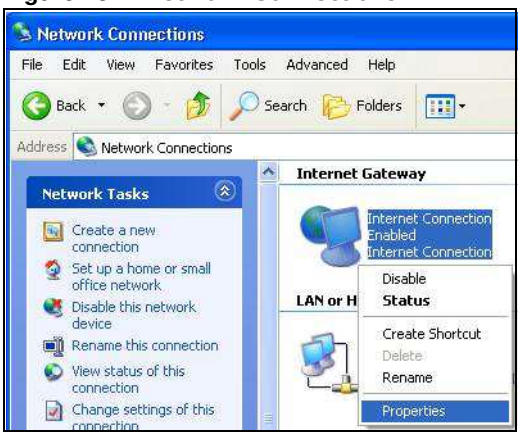
Make sure the computer is connected to a LAN port of the USG. Turn on your computer and the USG.

15.4.2.1 Auto-discover Your UPnP-enabled Network Device

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

2 Right-click the icon and select Properties.

Figure 182 Network Connections



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

Figure 183 Internet Connection Properties



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

Figure 184 Internet Connection Properties: Advanced Settings

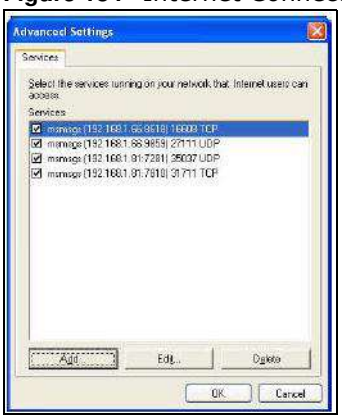


Figure 185 Internet Connection Properties: Advanced Settings: Add



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

5 Select Show icon in notification area when connected option and click OK. An icon displays in the system tray.

Figure 186 System Tray Icon



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

Figure 187 Internet Connection Status



15.4.3 Web Configurator Easy Access

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

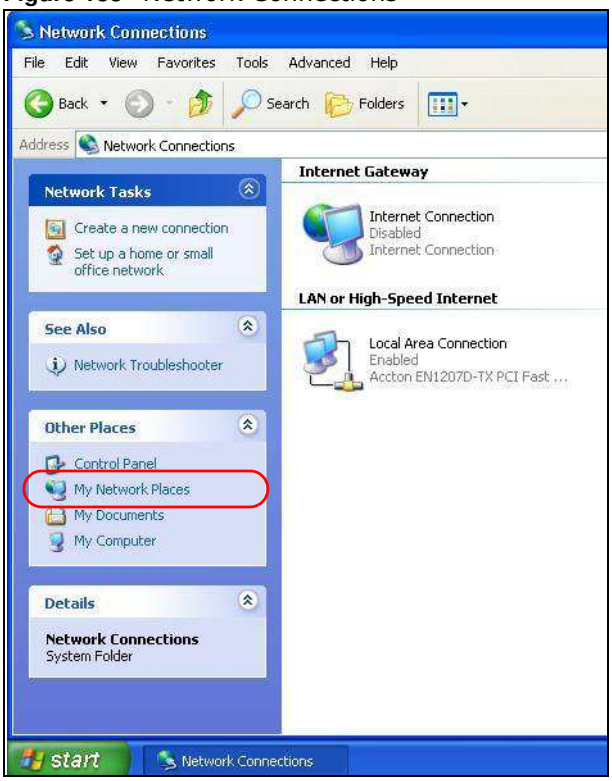
Follow the steps below to access the web configurator.

1 Click Start and then Control Panel.

2 Double-click Network Connections.

3 Select My Network Places under Other Places.

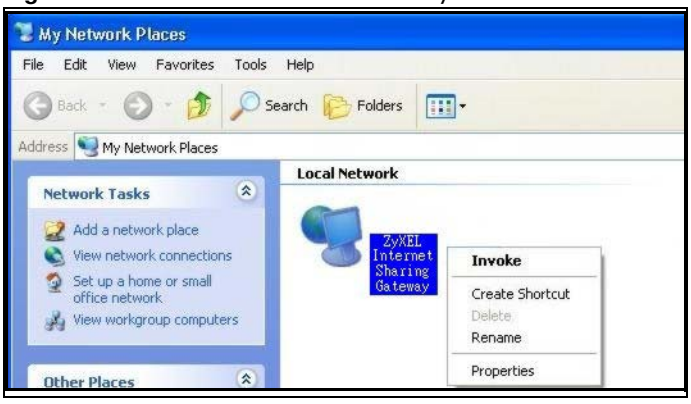
Figure 188 Network Connections



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

5 Right-click on the icon for your USG and select Invoke. The web configurator login screen displays.

Figure 189 Network Connections: My Network Places



6 Right-click on the icon for your USG and select Properties. A properties window displays with basic information about the USG.

Figure 190 Network Connections: My Network Places: Properties: Example



16

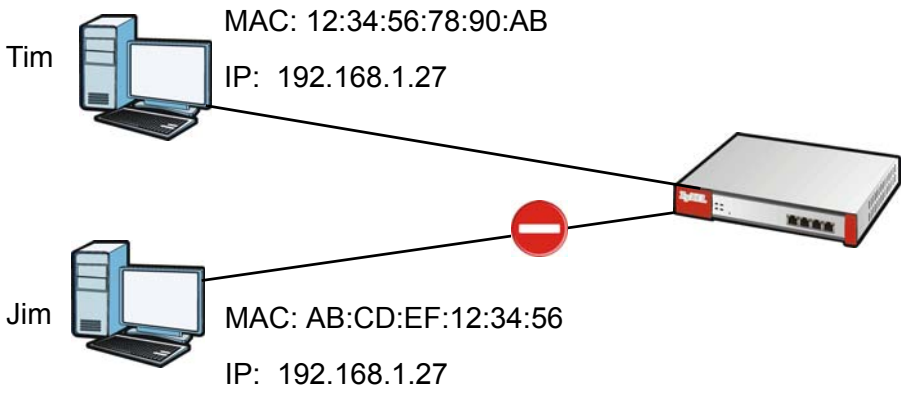
IP/MAC Binding

16.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The USG uses DHCP to assign IP addresses and records the MAC address it assigned to each IP address. The USG then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the USG.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer trying to use IP address 192.168.1.27 with another MAC address.

Figure 191 IP/MAC Binding Example



16.1.1 What You Can Do in this Chapter

- Use the Summary and Edit screens (Section 16.2 on page 284) to bind IP addresses to MAC addresses.
- Use the Exempt List screen (Section 16.3 on page 286) to configure ranges of IP addresses to which the USG does not apply IP/MAC binding.

16.1.2 What You Need to Know

DHCP

IP/MAC address bindings are based on the USG's dynamic and static DHCP entries.

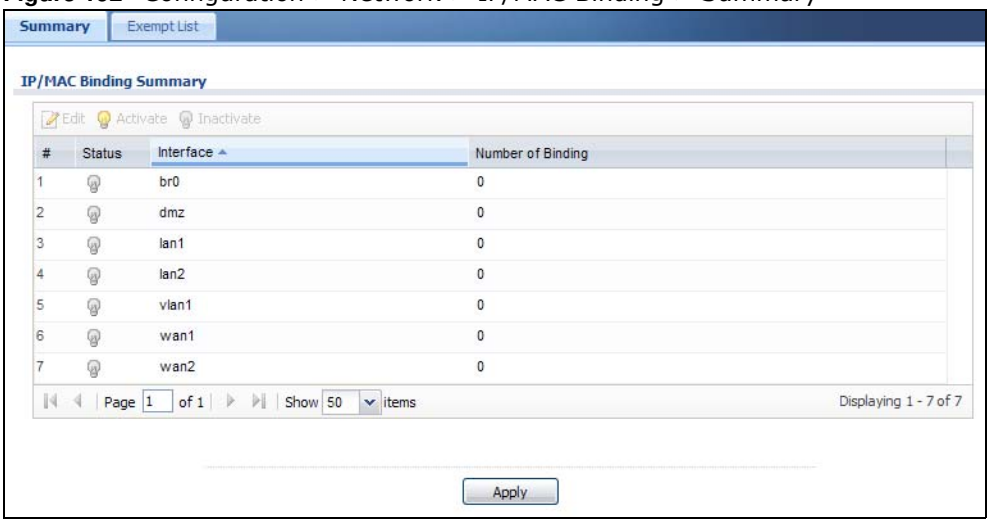
Interfaces Used With IP/MAC Binding

IP/MAC address bindings are grouped by interface. You can use IP/MAC binding with Ethernet, bridge, VLAN, and WLAN interfaces. You can also enable or disable IP/MAC binding and logging in an interface's configuration screen.

16.2 IP/MAC Binding Summary

Click Configuration > Network > IP/MAC Binding to open the IP/MAC Binding Summary screen. This screen lists the total number of IP to MAC address bindings for devices connected to each supported interface.

Figure 192 Configuration > Network > IP/MAC Binding > Summary



The following table describes the labels in this screen.

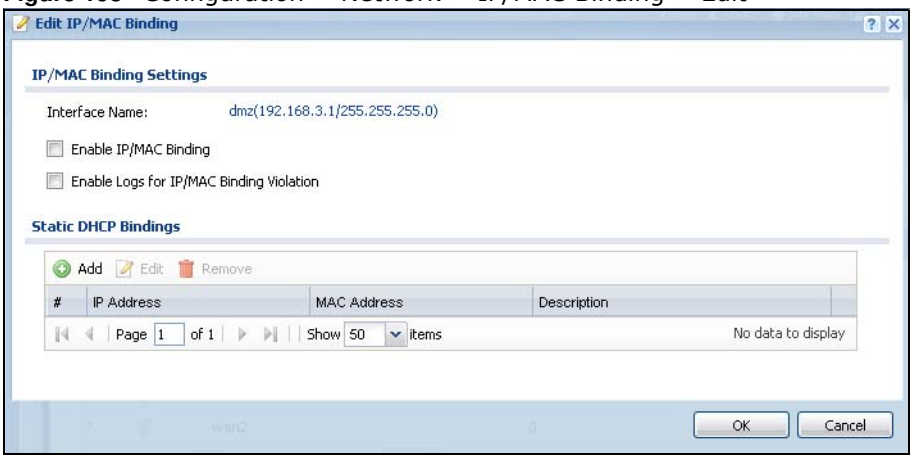
Table 110 Configuration > Network > IP/MAC Binding > Summary

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Interface	This is the name of an interface that supports IP/MAC binding.
Number of Binding	This field displays the interface's total number of IP/MAC bindings and IP addresses that the interface has assigned by DHCP.
Apply	Click Apply to save your changes back to the USG.

16.2.1 IP/MAC Binding Edit

Click Configuration > Network > IP/MAC Binding > Edit to open the IP/MAC Binding Edit screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 193 Configuration > Network > IP/MAC Binding > Edit



The following table describes the labels in this screen.

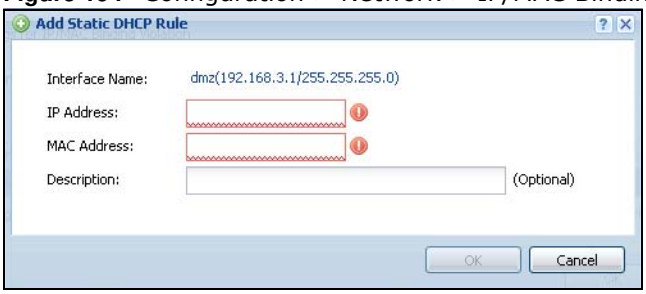
Table 111 Configuration > Network > IP/MAC Binding > Edit

LABEL	DESCRIPTION
IP/MAC Binding Settings	
Interface Name	This field displays the name of the interface within the USG and the interface's IP address and subnet mask.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the USG generate a log if a device connected to this interface attempts to use an IP address not assigned by the USG.
Static DHCP Bindings	This table lists the bound IP and MAC addresses. The USG checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the USG assigns the corresponding IP address. You can also access this table from the interface's edit screen.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
#	This is the index number of the static DHCP entry.
IP Address	This is the IP address that the USG assigns to a device with the entry's MAC address.
MAC Address	This is the MAC address of the device to which the USG assigns the entry's IP address.
Description	This helps identify the entry.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

16.2.2 Static DHCP Edit

Click Configuration > Network > IP/MAC Binding > Edit to open the IP/MAC Binding Edit screen. Click the Add or Edit icon to open the following screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 194 Configuration > Network > IP/MAC Binding > Edit > Add



The following table describes the labels in this screen.

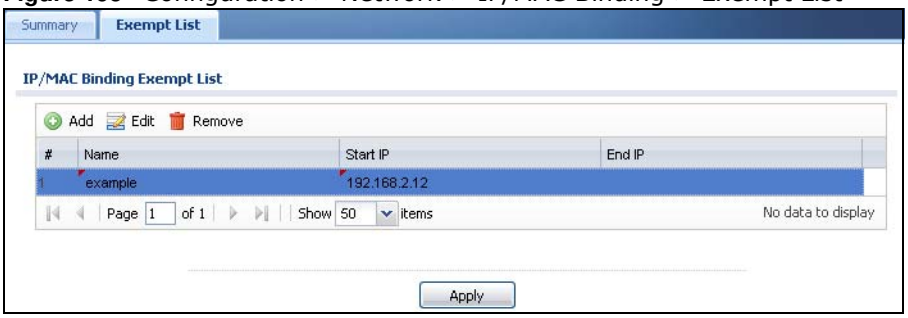
Table 112 Configuration > Network > IP/MAC Binding > Edit > Add

LABEL	DESCRIPTION
Interface Name	This field displays the name of the interface within the USG and the interface's IP address and subnet mask.
IP Address	Enter the IP address that the USG is to assign to a device with the entry's MAC address.
MAC Address	Enter the MAC address of the device to which the USG assigns the entry's IP address.
Description	Enter up to 64 printable ASCII characters to help identify the entry. For example, you may want to list the computer's owner.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

16.3 IP/MAC Binding Exempt List

Click Configuration > Network > IP/MAC Binding > Exempt List to open the IP/MAC Binding Exempt List screen. Use this screen to configure ranges of IP addresses to which the USG does not apply IP/MAC binding.

Figure 195 Configuration > Network > IP/MAC Binding > Exempt List



The following table describes the labels in this screen.

Table 113 Configuration > Network > IP/MAC Binding > Exempt List

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Click an entry or select it and click Edit to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.

Table 113 Configuration > Network > IP/MAC Binding > Exempt List (continued)

LABEL	DESCRIPTION
#	This is the index number of the IP/MAC binding list entry.
Name	Enter a name to help identify this entry.
Start IP	Enter the first IP address in a range of IP addresses for which the USG does not apply IP/MAC binding.
End IP	Enter the last IP address in a range of IP addresses for which the USG does not apply IP/MAC binding.
Add icon	Click the Add icon to add a new entry. Click the Remove icon to delete an entry. A window displays asking you to confirm that you want to delete it.
Apply	Click Apply to save your changes back to the USG.

17

Layer 2 Isolation

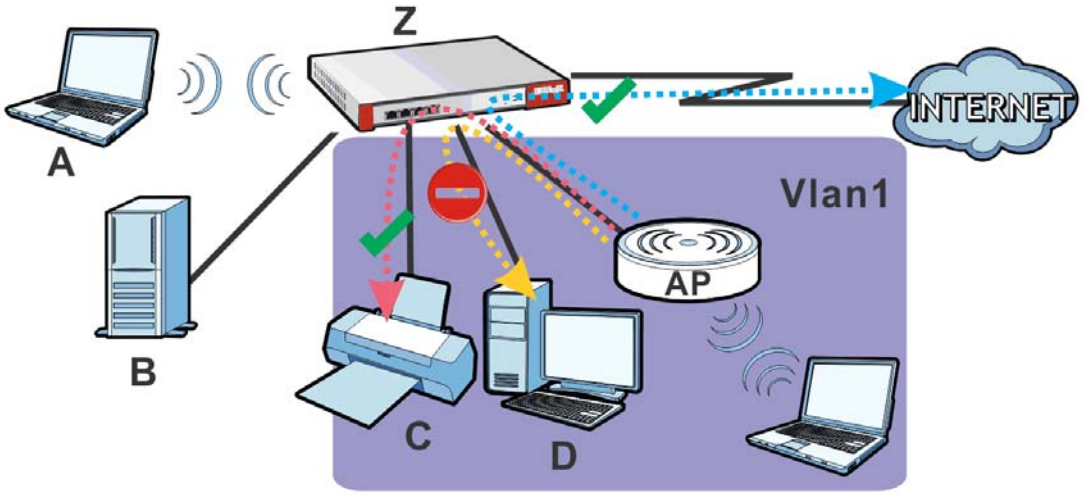
17.1 Overview

Layer-2 isolation is used to prevent connected devices from communicating with each other in the USG's local network(s), except for the devices in the white list, when layer-2 isolation is enabled on the USG and the local interface(s).

Note: The security policy control must be enabled before you can use layer-2 isolation.

In the following example, layer-2 isolation is enabled on the USG's interface Vlan1. A printer, PC and AP are in the Vlan1. The IP address of network printer (C) is added to the white list. With this setting, the connected AP then cannot communicate with the PC (D), but can access the network printer (C), server (B), wireless client (A) and the Internet.

Figure 196 Layer-2 Isolation Application



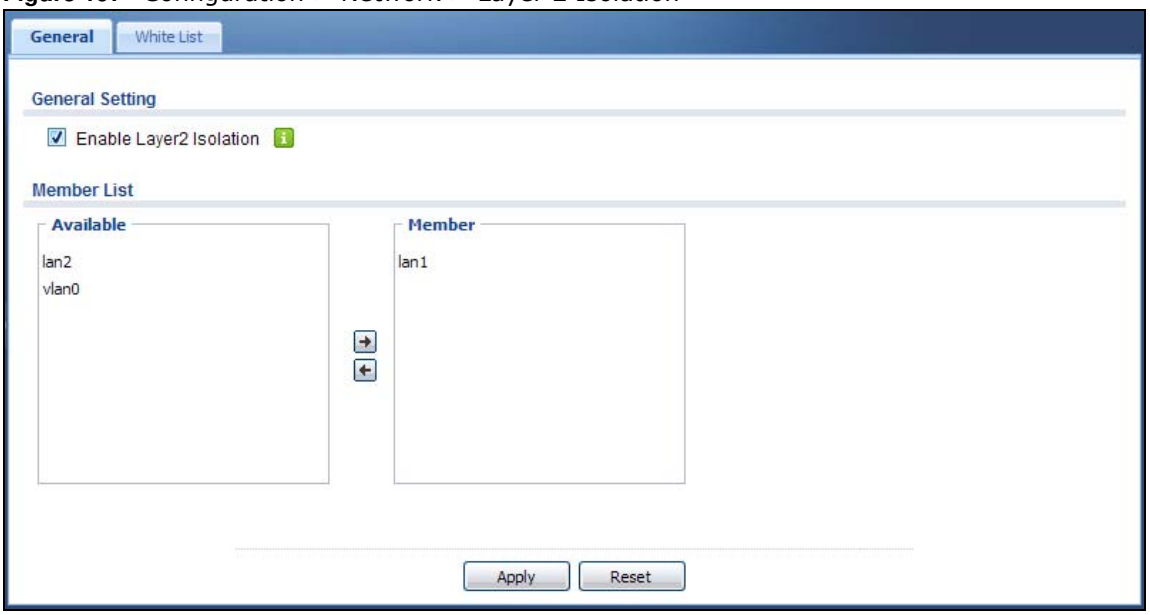
17.1.1 What You Can Do in this Chapter

- Use the General screen (Section 17.2 on page 289) to enable layer-2 isolation on the USG and the internal interface(s).
- Use the White List screen (Section 17.3 on page 289) to enable and configures the white list.

17.2 Layer-2 Isolation General Screen

This screen allows you to enable Layer-2 isolation on the USG and specific internal interface(s). To access this screen click Configuration > Network > Layer 2 Isolation.

Figure 197 Configuration > Network > Layer 2 Isolation



The following table describes the labels in this screen.

Table 114 Configuration > Network > Layer 2 Isolation

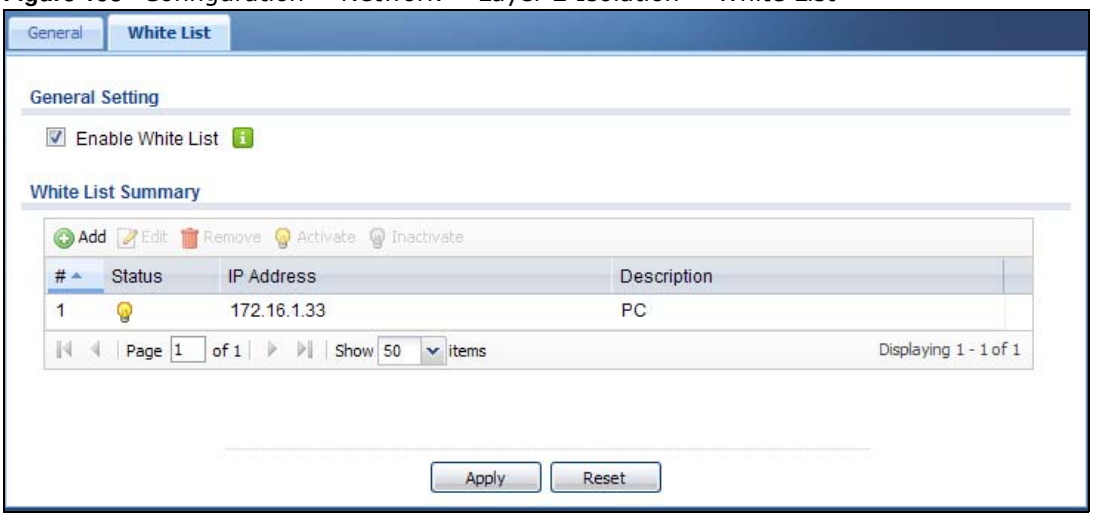
LABEL	DESCRIPTION
Enable Layer2 Isolation	Select this option to turn on the layer-2 isolation feature on the USG. Note: You can enable this feature only when the security policy is enabled.
Member List	The Available list displays the name(s) of the internal interface(s) on which you can enable layer-2 isolation. To enable layer-2 isolation on an interface, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entriess and click the right arrow button to add to the Member list. To remove an interface, select the name(s) in the Member list and click the left arrow button.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

17.3 White List Screen

IP addresses that are not listed in the white list are blocked from communicating with other devices in the layer-2-isolation-enabled internal interface(s) except for broadcast packets.

To access this screen click Configuration > Network > Layer 2 Isolation > White List.

Figure 198 Configuration > Network > Layer 2 Isolation > White List



The following table describes the labels in this screen.

Table 115 Configuration > Network > Layer 2 Isolation > White List

LABEL	DESCRIPTION
Enable White List	Select this option to turn on the white list on the USG. Note: You can enable this feature only when the security policy is enabled.
Add	Click this to add a new rule.
Edit	Click this to edit the selected rule.
Remove	Click this to remove the selected rule.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This field is a sequential value, and it is not associated with a specific rule.
Status	This icon is lit when the rule is active and dimmed when the rule is inactive.
IP Address	This field displays the IP address of device that can be accessed by the devices connected to an internal interface on which layer-2 isolation is enabled.
Description	This field displays the description for the IP address in this rule.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

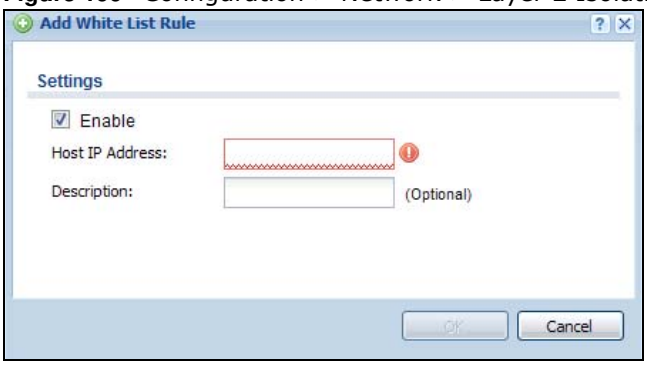
17.3.1 Add/Edit White List Rule

This screen allows you to create a new rule in the white list or edit an existing one. To access this screen, click the Add button or select an entry from the list and click the Edit button.

Note: You can configure up to 100 white list rules on the USG.

Note: You need to know the IP address of each connected device that you want to allow to be accessed by other devices when layer-2 isolation is enabled.

Figure 199 Configuration > Network > Layer 2 Isolation > White List > Add/Edit



The following table describes the labels in this screen.

Table 116 Configuration > Network > Layer 2 Isolation > White List > Add/Edit

LABEL	DESCRIPTION
Enable	Select this option to turn on the rule.
Host IP Address	Enter an IPv4 address associated with this rule.
Description	Specify a description for the IP address associated with this rule. Enter up to 60 characters, spaces and underscores allowed.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

18

Inbound Load Balancing

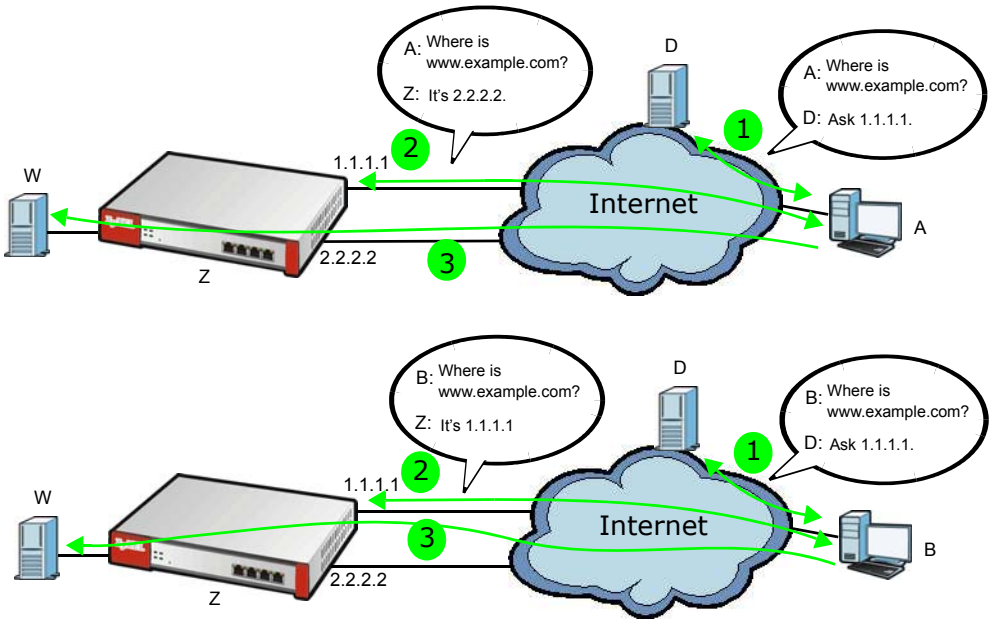
18.1 Inbound Load Balancing Overview

Inbound load balancing enables the USG to respond to a DNS query message with a different IP address for DNS name resolution. The USG checks which member interface has the least load and responds to the DNS query message with the interface's IP address.

In the following figure, an Internet host (A) sends a DNS query message to the DNS server (D) in order to resolve a domain name of www.example.com. DNS server D redirects it to the USG (Z)'s WAN1 with an IP address of 1.1.1.1. The USG receives the DNS query message and responds to it with the WAN2's IP address, 2.2.2.2, because the WAN2 has the least load at that moment.

Another Internet host (B) also sends a DNS query message to ask where www.example.com is. The USG responds to it with the WAN1's IP address, 1.1.1.1, since WAN1 has the least load this time.

Figure 200 DNS Load Balancing Example



18.1.1 What You Can Do in this Chapter

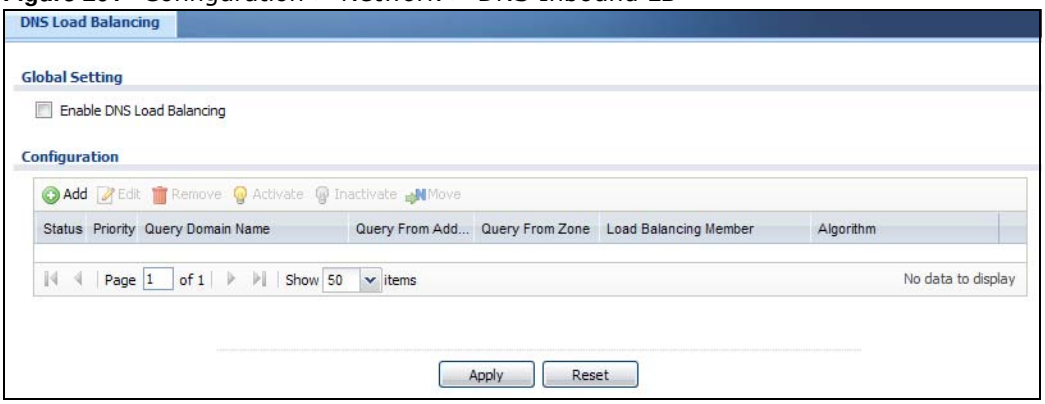
- Use the Inbound LB screen (see Section 18.2 on page 293) to view a list of the configured DNS load balancing rules.
- Use the Inbound LB Add/ Edit screen (see Section 18.2.1 on page 294) to add or edit a DNS load balancing rule.

18.2 The Inbound LB Screen

The Inbound LB screen provides a summary of all DNS load balancing rules and the details. You can also use this screen to add, edit, or remove the rules. Click Configuration > Network > Inbound LB to open the following screen.

Note: After you finish the inbound load balancing settings, go to security policy and NAT screens to configure the corresponding rule and virtual server to allow the Internet users to access your internal servers.

Figure 201 Configuration > Network > DNS Inbound LB



The following table describes the labels in this screen.

Table 117 Configuration > Network > Inbound LB

LABEL	DESCRIPTION
Global Setting	
Enable DNS Load Balancing	Select this to enable DNS load balancing.
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	To move an entry to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This field displays the order in which the USG checks the member interfaces of this DNS load balancing rule.
Query Domain Name	This field displays the domain name for which the USG manages load balancing between the specified interfaces.
Query From Address	This field displays the source IP address of the DNS query messages to which the USG applies the DNS load balancing rule.
Query From Zone	The USG applies the DNS load balancing rule to the query messages received from this zone.

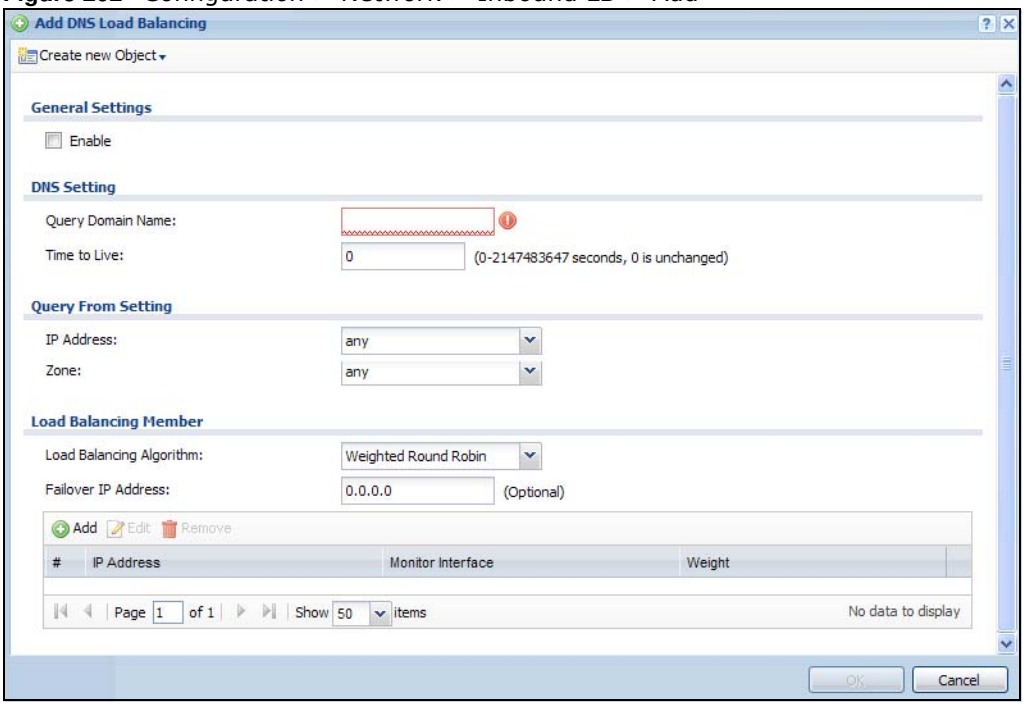
Table 117 Configuration > Network > Inbound LB (continued)

LABEL	DESCRIPTION
Load Balancing Member	This field displays the member interfaces which the USG manages for load balancing.
Algorithm	This field displays the load balancing method the USG uses for this DNS load balancing rule. Weighted Round Robin - Each member interface is assigned a weight. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the USG chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. Least Connection - The USG chooses choose a member interface which is handling the least number of sessions. Least Load - Outbound - The USG chooses a member interface which is handling the least amount of outgoing traffic. Least Load - Inbound - The USG chooses a member interface which is handling the least amount of incoming traffic. Least Load - Total - The USG chooses a member interface which is handling the least amount of outgoing and incoming traffic.
Apply	Click this button to save your changes to the USG.
Reset	Click this button to return the screen to its last-saved settings.

18.2.1 The Inbound LB Add/Edit Screen

The Add DNS Load Balancing screen allows you to add a domain name for which the USG manages load balancing between the specified interfaces. You can configure the USG to apply DNS load balancing to some specific hosts only by configuring the Query From settings. Click Configuration > Network > Inbound LB and then the Add or Edit icon to open this screen.

Figure 202 Configuration > Network > Inbound LB > Add



The following table describes the labels in this screen.

Table 118 Configuration > Network > Inbound LB > Add/Edit

LABEL	DESCRIPTION
Create New Object	Use this to configure any new setting objects that you need to use in this screen.
General Settings	
Enable	Select this to enable this DNS load balancing rule.
DNS Setting	
Query Domain Name	Type up to 255 characters for a domain name for which you want the USG to manage DNS load balancing. You can use a wildcard (*) to let multiple domains match the name. For example, use *.example.com to specify any domain name that ends with "example.com" would match.
Time to Live	Enter the number of seconds the USG recommends DNS request hosts to keep the DNS entry in their caches before removing it. Enter 0 to have the USG not recommend this so the DNS request hosts will follow their DNS server's TTL setting.
Query From Setting	
IP Address	Enter the IP address of a computer or a DNS server which makes the DNS queries upon which to apply this rule. DNS servers process client queries using recursion or iteration: • In recursion, DNS servers make recursive queries on behalf of clients. So you have to configure this field to the DNS server's IP address when recursion is used. • In iteration, a client asks the DNS server and expects the best and immediate answer without the DNS server contacting other DNS servers. If the primary DNS server cannot provide the best answer, the client makes iteration queries to other configured DNS servers to resolve the name. You have to configure this field to the client's IP address when iteration is used.
Zone	Select the zone of DNS query messages upon which to apply this rule.
Load Balancing Member	
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box. Select Weighted Round Robin to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the USG chooses wan1 for 2 sessions' traffic and wan2 for every session's traffic in each round of 3 new sessions. Select Least Connection to have the USG choose the member interface which is handling the least number of sessions. Select Least Load - Outbound to have the USG choose the member interface which is handling the least amount of outgoing traffic. Select Least Load - Inbound to have the USG choose the member interface which is handling the least amount of incoming traffic. Select Least Load - Total to have the USG choose the member interface which is handling the least amount of outgoing and incoming traffic.
Failover IP Address	Enter an alternate IP address with which the USG will respond to a DNS query message when the load balancing algorithm cannot find any available interface.
Add	Click this to create a new member interface for this rule.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.

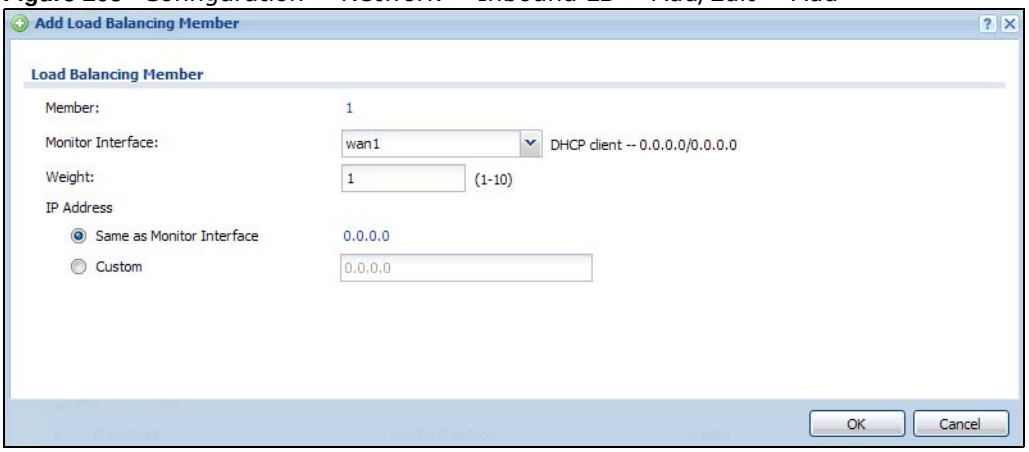
Table 118 Configuration > Network > Inbound LB > Add/Edit (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
#	This field displays the order in which the USG checks this rule's member interfaces.
IP Address	This field displays the IP address of the member interface.
Monitor Interface	This field displays the name of the member interface. The USG manages load balancing between the member interfaces.
Weight	This field is available if you selected Weighted Round Robin as the load balancing algorithm. This field displays the weight of the member interface. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

18.2.2 The Inbound LB Member Add/Edit Screen

The Add Load Balancing Member screen allows you to add a member interface for the DNS load balancing rule. Click Configuration > Network > Inbound LB > Add or Edit and then an Add or Edit icon to open this screen.

Figure 203 Configuration > Network > Inbound LB > Add/Edit > Add



The following table describes the labels in this screen.

Table 119 Configuration > Network > Inbound LB > Add/Edit > Add/Edit

LABEL	DESCRIPTION
Member	The USG checks each member interface's loading in the order displayed here.
Monitor Interface	Select an interface to associate it with the DNS load balancing rule. This field also displays whether the IP address is a static IP address (Static), dynamically assigned (Dynamic) or obtained from a DHCP server (DHCP Client), as well as the IP address and subnet mask.
Weight	This field is available if you selected Weighted Round Robin for the load balancing algorithm. Specify the weight of the member interface. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.
IP Address	

Table 119 Configuration > Network > Inbound LB > Add/Edit > Add/Edit (continued)

LABEL	DESCRIPTION
Same as Monitor Interface	Select this to send the IP address displayed in the Monitor Interface field to the DNS query senders.
Custom	Select this and enter another IP address to send to the DNS query senders.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

19

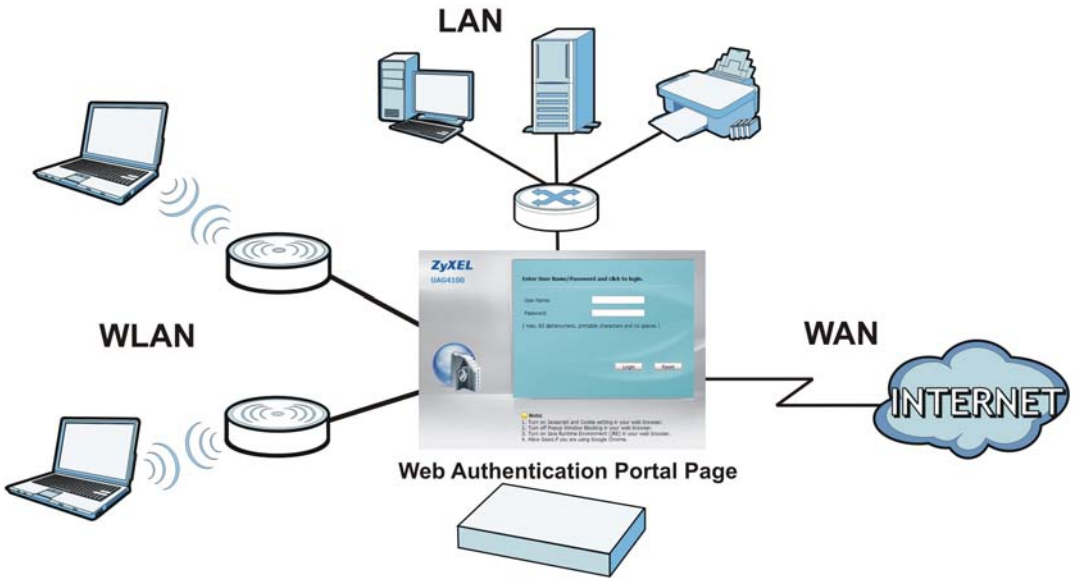
Web Authentication

19.1 Web Auth Overview

Web authentication can intercept network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. This means all web page requests can initially be redirected to a special web page that requires users to authenticate their sessions. Once authentication is successful, they can then connect to the rest of the network or Internet.

As soon as a user attempt to open a web page, the USG reroutes his/her browser to a web portal page that prompts him/her to log in.

Figure 204 Web Authentication Example



The web authentication page only appears once per authentication session. Unless a user session times out or he/she closes the connection, he or she generally will not see it again during the same session.

19.1.1 What You Can Do in this Chapter

- Use the Configuration > Web Authentication screens (Section 19.2 on page 299) to create and manage web authentication policies.
- Use the Configuration > Web Authentication > SSO screen (Section 19.3 on page 303) to configure how the USG communictates with a Single Sign-On agent.

19.1.2 What You Need to Know

Single Sign-On

A SSO (Single Sign On) agent integrates Domain Controller and USG authentication mechanisms, so that users just need to log in once (single) to get access to permitted resources.

Forced User Authentication

Instead of making users for which user-aware policies have been configured go to the USG Login screen manually, you can configure the USG to display the Login screen automatically whenever it routes HTTP traffic for anyone who has not logged in yet.

Note: This works with HTTP traffic only. The USG does not display the Login screen when users attempt to send other kinds of traffic.

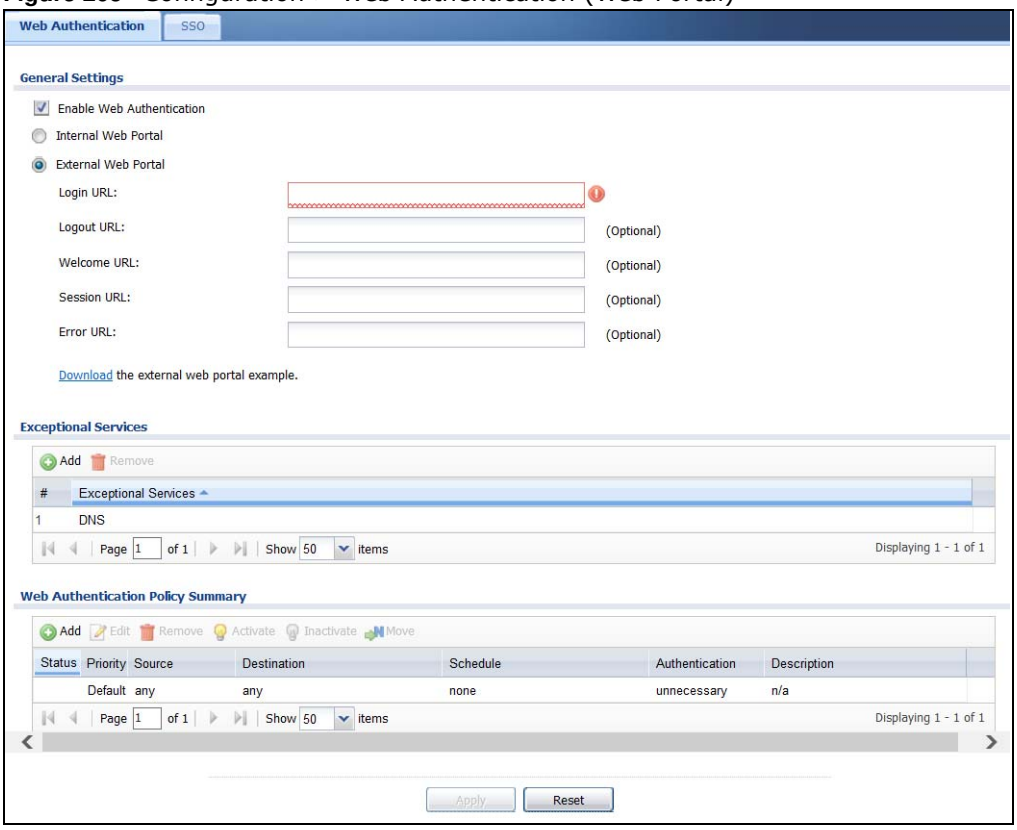
The USG does not automatically route the request that prompted the login, however, so users have to make this request again.

19.2 Web Authentication Screen

The Web Authentication screen displays the web portal settings and web authentication policies you have configured on the USG. The screen differs depending on what you select in the Authentication field.

Click Configuration > Web Authentication to display the screen.

Figure 205 Configuration > Web Authentication (Web Portal)



The following table gives an overview of the objects you can configure.

Table 120 Configuration > Web Authentication

LABEL	DESCRIPTION
Enable Web Authentication	Select Enable Web Authentication to turn on the web authentication feature. Once enabled, all network traffic is blocked until a client authenticates with the USG through the specifically designated web portal.
Internal Web Portal	Select this to use the default login page built into the USG. If you later assign a custom login page, you can still return to the USG's default page as it is saved indefinitely. The login page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network. You can customize the login page built into the USG in the System > WWW > Login Page screen.
External Web Portal	Select this to use a custom login page from an external web portal instead of the default one built into the USG. You can configure the look and feel of the web portal page.
Login URL	Specify the login page's URL; for example, http://IIS server IP Address/login.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Logout URL	Specify the logout page's URL; for example, http://IIS server IP Address/logout.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Welcome URL	Specify the welcome page's URL; for example, http://IIS server IP Address/welcome.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.

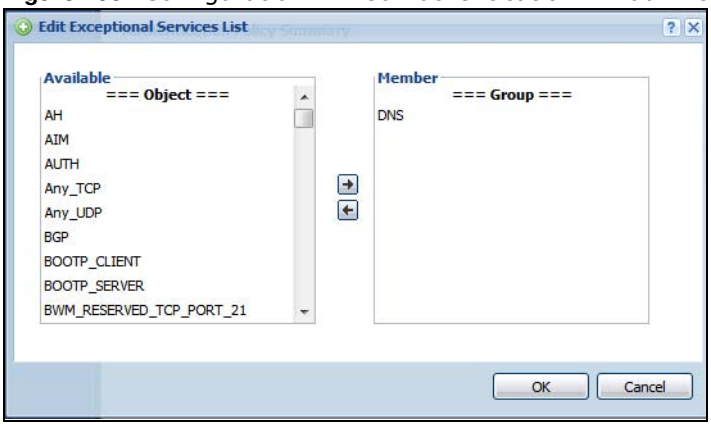
Table 120 Configuration > Web Authentication (continued)

LABEL	DESCRIPTION
Session URL	Specify the session page's URL; for example, http://IIS server IP Address/session.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Error URL	Specify the error page's URL; for example, http://IIS server IP Address/error.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Download	Click this to download an example web portal file for your reference.
Exceptional Services	Use this table to list services that users can access without logging in. In the list, select one or more entries and click Remove to delete it or them. Keeping DNS as a member allows users' computers to resolve domain names into IP addresses. Click Add to add new services that users can access without logging in.
Web Authentication Policy Summary	Use this table to manage the USG's list of web authentication policies.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	To move an entry to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This is the position of the authentication policy in the list. The priority is important as the policies are applied in order of priority. Default displays for the default authentication policy that the USG uses on traffic that does not match any exceptional service or other authentication policy. You can edit the default rule but not delete it.
Source	This displays the source address object to which this policy applies.
Destination	This displays the destination address object to which this policy applies.
Schedule	This field displays the schedule object that dictates when the policy applies. none means the policy is active at all times if enabled.
Authentication	This field displays the authentication requirement for users when their traffic matches this policy. unnecessary - Users do not need to be authenticated. required - Users need to be authenticated. They must manually go to the login screen. The USG will not redirect them to the login screen. force - Users need to be authenticated. The USG automatically displays the login screen whenever it routes HTTP traffic for users who have not logged in yet.
Description	If the entry has a description configured, it displays here. This is n/a for the default policy.
Apply	Click this button to save your changes to the USG.
Reset	Click this button to return the screen to its last-saved settings.

19.2.1 Creating Exceptional Services

This screen lists services that users can access without logging in. Click Add under Exceptional Services in the previous screen to display this screen. You can change the list's membership here. Available services appear on the left. Select any services you want users to be able to access without logging in and click the right arrow button -> to add them. The member services are on the right. Select any service that you want to remove from the member list, and click the left arrow <- button to remove them. Then click OK to apply the changes and return to the main Web Authentication screen. Alternatively, click Cancel to discard the changes and return to the main Web Authentication screen.

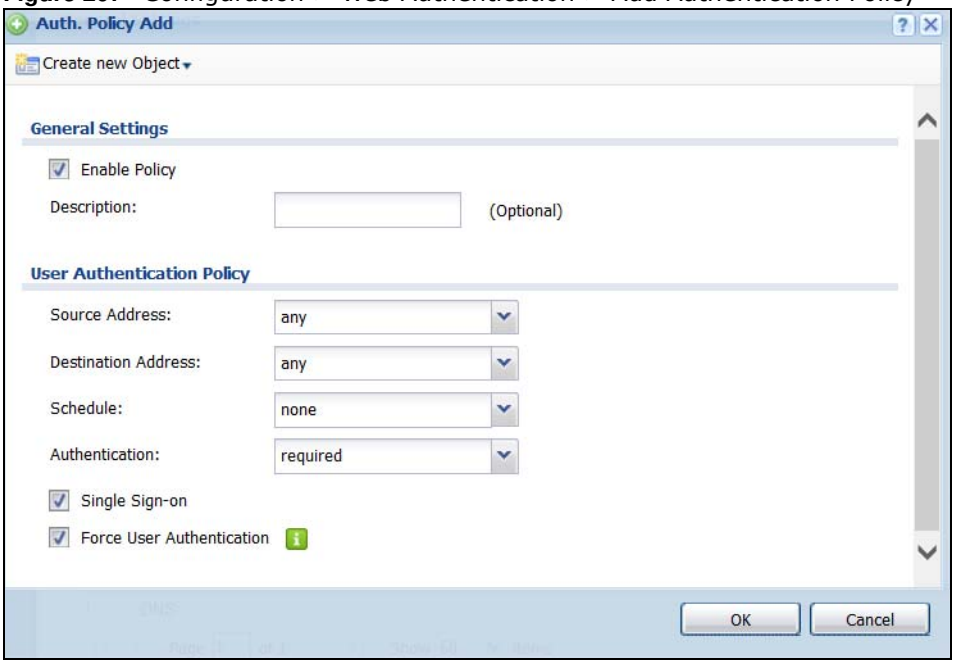
Figure 206 Configuration > Web Authentication > Add Exceptional Service



19.2.2 Creating/Editing an Authentication Policy

Click Configuration > Web Authentication and then the Add (or Edit) icon in the Web Authentication Policy Summary section to open the Auth. Policy Add/ Edit screen. Use this screen to configure an authentication policy.

Figure 207 Configuration > Web Authentication > Add Authentication Policy



The following table gives an overview of the objects you can configure.

Table 121 Configuration > Web Authentication > Add Authentication Policy

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen. Select Address or Schedule.
Enable Policy	Select this check box to activate the authentication policy. This field is available for user-configured policies.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the policy. Spaces are allowed. This field is available for user-configured policies.
User Authentication Policy	Use this section of the screen to determine which traffic requires (or does not require) the senders to be authenticated in order to be routed.
Source Address	Select a source address or address group for whom this policy applies. Select any if the policy is effective for every source. This is any and not configurable for the default policy.
Destination Address	Select a destination address or address group for whom this policy applies. Select any if the policy is effective for every destination. This is any and not configurable for the default policy.
Schedule	Select a schedule that defines when the policy applies. Otherwise, select none and the rule is always effective. This is none and not configurable for the default policy.
Authentication	Select the authentication requirement for users when their traffic matches this policy. unnecessary - Users do not need to be authenticated. required - Users need to be authenticated. If Force User Authentication is selected, all HTTP traffic from unauthenticated users is redirected to a default or user-defined login page. Otherwise, they must manually go to the login screen. The USG will not redirect them to the login screen.
Single Sign-on	This field is available for user-configured policies that require Single Sign-On (SSO). Select this to have the USG enable the SSO feature. You can set up this feature in the SSO screen.
Force User Authentication	This field is available for user-configured policies that require authentication. Select this to have the USG automatically display the login screen when users who have not logged in yet try to send HTTP traffic.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving.

19.3 SSO Overview

The SSO (Single Sign-On) function integrates Domain Controller and USG authentication mechanisms, so that users just need to log in once (single login) to get access to permitted resources.

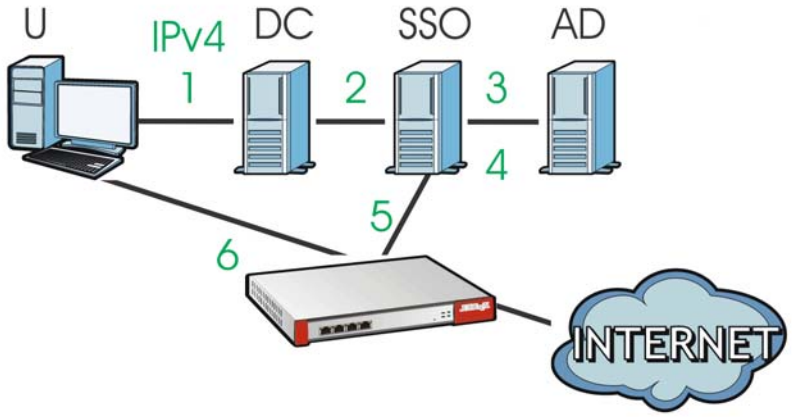
In the following figure, U user logs into a Domain Controller (DC) which passes the user's login credentials to the SSO agent. The SSO agent checks that these credentials are correct with the AD server, and if the AD server confirms so, the SSO then notifies the USG to allow access for the user to the permitted resource (Internet access, for example).

Note: The USG, the DC, the SSO agent and the AD server must all be in the same domain and be able to communicate with each other.

SSO does not support IPv6, LDAP or RADIUS; you must use it in an IPv4 network environment with Windows AD (Active Directory) authentication database.

You must enable Web Authentication in the Configuration > Web Authentication screen.

Figure 208 SSO Overview



U	User
DC	Domain Controller
SSO	Single Sign-On agent
AD	Active Directory

Install the SSO Agent on one of the following platforms:

- Windows 7 Professional (32-bit and 64-bit)
- Windows Server 2008 Enterprise (32-bit and 64-bit)
- Windows 2008 R2 (64-bit)
- Windows Server 2012 (64-bit)

19.4 SSO - USG Configuration

This section shows what you have to do on the USG in order to use SSO.

Table 122 USG - SSO Agent Field Mapping

USG		SSO	
SCREEN	**FIELD**	**SCREEN**	**FIELD**
Web Authentication > SSO	Listen Port	Agent Configuration Page > Gateway Setting	Gateway Port
Web Authentication > SSO	Primary Agent Port	Agent Configuration Page	Agent Listening Port
Object > User/Group > User > Add	Group Identifier	Agent Configuration Page > Configure LDAP/AD Server	Group Membership
Object > AAA Server > Active Directory > Add	Base DN	Agent Configuration Page > Configure LDAP/AD Server	Base DN
Object > AAA Server > Active Directory > Add	Bind DN	Agent Configuration Page > Configure LDAP/AD Server	Bind DN
Object > User/Group > User > Add	User Name	Agent Configuration Page > Configure LDAP/AD Server	Login Name Attribute
Object > AAA Server > Active Directory > Add	Server Address	Agent Configuration Page > Configure LDAP/AD Server	Server Address
Network > Interface > Ethernet > wan (IPv4)	IP address	Agent Configuration Page > Gateway Setting	Gateway IP

19.4.1 Configuration Overview

These are the screens you need to configure:

- Configure the USG to Communicate with SSO on page 305
- Enable Web Authentication on page 306
- Create a Security Policy on page 307
- Configure User Information on page 308
- Configure an Authentication Method on page 309
- Configure Active Directory on page 310 or Configure Active Directory on page 310

19.4.2 Configure the USG to Communicate with SSO

Use Configuration > Web Authentication > SSO to configure how the USG communicates with the Single Sign-On (SSO) agent.

Figure 209 Configuration > Web Authentication > SSO



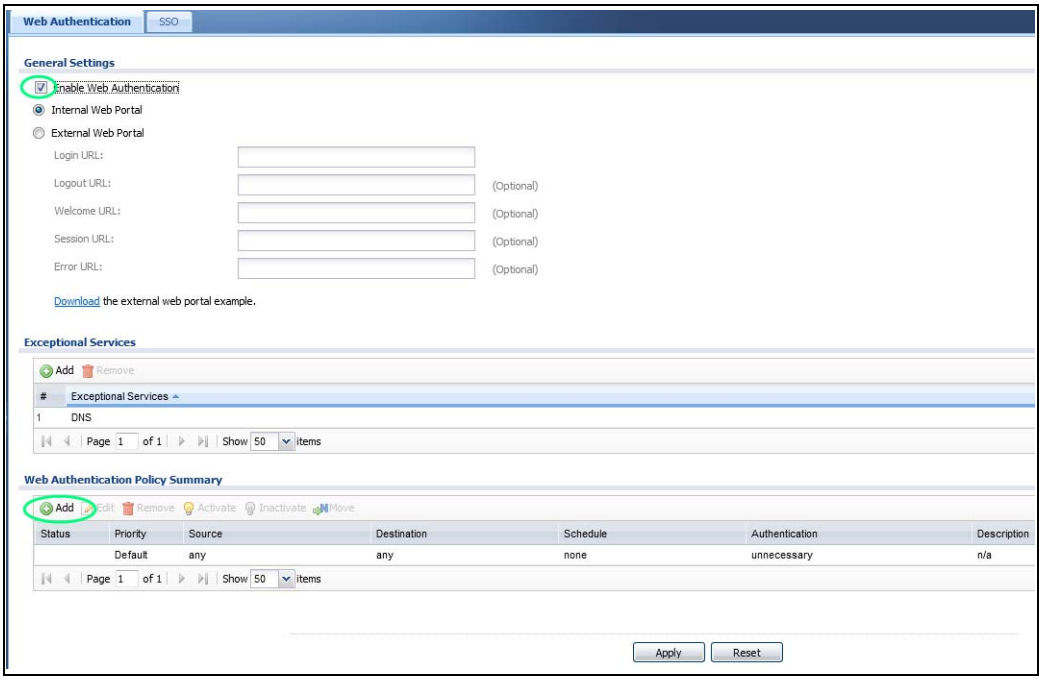
The following table gives an overview of the objects you can configure.

Table 123 Configuration > Web Authentication > SSO

LABEL	DESCRIPTION
Listen Port	The default agent listening port is 2158. If you change it on the USG, then change it to the same number in the Gateway Port field on the SSO agent too. Type a number ranging from 1025 to 65535.
Agent PreShareKey	Type 8-32 printable ASCII characters or exactly 32 hex characters (0-9; a-f). The Agent PreShareKey is used to encrypt communications between the USG and the SSO agent.
Primary Agent Address	Type the IPv4 address of the SSO agent. The USG and the SSO agent must be in the same domain and be able to communicate with each other.
Primary Agent Port	Type the same port number here as in the Agent Listening Port field on the SSO agent. Type a number ranging from 1025 to 65535.
Secondary Agent Address (Optional)	Type the IPv4 address of the backup SSO agent if there is one. The USG and the backup SSO agent must be in the same domain and be able to communicate with each other.
Secondary Agent Port (Optional)	Type the same port number here as in the Agent Listening Port field on the backup SSO agent if there is one. Type a number ranging from 1025 to 65535.
Apply	Click this button to save your changes to the USG.
Reset	Click this button to return the screen to its last-saved settings

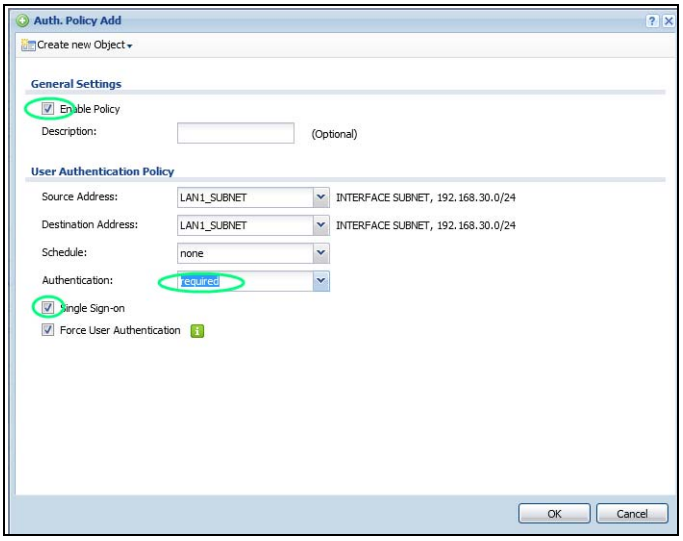
19.4.3 Enable Web Authentication

Enable Web Authentication and add a web authentication policy.



Make sure you select Enable Policy, Single Sign-On and choose required in Authentication.

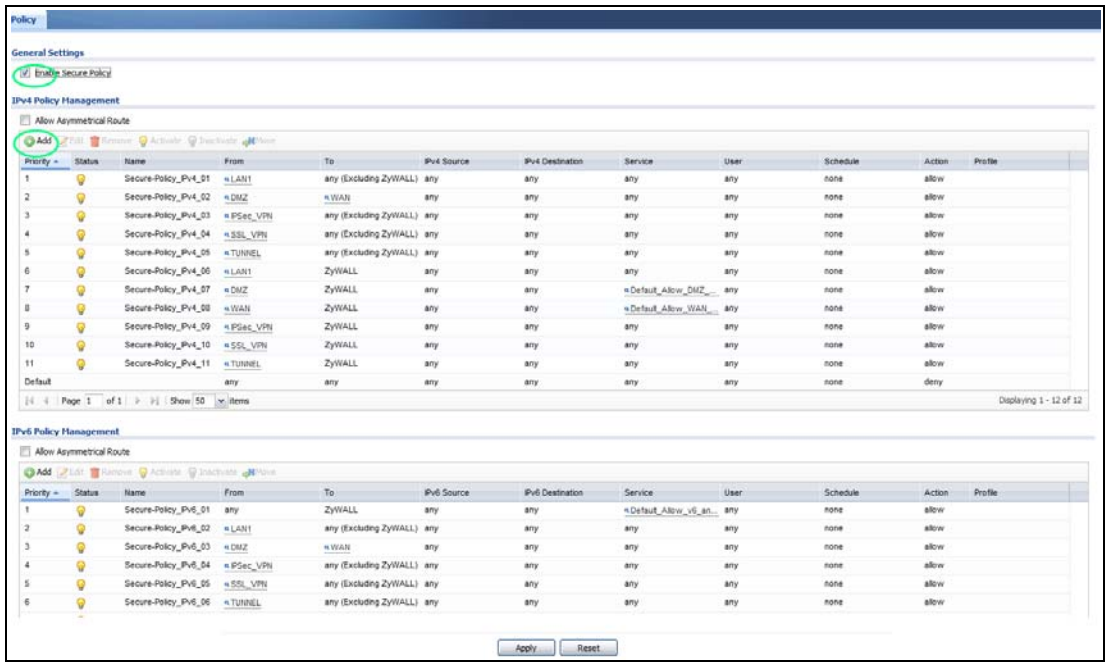
Do NOT select any as the source address unless you want all incoming connections to be authenticated!



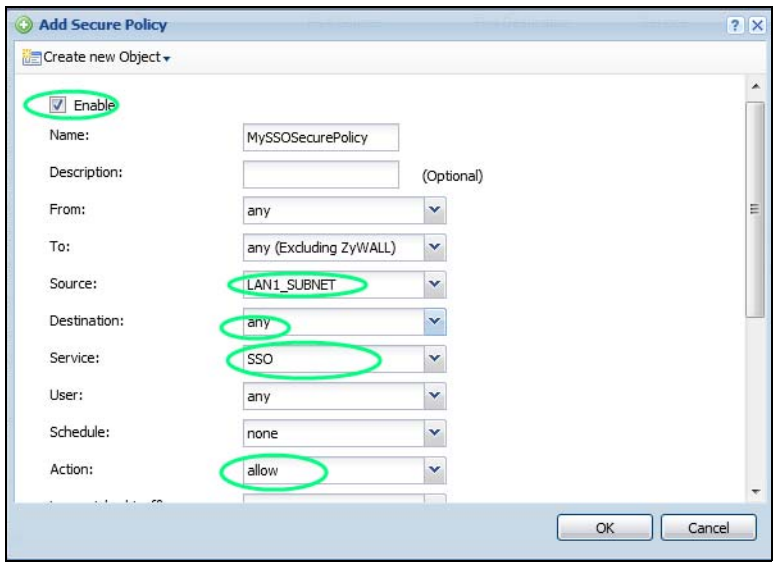
See Table 120 on page 300 and Table 121 on page 303 for more information on configuring these screens.

19.4.4 Create a Security Policy

Configure a Security Policy for SSO traffic source and destination direction in order to prevent the security policy from blocking this traffic. Go to Configuration > Security Policy > Policy and add a new policy if a default one does not cover the SSO web authentication traffic direction.

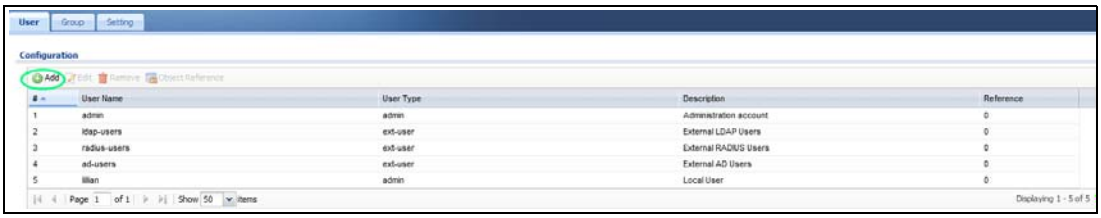


Configure the fields as shown in the following screen. Configure the source and destination addresses according to the SSO web authrntication traffic in your network.

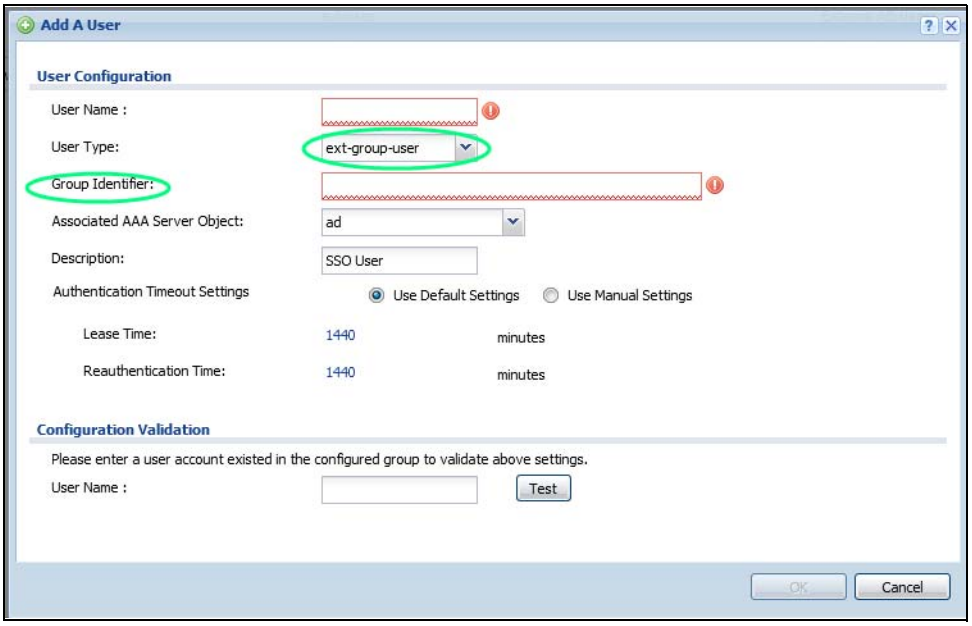


19.4.5 Configure User Information

Configure a User account of the ext-group-user type.

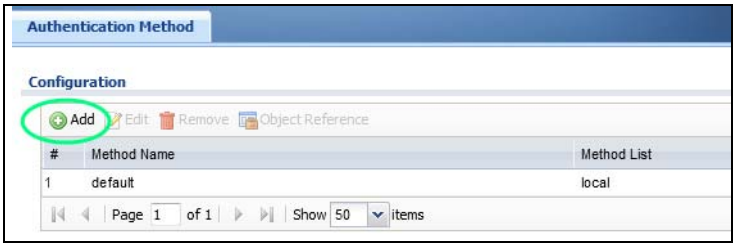


Configure `Group Identifier` to be the same as `Group Membership` on the SSO agent.

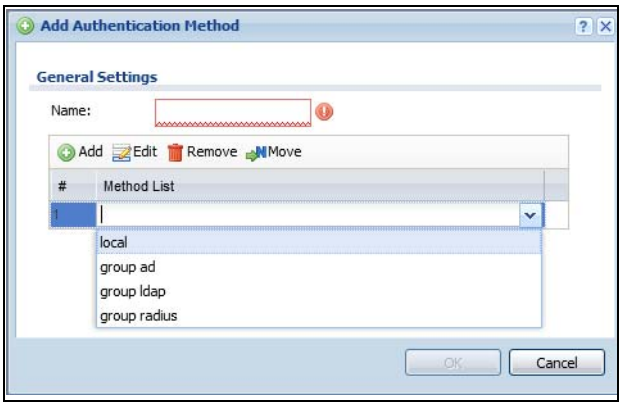


19.4.6 Configure an Authentication Method

Configure Active Directory (AD) for authentication with SSO.



Choose `group ad` as the authentication server for SSO.

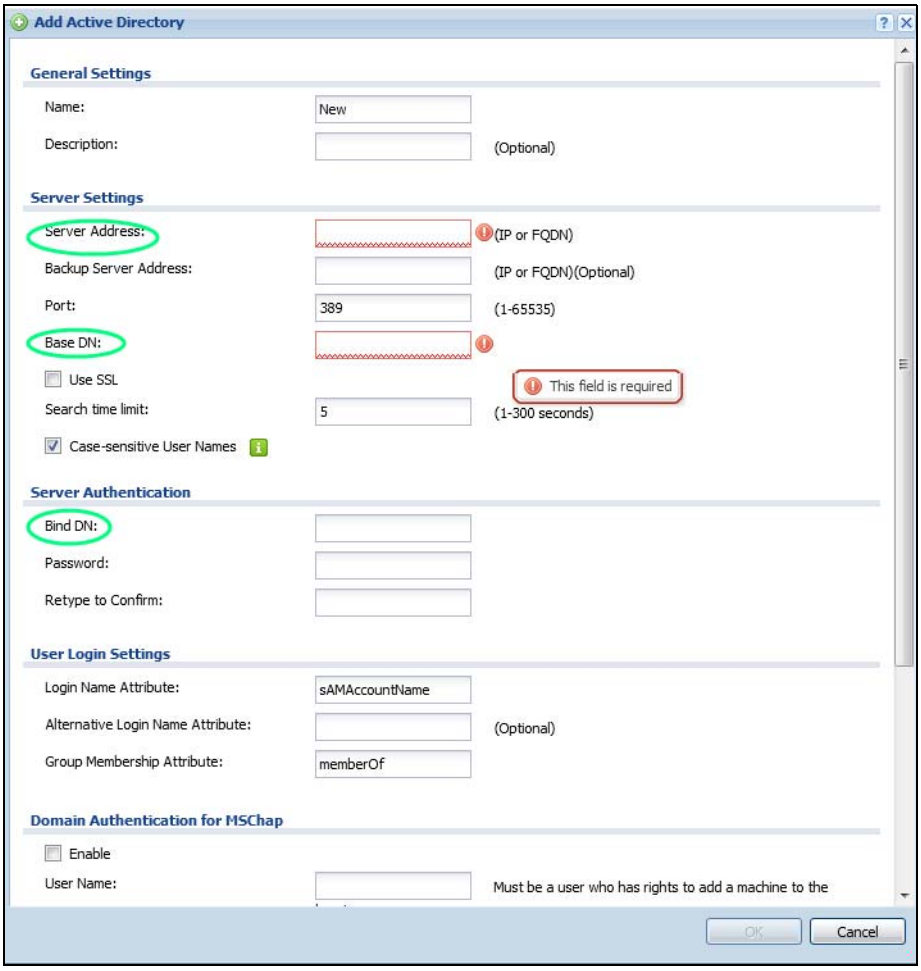


19.4.7 Configure Active Directory

You must configure an Active Directory (AD) server in AAA Setup to be the same as AD configured on the SSO agent.



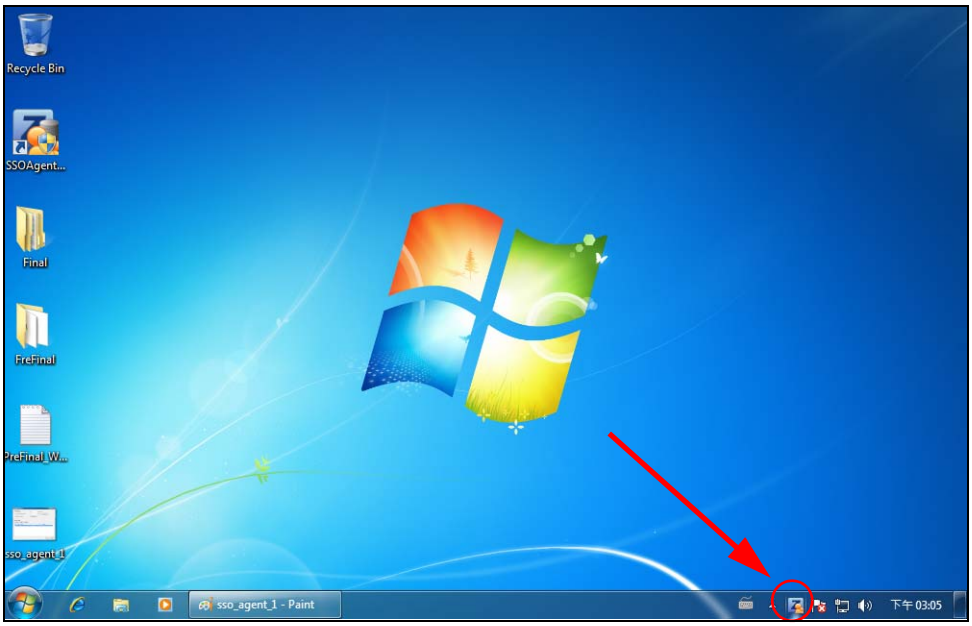
The default AD server port is 389. If you change this, make sure you make the same changes on the SSO. Configure the Base DN exactly the same as on the Domain Controller and SSO. Bind DN is a user name and password that allows the USG to join the domain with administrative privileges. It is a required field.



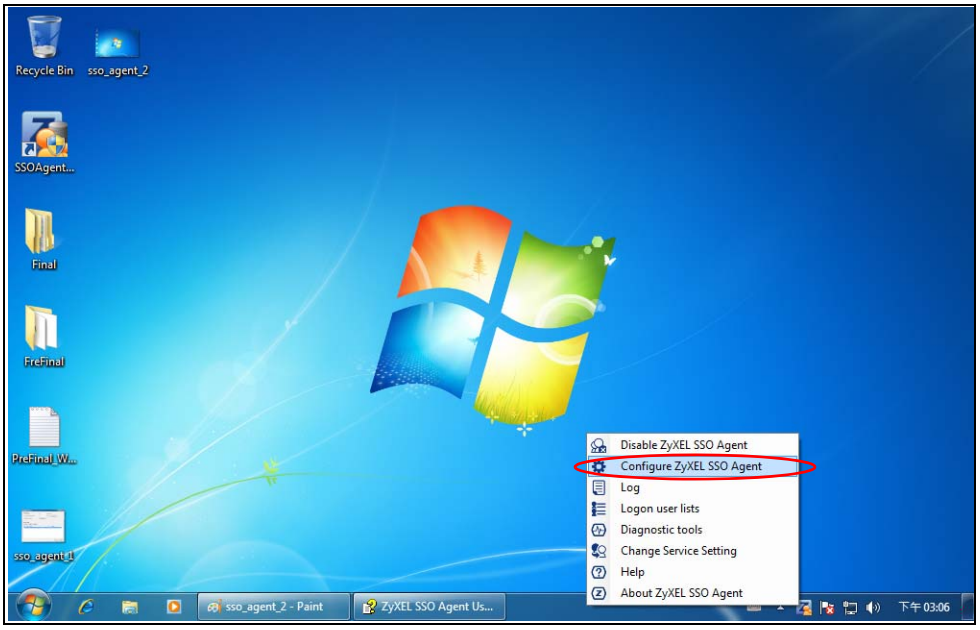
19.5 SSO Agent Configuration

This section shows what you have to do on the SSO agent in order to work with the USG.

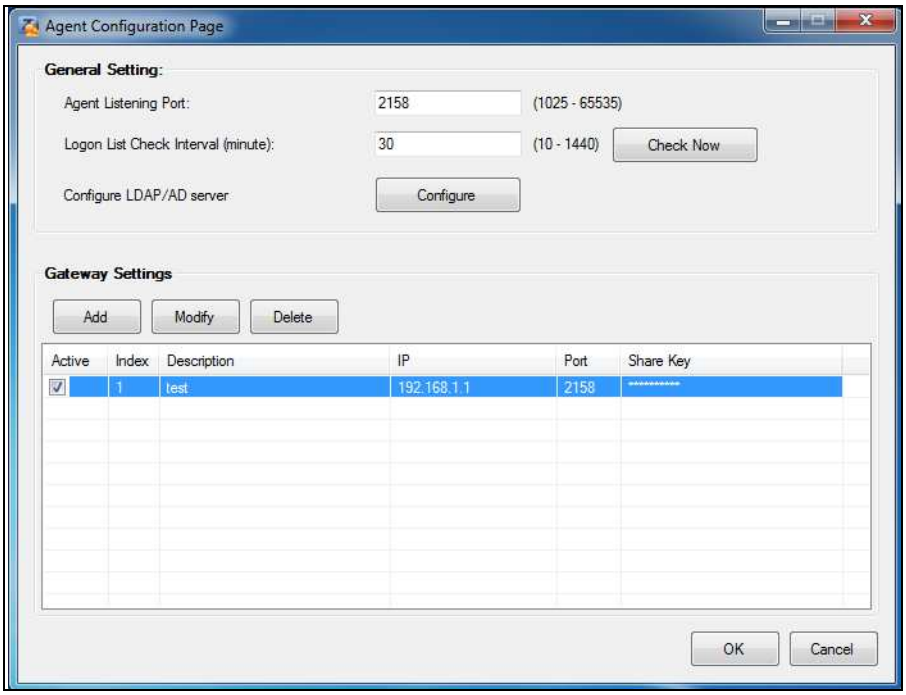
After you install the SSO agent, you will see an icon in the system tray (bottom right of the screen)



Right-click the SSO icon and select Configure ZyXEL SSO Agent.

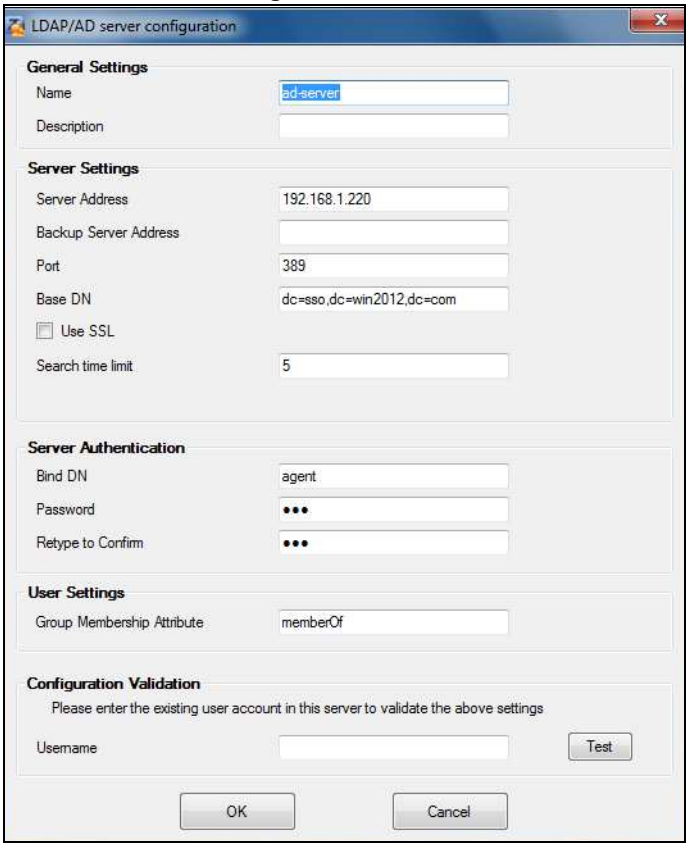


Configure the Agent Listening Port, AD server exactly as you have done on the USG. Add the USG IP address as the Gateway. Make sure the USG and SSO agent are able to communicate with each other.

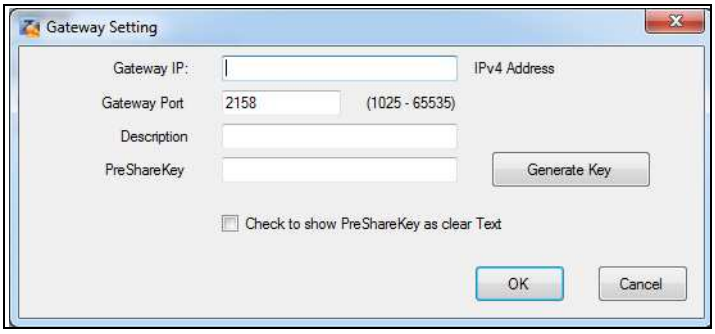


Configure the Server Address, Port, Base DN, Bind DN, Login Name Attribute and Group Membership for the AD server settings exactly as you have done on the USG. Group Membership is called Group Identifier on the USG.

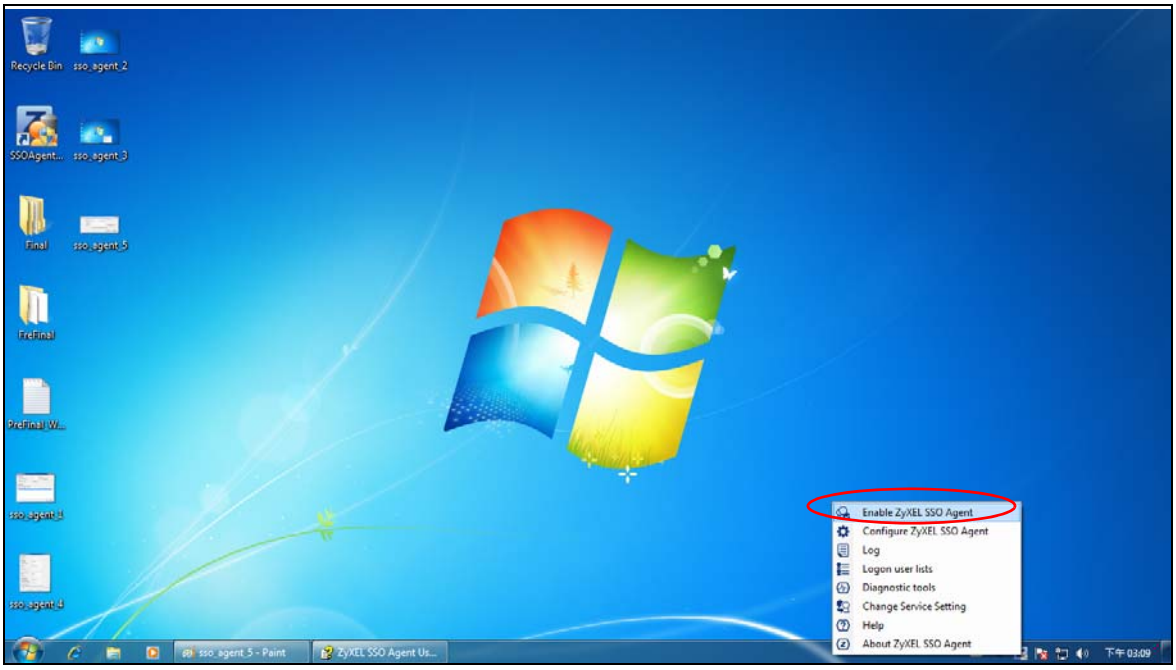
LDAP/AD Server Configuration



Configure the Gateway IP address, Gateway Port and PreShareKey exactly as you have done in the USG Configuration > Web Authentication > SSO screen. If you want to use Generate Key to have the SSO create a random password, select Check to show PreShareKey as clear Text so as to see the password, then copy and paste it to the USG.



After all SSO agent configurations are done, right-click the SSO icon in the system tray and select Enable ZyXEL SSO Agent.



20

Security Policy

20.1 Overview

A security policy is a template of security settings that can be applied to specific traffic at specific times. The policy can be applied:

- to a specific direction of travel of packets (from / to)
- to a specific source and destination address objects
- to a specific type of traffic (services)
- to a specific user or group of users
- at a specific schedule

The policy can be configured:

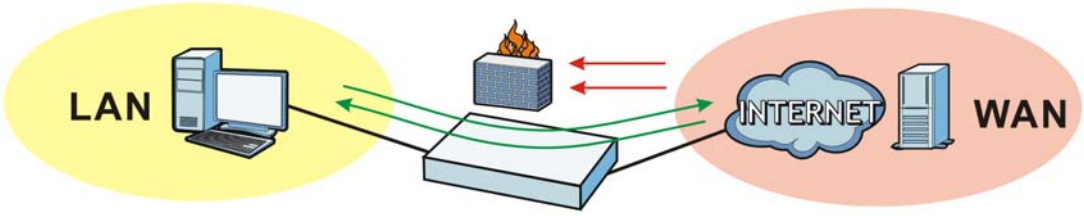
- to allow or deny traffic that matches the criteria above
- send a log or alert for traffic that matches the criteria above
- to apply the actions configured in the UTM profile (content filter,) to traffic that matches the criteria above

Note: Security policies can be applied to both IPv4 and IPv6 traffic.

The security policies can also limit the number of user sessions.

The following example shows the USG's default security policies behavior for a specific direction of travel of packets. WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the USG allows the response. However, the USG blocks incoming Telnet traffic initiated from the WAN zone and destined for the LAN zone.

Figure 210 Default Directional Security Policy Example



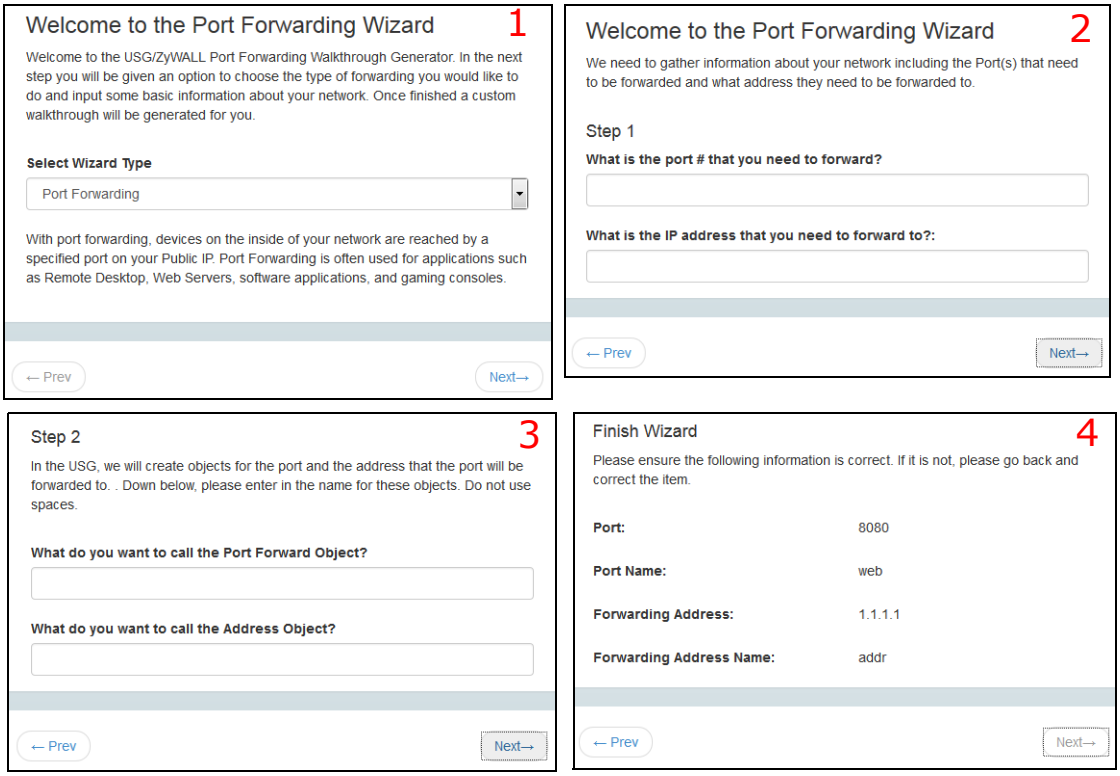
20.2 One Security

OneSecurity.com is a website with guidance on configuration walkthroughs, troubleshooting, and other information.

Note: Note that the walkthroughs do not perform the actual configuring, but just show you how to do it.

This is an example of a port forwarding configuration walkthrough.

Figure 211 Example of a Port Forwarding Configuration Walkthrough.



This is an example of L2TP over IPSec VPN Troubleshooting troubleshooting.

Figure 212 Example of L2TP over IPSec Troubleshooting - 1

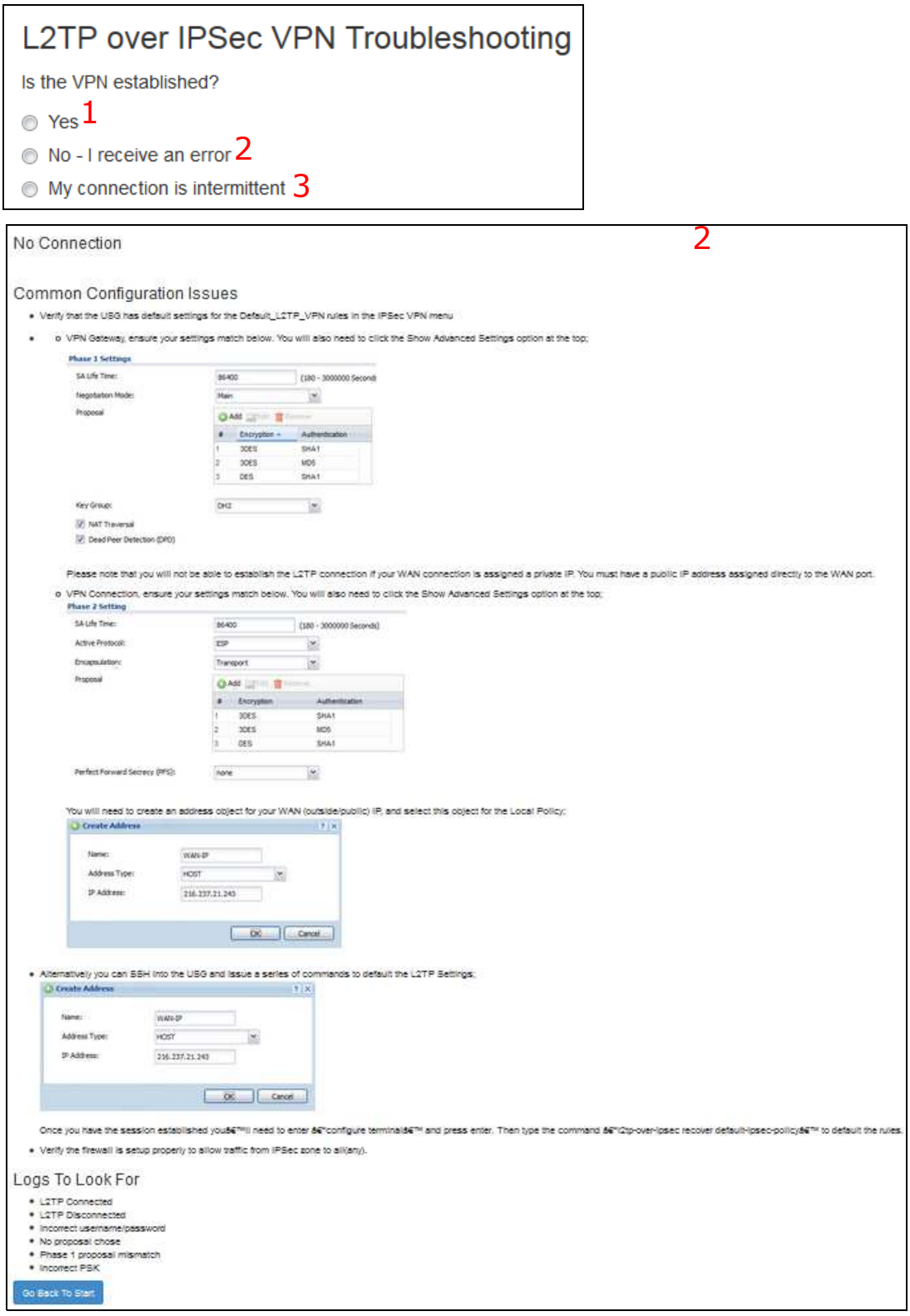
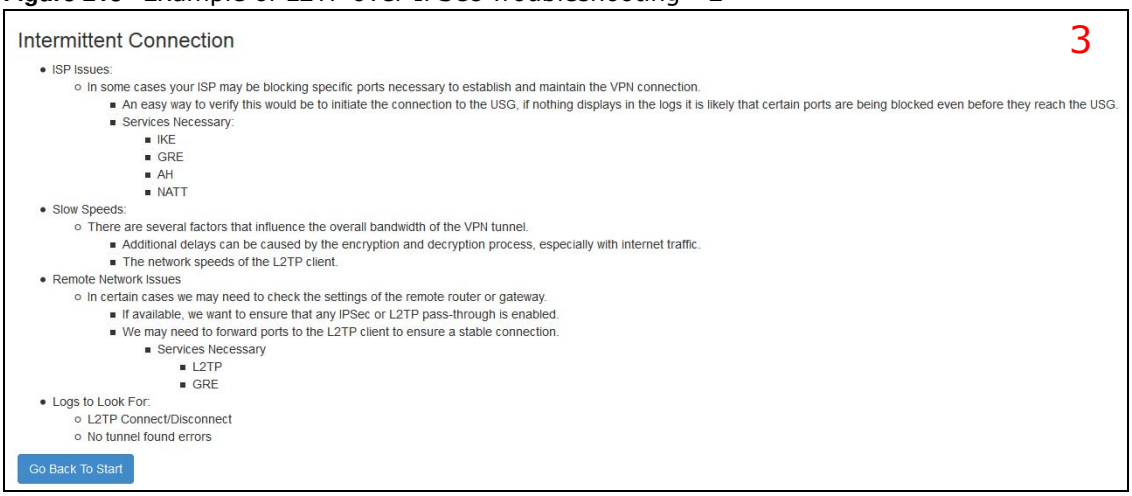


Figure 213 Example of L2TP over IPSec Troubleshooting - 2



In the USG, you will see icons that link to OneSecurity walkthroughs, troubleshooting and so on in certain screens.

For example, at the time of writing, these are the OneSecurity icons you can see.

Table 124 OneSecurity Icons

ONESECURITY ICON	SCREEN
Configuration Walkthrough	Click this icon to go to a series of screens that guide you how to configure the feature. Note that the walkthroughs do not perform the actual configuring, but just show you how to do it. • Licensing > Registration • Network > NAT • Network > Routing > Policy Route • UTM Profile > Content Filter • UTM Profile > Anti-Spam • VPN > IPSec VPN • VPN > SSL VPN • VPN > L2TP VPN
Troubleshooting	Click this icon to go to a series of screens that guide you how to fix problems with the feature. • Network > NAT • Network > Routing > Policy Route • UTM Profile > Content Filter • UTM Profile > Anti-Spam • VPN > IPSec VPN • VPN > SSL VPN • VPN > L2TP VPN
Content Filter	Click this icon for more information on Content Filter, which controls access to specific web sites or web content. • UTM Profile > Content Filter
Anti-Spam	Click this icon for more information on Anti-Spam which can mark or discard spam (unsolicited commercial or junk e-mail) and e-mail from certain servers suspect of being used by spammers. • UTM Profile > Anti-Spam

Table 124 OneSecurity Icons (continued)

ONESECURITY ICON	SCREEN
	Click this icon for more information on IPSec and SSL VPN. Internet Protocol Security (IPSec) VPN connects IPSec routers or remote users using IPSec client software. SSL VPN allows users to use a web browser for secure remote user login without need of a VPN router or VPN client software. • VPN > IPSec VPN • VPN > SSL VPN
	Click this icon to download VPN client software. • VPN > IPSec VPN • VPN > SSL VPN
	Click this icon for more information on the Wireless AP Controller which sets how the USG allows APs to connect to the wireless network. • Wireless > AP Management > Mgnt. AP List

20.3 What You Can Do in this Chapter

- Use the Security Policy Control screens (Section 20.4 on page 321) to enable or disable policies, asymmetrical routes, and manage and configure policies.
- Use the Session Control screens (see Section 20.5 on page 327) to limit the number of concurrent NAT/security policies traffic sessions a client can use.

20.3.1 What You Need to Know

Stateful Inspection

The USG uses stateful inspection in its security policies. The USG restricts access by screening data packets against defined access rules. It also inspects sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

Zones

A zone is a group of interfaces. Group the USG's interfaces into different zones based on your needs. You can configure security policies for data passing between zones or even between interfaces.

Default Directional Security Policy Behavior

Security Policies can be grouped based on the direction of travel of packets to which they apply. Here is the The USG has default Security Policy behavior for traffic going through the USG in various directions.

Table 125 Directional Security Policy Behavior

FROM ZONE TO ZONE	BEHAVIOR
From any to Device	DHCP traffic from any interface to the USG is allowed.
From LAN1 to any (other than the USG)	Traffic from the LAN1 to any of the networks connected to the USG is allowed.
From LAN2 to any (other than the USG)	Traffic from the LAN2 to any of the networks connected to the USG is allowed.
From LAN1 to Device	Traffic from the LAN1 to the USG itself is allowed.
From LAN2 to Device	Traffic from the LAN2 to the USG itself is allowed.
From WAN to Device	The default services listed in To-Device Policies on page 320 are allowed from the WAN to the USG itself. All other WAN to USG traffic is dropped.
From any to any	Traffic that does not match any security policy is dropped. This includes traffic from the WAN to any of the networks behind the USG. This also includes traffic to or from interfaces that are not assigned to a zone (extra-zone traffic).

To-Device Policies

Policies with Device as the To Zone apply to traffic going to the USG itself. By default:

- The Security Policy allows only LAN, or WAN computers to access or manage the USG.
- The USG allows DHCP traffic from any interface to the USG.
- The USG drops most packets from the WAN zone to the USG itself and generates a log except for AH, ESP, GRE, HTTPS, IKE, NATT.

When you configure a Security Policy rule for packets destined for the USG itself, make sure it does not conflict with your service control rule. The USG checks the security policy before the service control rules for traffic destined for the USG.

A From Any To Device direction policy applies to traffic from an interface which is not in a zone.

Global Security Policies

Security Policies with from any and/or to any as the packet direction are called global Security Policies. The global Security Policies are the only Security Policies that apply to an interface that is not included in a zone. The from any policies apply to traffic coming from the interface and the to any policies apply to traffic going to the interface.

Security Policy Rule Criteria

The USG checks the schedule, user name (user's login name on the USG), source IP address and object, destination IP address and object, IP protocol type of network traffic (service) and UTM profile criteria against the Security Policies (in the order you list them). When the traffic matches a policy, the USG takes the action specified in the policy.

User Specific Security Policies

You can specify users or user groups in Security Policies. For example, to allow a specific user from any computer to access a zone by logging in to the USG, you can set up a policy based on the user name only. If you also apply a schedule to the Security Policy, the user can only access the network at the scheduled time. A user-aware Security Policy is activated whenever the user logs in to the USG and will be disabled after the user logs out of the USG.

Session Limits

Accessing the USG or network resources through the USG requires a NAT session and corresponding Security Policy session. Peer to peer applications, such as file sharing applications, may use a large number of NAT sessions. A single client could use all of the available NAT sessions and prevent others from connecting to or through the USG. The USG lets you limit the number of concurrent NAT/Security Policy sessions a client can use.

20.4 The Security Policy Screen

Asymmetrical Routes

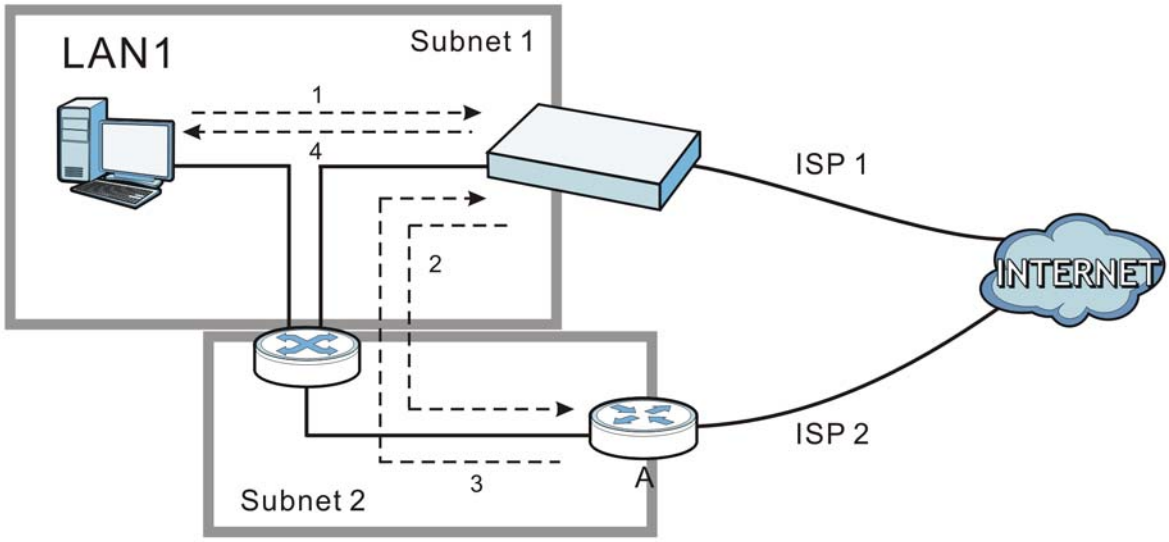
If an alternate gateway on the LAN has an IP address in the same subnet as the USG's LAN IP address, return traffic may not go through the USG. This is called an asymmetrical or "triangle" route. This causes the USG to reset the connection, as the connection has not been acknowledged.

You can have the USG permit the use of asymmetrical route topology on the network (not reset the connection). However, allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the USG. A better solution is to use virtual interfaces to put the USG and the backup gateway on separate subnets. Virtual interfaces allow you to partition your network into logical sections over the same interface. See the chapter about interfaces for more information.

By putting LAN 1 and the alternate gateway (A in the figure) in different subnets, all returning network traffic must pass through the USG to the LAN. The following steps and figure describe such a scenario.

1. A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The USG reroutes the packet to gateway A, which is in Subnet 2.
3. The reply from the WAN goes to the USG.
4. The USG then sends it to the computer on the LAN1 in Subnet 1.

Figure 214 Using Virtual Interfaces to Avoid Asymmetrical Routes



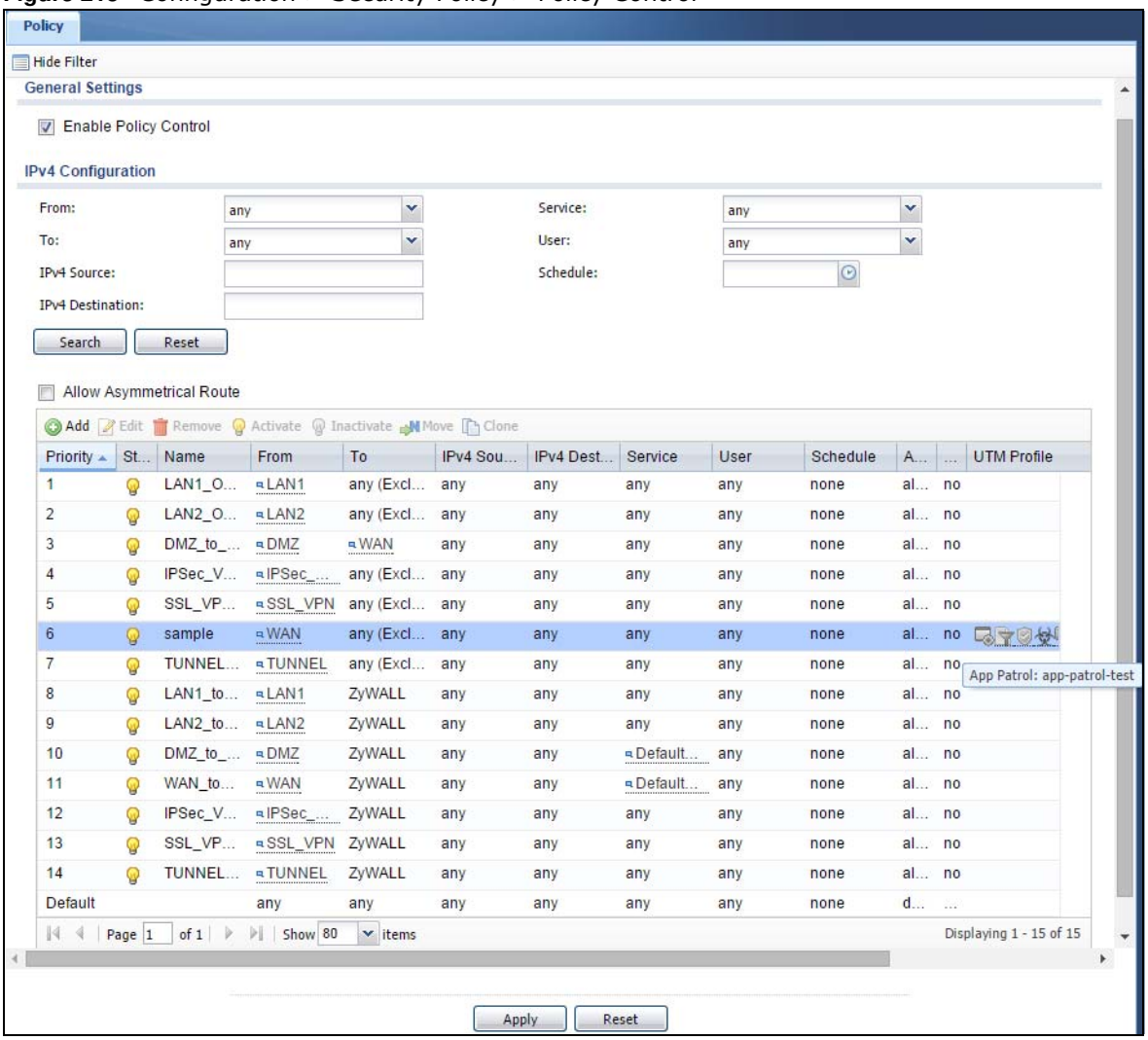
20.4.1 Configuring the Security Policy Control Screen

Click Configuration > Security Policy > Policy Control to open the Security Policy screen. Use this screen to enable or disable the Security Policy and asymmetrical routes, set a maximum number of sessions per host, and display the configured Security Policies. Specify from which zone packets come and to which zone packets travel to display only the policies specific to the selected direction. Note the following.

- Besides configuring the Security Policy, you also need to configure NAT rules to allow computers on the WAN to access LAN devices.
- The USG applies NAT (Destination NAT) settings before applying the Security Policies. So for example, if you configure a NAT entry that sends WAN traffic to a LAN IP address, when you configure a corresponding Security Policy to allow the traffic, you need to set the LAN IP address as the destination.
- The ordering of your policies is very important as policies are applied in sequence.

The following screen shows the Security Policy summary screen.

Figure 215 Configuration > Security Policy > Policy Control



The following table describes the labels in this screen.

Table 126 Configuration > Security Policy > Policy Control

LABEL	DESCRIPTION
Show Filter/Hide Filter	Click Show Filter to display IPv4 and IPv6 (if enabled) security policy search filters.
IPv4 / IPv6 Configuration	Use IPv4 / IPv6 search filters to find specific IPv4 and IPv6 (if enabled) security policies based on direction, application, user, source, destination and/or schedule.
From / To	Select a zone to view all security policies from a particular zone and/or to a particular zone. any means all zones.
IPv4 / IPv6 Source	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 source address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address: 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.

Table 126 Configuration > Security Policy > Policy Control (continued)

LABEL	DESCRIPTION
IPv4 / IPv6 Destination	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 destination address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address: 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.
Service	View all security policies based the service object used.
User	View all security policies based on user or user group object used.
Schedule	View all security policies based on the schedule object used.
General Settings	Enable or disable the Security Policy feature on the USG.
Enable Policy Control	Select this to activate Security Policy on the USG to perform access control.
IPv4/IPv6 Policy Management	Use the following items to manage IPv4 and IPv6 policies.
Allow Asymmetrical Route	If an alternate gateway on the LAN has an IP address in the same subnet as the USG's LAN IP address, return traffic may not go through the USG. This is called an asymmetrical or "triangle" route. This causes the USG to reset the connection, as the connection has not been acknowledged. Select this check box to have the USG permit the use of asymmetrical route topology on the network (not reset the connection). Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the USG. A better solution is to use virtual interfaces to put the USG and the backup gateway on separate subnets.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	To change a policy's position in the numbered list, select the policy and click Move to display a field to type a number for where you want to put that policy and press [ENTER] to move the policy to the number that you typed. The ordering of your policies is important as they are applied in order of their numbering.
Clone	Use Clone to create a new entry by modifying an existing one. • Select an existing entry. • Click Clone, type a number where the new entry should go and then press [ENTER]. • A configuration copy of the selected entry pops up. You must at least change the name as duplicate entry names are not allowed.
The following read-only fields summarize the policies you have created that apply to traffic traveling in the selected packet direction.	
Priority	This is the position of your Security Policy in the global policy list (including all through-USG and to-USG policies). The ordering of your policies is important as policies are applied in sequence. Default displays for the default Security Policy behavior that the USG performs on traffic that does not match any other Security Policy.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.

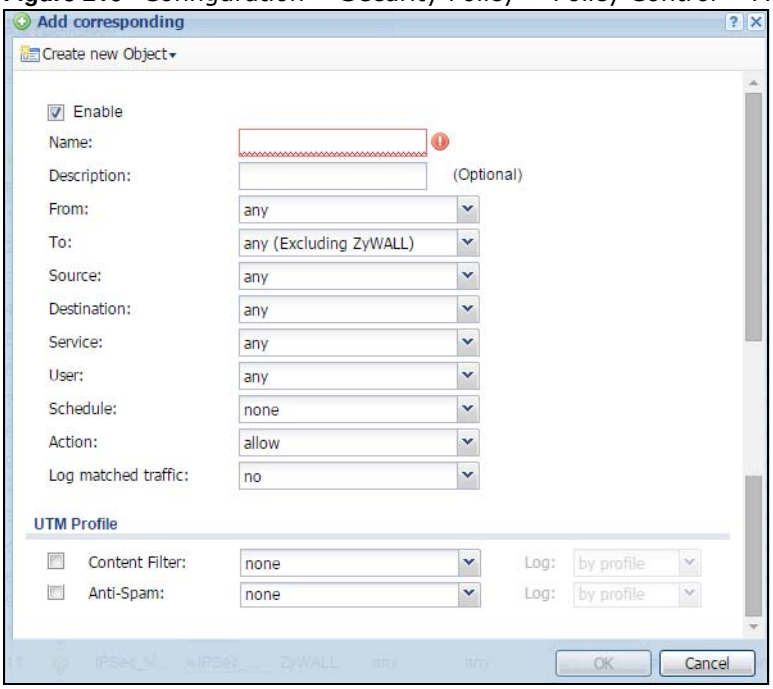
Table 126 Configuration > Security Policy > Policy Control (continued)

LABEL	DESCRIPTION
Name	This is the name of the Security policy.
From / To	This is the direction of travel of packets. Select from which zone the packets come and to which zone they go. Security Policies Rare grouped based on the direction of travel of packets to which they apply. For example, from LAN to LAN means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN. From any displays all the Security Policies for traffic going to the selected To Zone. To any displays all the Security Policies for traffic coming from the selected From Zone. From any to any displays all of the Security Policies. To ZyWALL policies are for traffic that is destined for the USG and control which computers can manage the USG.
IPv4 / IPv6 Source	This displays the IPv4 / IPv6 source address object to which this Security Policy applies.
IPv4 / IPv6 Destination	This displays the IPv4 / IPv6 destination address object to which this Security Policy applies.
Service	This displays the service object to which this Security Policy applies.
User	This is the user name or user group name to which this Security Policy applies.
Schedule	This field tells you the schedule object that the policy uses. none means the policy is active at all times if enabled.
Action	This field displays whether the Security Policy silently discards packets without notification (deny), permits the passage of packets (allow) or drops packets with notification (reject)
UTM Profile	This field shows you which UTM profiles (content filter, anti-spam) apply to this Security policy. Click an applied UTM profile icon to edit the profile directly.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

20.4.2 The Security Policy Control Add/Edit Screen

In the Security Policy Control screen, click the Edit or Add icon to display the Security Policy Edit or Add screen.

Figure 216 Configuration > Security Policy > Policy Control > Add



The following table describes the labels in this screen.

Table 127 Configuration > Security Policy > Policy Control > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable	Select this check box to activate the Security policy.
Name	Type a name to identify the policy
Description	Enter a descriptive name of up to 60 printable ASCII characters for the Policy. Spaces are allowed.
From To	For through-USG policies, select the direction of travel of packets to which the policy applies. any means all interfaces. Device means packets destined for the USG itself.
Source	Select an IPv4 / IPv6 address or address group object to apply the policy to traffic coming from it. Select any to apply the policy to all traffic coming from IPv4 / IPv6 addresses.
Destination	Select an IPv4 / IPv6 address or address group to apply the policy to traffic going to it. Select any to apply the policy to all traffic going to IPv4 / IPv6 addresses.
Service	Select a service or service group from the drop-down list box.
User	This field is not available when you are configuring a to-USG policy. Select a user name or user group to which to apply the policy. The Security Policy is activated only when the specified user logs into the system and the policy will be disabled when the user logs out. Otherwise, select any and there is no need for user logging. Note: If you specified a source IP address (group) instead of **any** in the field below, the user's IP address should be within the IP address range.
Schedule	Select a schedule that defines when the policy applies. Otherwise, select none and the policy is always effective.

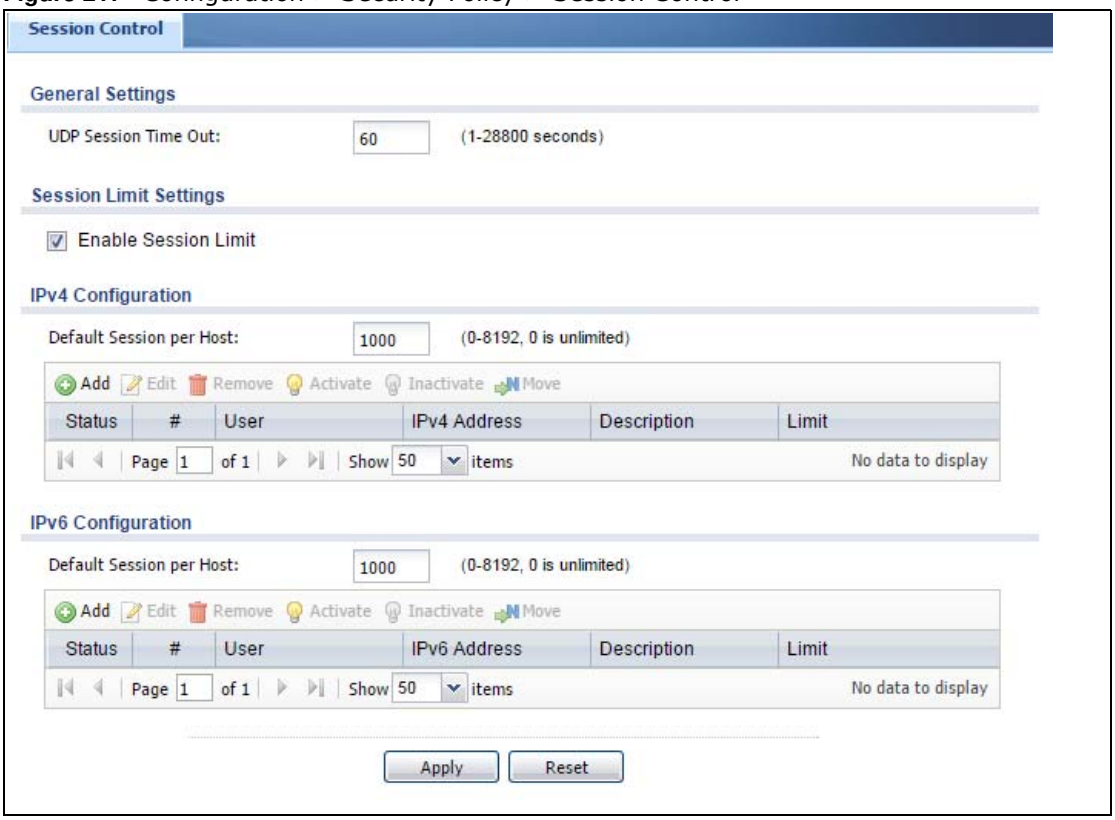
Table 127 Configuration > Security Policy > Policy Control > Add (continued)

LABEL	DESCRIPTION
Action	Use the drop-down list box to select what the Security Policy is to do with packets that match this policy. Select deny to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select reject to discard the packets and send a TCP reset packet or an ICMP destination-unreachable message to the sender. Select allow to permit the passage of the packets.
Log matched traffic	Select whether to have the USG generate a log (log), log and alert (log alert) or not (no) when the policy is matched to the criteria listed above..
UTM Profile	Use this section to apply anti- x profiles (created in the Configuration > UTM Profile screens) to traffic that matches the criteria above. You must have created a profile first; otherwise none displays. Use Log to generate a log (log), log and alert (log alert) or not (no) for all traffic that matches criteria in the profile.
Content Filter	Select a Content Filter profile from the list box; none displays if no profiles have been created in the Configuration > UTM Profile > Content Filter screen.
Anti-Spam	Select an Anti-Spam profile from the list box; none displays if no profiles have been created in the Configuration > UTM Profile > Anti-Spam screen.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

20.5 The Session Control Screen

Click Configuration > Security Policy > Session Control to display the Security Policy Session Control screen. Use this screen to limit the number of concurrent NAT/Security Policy sessions a client can use. You can apply a default limit for all users and individual limits for specific users, addresses, or both. The individual limit takes priority if you apply both.

Figure 217 Configuration > Security Policy > Session Control



The following table describes the labels in this screen.

Table 128 Configuration > Security Policy > Session Control

LABEL	DESCRIPTION
General Settings	
UDP Session Time Out	Set how many seconds the USG will allow a UDP session to remain idle (without UDP traffic) before closing it.
Session Limit Settings	
Enable Session limit	Select this check box to control the number of concurrent sessions hosts can have.
IPv4 / IPv6 Rule Summary	This table lists the rules for limiting the number of concurrent sessions hosts can have.
Default Session per Host	This field is configurable only when you enable session limit. Use this field to set a common limit to the number of concurrent NAT/Security Policy sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions. Create rules below to apply other limits for specific users or addresses.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.

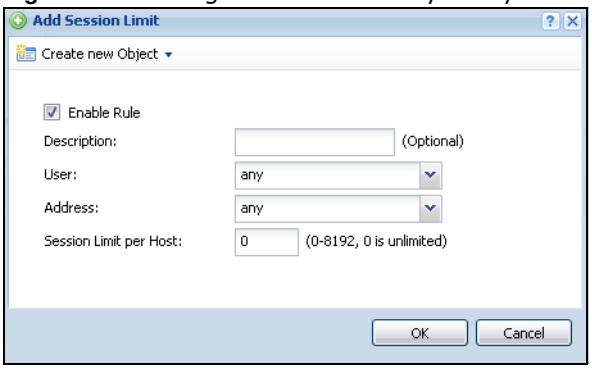
Table 128 Configuration > Security Policy > Session Control (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the index number of a session limit rule. It is not associated with a specific rule.
User	This is the user name or user group name to which this session limit rule applies.
IPv4 / IPv6 Address	This is the IPv4 / IPv6 address object to which this session limit rule applies.
Description	This is the information configured to help you identify the rule.
Limit	This is how many concurrent sessions this user or address is allowed to have.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

20.5.1 The Session Control Add/Edit Screen

Click Configuration > Security Policy > Session Control and the Add or Edit icon to display the Add or Edit screen. Use this screen to configure rules that define a session limit for specific users or addresses.

Figure 218 Configuration > Security Policy > Session Control > Edit



The following table describes the labels in this screen.

Table 129 Configuration > Security Policy > Session Control > Add / Edit

LABEL	DESCRIPTION
Create new Object	Use to configure new settings for User or Address objects that you need to use in this screen.Click on the down arrow to see the menu.
Enable Rule	Select this check box to turn on this session limit rule.
Description	Enter information to help you identify this rule. Use up to 60 printable ASCII characters. Spaces are allowed.

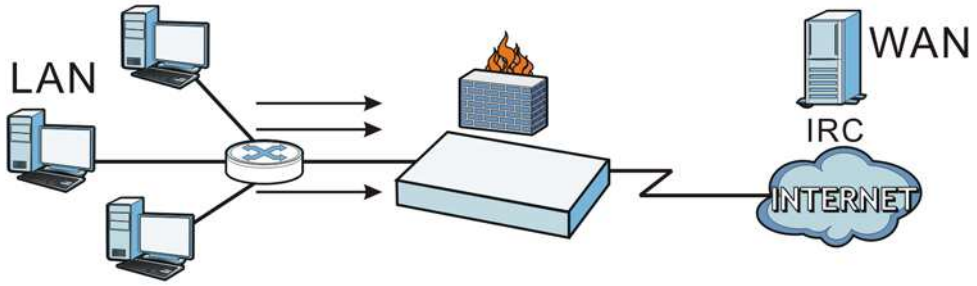
Table 129 Configuration > Security Policy > Session Control > Add / Edit (continued)

LABEL	DESCRIPTION
User	Select a user name or user group to which to apply the rule. The rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out. Otherwise, select any and there is no need for user logging. Note: If you specified an IP address (or address group) instead of **any** in the field below, the user's IP address should be within the IP address range.
Address	Select the IPv4 source address or address group to which this rule applies. Select any to apply the rule to all IPv4 source addresses.
IPv6 Address	Select the IPv6 source address or address group to which this rule applies. Select any to apply the rule to all IPv6 source addresses.
Session Limit per Host	Use this field to set a limit to the number of concurrent NAT/Security Policy sessions this rule's users or addresses can have. For this rule's users and addresses, this setting overrides the Default Session per Host setting in the general Security Policy Session Control screen.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

20.6 Security Policy Example Applications

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

Figure 219 Blocking All LAN to WAN IRC Traffic Example



Your Security Policy would have the following settings.

Table 130 Blocking All LAN to WAN IRC Traffic Example

#	USER	SOURCE	DESTINATION	SCHEDULE	UTM PROFILE	ACTION
1	Any	Any	Any	Any	IRC	Deny
2	Any	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the Security Policy's default policy that allows all LAN1 to WAN traffic.

The USG applies the security policies in order. So for this example, when the USG receives traffic from the LAN, it checks it against the first policy. If the traffic matches (if it is IRC traffic) the security policy takes the action in the policy (drop) and stops checking the subsequent security policies. Any traffic that does not match the first security policy will match the second security policy and the USG forwards it.

Now suppose you need to let the CEO use IRC. You configure a LAN1 to WAN security policy that allows IRC traffic from the IP address of the CEO's computer. You can also configure a LAN to WAN policy that allows IRC traffic from any computer through which the CEO logs into the USG with his/her user name. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

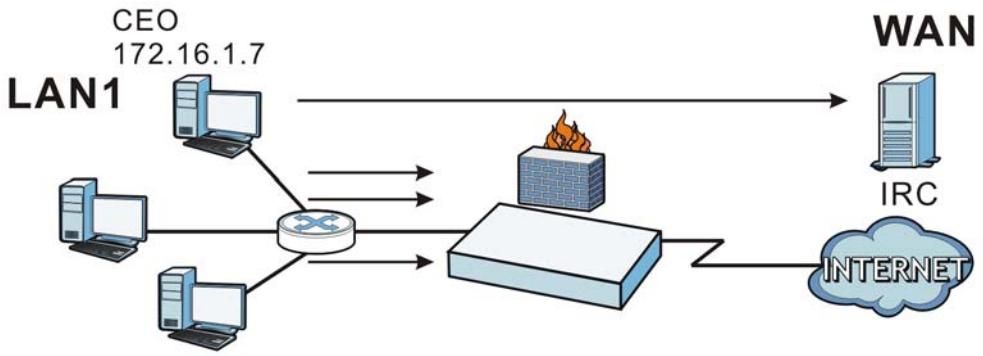
- Has a static IP address,

  or

- You configure a static DHCP entry for it so the USG always assigns it the same IP address.

Now you configure a LAN1 to WAN security policy that allows IRC traffic from the IP address of the CEO's computer (172.16.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the security policy to always be in effect. The following figure shows the results of your two custom policies.

Figure 220 Limited LAN to WAN IRC Traffic Example



Your security policy would have the following configuration.

Table 131 Limited LAN1 to WAN IRC Traffic Example 1

#	USER	SOURCE	DESTINATION	SCHEDULE	UTM PROFILE	ACTION
1	Any	172.16.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows the LAN1 computer at IP address 172.16.1.7 to access the IRC service on the WAN.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the default policy of allowing all traffic from the LAN1 to go to the WAN.

Alternatively, you configure a LAN1 to WAN policy with the CEO's user name (say CEO) to allow IRC traffic from any source IP address to go to any destination address.

Your Security Policy would have the following settings.

Table 132 Limited LAN1 to WAN IRC Traffic Example 2

#	USER	SOURCE	DESTINATION	SCHEDULE	UTM PROFILE	ACTION
1	CEO	Any	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows any LAN1 computer to access the IRC service on the WAN by logging into the USG with the CEO's user name.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the default policy of allowing allows all traffic from the LAN1 to go to the WAN.

The policy for the CEO must come before the policy that blocks all LAN1 to WAN IRC traffic. If the policy that blocks all LAN1 to WAN IRC traffic came first, the CEO's IRC traffic would match that policy and the USG would drop it and not check any other security policies.

21

IPSec VPN

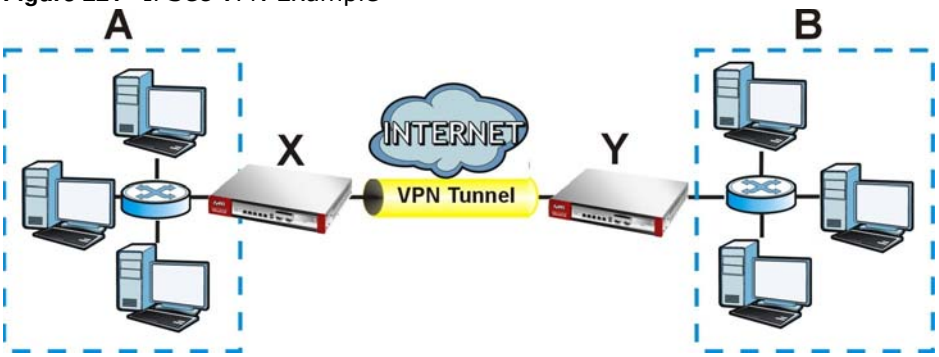
21.1 Virtual Private Networks (VPN) Overview

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

IPSec VPN

Internet Protocol Security (IPSec) VPN connects IPSec routers or remote users using IPSec client software. This standards-based VPN offers flexible solutions for secure data communications across a public network. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The USG can also combine multiple IPSec VPN connections into one secure network. Here local USG X uses an IPSec VPN tunnel to remote (peer) USG Y to connect the local (A) and remote (B) networks.

Figure 221 IPSec VPN Example



Internet Key Exchange (IKE): IKEv1 and IKEv2

The USG supports IKEv1 and IKEv2 for IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely.

IKE uses certificates or pre-shared keys for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which encryption keys are derived. A security policy for each peer must be manually created.

IPSec VPN consists of two phases: Phase 1 and Phase 2. Phase 1's purpose is to establish a secure authenticated communication channel by using the Diffie–Hellman key exchange algorithm to generate a shared secret key to encrypt IKE communications. This negotiation results in one single bi-directional ISAKMP Security Association (SA). The authentication can be performed using either pre-shared key (shared secret), signatures, or public key encryption. Phase 1 operates in either

Main Mode or Aggressive Mode. Main Mode protects the identity of the peers, but Aggressive Mode does not.

During Phase 2, the remote IPSec routers use the secure channel established in Phase 1 to negotiate Security Associations for IPsec. The negotiation results in a minimum of two unidirectional security associations (one inbound and one outbound). Phase 2 uses Quick Mode (only). Quick mode occurs after IKE has established the secure tunnel in Phase 1. It negotiates a shared IPSec policy, derives shared secret keys used for the IPSec security algorithms, and establishes IPSec SAs. Quick mode is also used to renegotiate a new IPSec SA when the IPSec SA lifetime expires.

In the USG, use the VPN Connection tab to set up Phase 2 and the VPN Gateway tab to set up Phase 1.

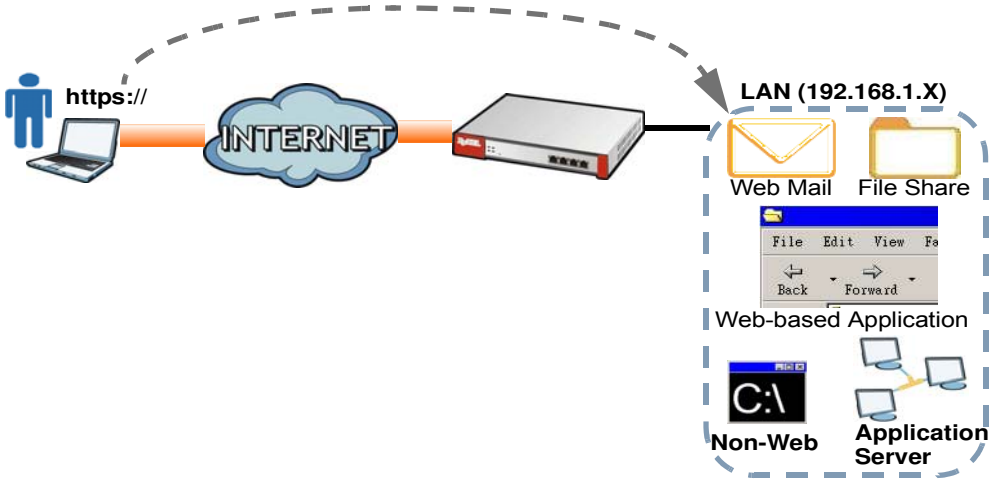
Some differences between IKEv1 and IKEv2 include:

- IKEv2 uses less bandwidth than IKEv1. IKEv2 uses one exchange procedure with 4 messages. IKEv1 uses two phases with Main Mode (9 messages) or Aggressive Mode (6 messages) in phase 1.
- IKEv2 supports Extended Authentication Protocol (EAP) authentication, and IKEv1 supports X-Auth. EAP is important when connecting to existing enterprise authentication systems.
- IKEv2 always uses NAT traversal and Dead Peer Detection (DPD), but they can be disabled in IKEv1 using USG firmware (the default is on).
- Configuration payload (includes the IP address pool in the VPN setup data) is supported in IKEv2 (off by default), but not in IKEv1.
- Narrowed (has the SA apply only to IP addresses in common between the USG and the remote IPSec router) is supported in IKEv2, but not in IKEv1.
- The IKEv2 protocol supports connectivity checks which is used to detect whether the tunnel is still up or not. If the check fails (the tunnel is down), IKEv2 can re-establish the connection automatically. The USG uses firmware to perform connectivity checks when using IKEv1.

SSL VPN

SSL VPN uses remote users' web browsers to provide the easiest-to-use of the USG's VPN solutions. A user just browses to the USG's web address and enters his user name and password to securely connect to the USG's network. Remote users do not need to configure security settings. Here a user uses his browser to securely connect to network resources in the same way as if he were part of the internal network. See Chapter 22 on page 368 for more on SSL VPN.

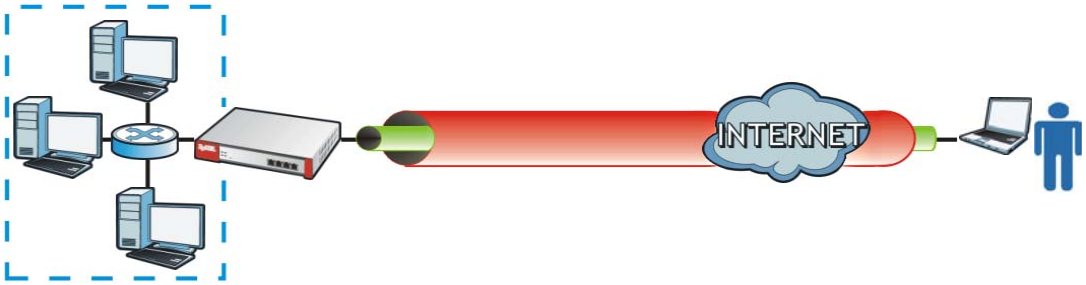
Figure 222 SSL VPN



L2TP VPN

L2TP VPN uses the L2TP and IPSec client software included in remote users' Android, iOS, or Windows operating systems for secure connections to the network behind the USG. The remote users do not need their own IPSec gateways or third-party VPN client software. For example, configure sales representatives' laptops, tablets, or smartphones to securely connect to the USG's network. See Chapter 25 on page 396 for more on L2TP over IPSec.

Figure 223 L2TP VPN



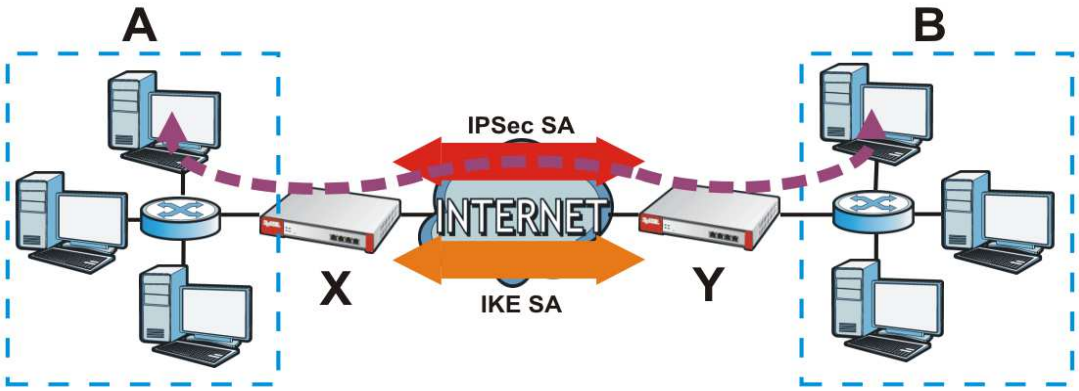
21.1.1 What You Can Do in this Chapter

- Use the VPN Connection screens (see Section 21.2 on page 338) to specify which IPSec VPN gateway an IPSec VPN connection policy uses, which devices behind the IPSec routers can use the VPN tunnel, and the IPSec SA settings (phase 2 settings). You can also activate or deactivate and connect or disconnect each VPN connection (each IPSec SA).
- Use the VPN Gateway screens (see Section 21.2.1 on page 339) to manage the USG's VPN gateways. A VPN gateway specifies the IPSec routers at either end of a VPN tunnel and the IKE SA settings (phase 1 settings). You can also activate and deactivate each VPN gateway.
- Use the VPN Concentrator screens (see Section 21.4 on page 354) to combine several IPSec VPN connections into a single secure network.
- Use the Configuration Provisioning screen (see Section 21.5 on page 356) to set who can retrieve VPN rule settings from the USG using the USG IPSec VPN Client.

21.1.2 What You Need to Know

An IPSec VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the USG and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the USG and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the USG and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 224 VPN: IKE SA and IPSec SA

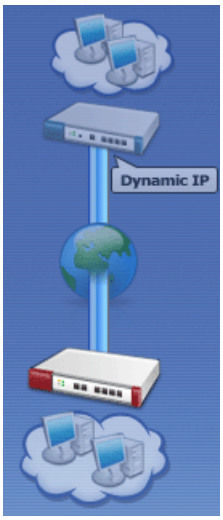


In this example, a computer in network A is exchanging data with a computer in network B. Inside networks A and B, the data is transmitted the same way data is normally transmitted in the networks. Between routers X and Y, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers X and Y established the IKE SA first.

Application Scenarios

The USG's application scenarios make it easier to configure your VPN connection settings.

Table 133 IPSec VPN Application Scenarios

SITE-TO-SITE	SITE-TO-SITE WITH DYNAMIC PEER	REMOTE ACCESS (SERVER ROLE)	REMOTE ACCESS (CLIENT ROLE)
			
Choose this if the remote IPSec router has a static IP address or a domain name. This USG can initiate the VPN tunnel. The remote IPSec router can also initiate the VPN tunnel if this USG has a static IP address or a domain name.	Choose this if the remote IPSec router has a dynamic IP address. You don't specify the remote IPSec router's address, but you specify the remote policy (the addresses of the devices behind the remote IPSec router). This USG must have a static IP address or a domain name. Only the remote IPSec router can initiate the VPN tunnel.	Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. You don't specify the addresses of the client IPSec routers or the remote policy. This creates a dynamic IPSec VPN rule that can let multiple clients connect. Only the clients can initiate the VPN tunnel.	Choose this to connect to an IPSec server. This USG is the client (dial-in user). Client role USGs initiate IPSec VPN connections to a server role USG. This USG can have a dynamic IP address. The IPSec server doesn't configure this USG's IP address or the addresses of the devices behind it. Only this USG can initiate the VPN tunnel.

Finding Out More

- See Section 21.6 on page 358 for IPSec VPN background information.
- See the help in the IPSec VPN quick setup wizard screens.

21.1.3 Before You Begin

This section briefly explains the relationship between VPN tunnels and other features. It also gives some basic suggestions for troubleshooting.

You should set up the following features before you set up the VPN tunnel.

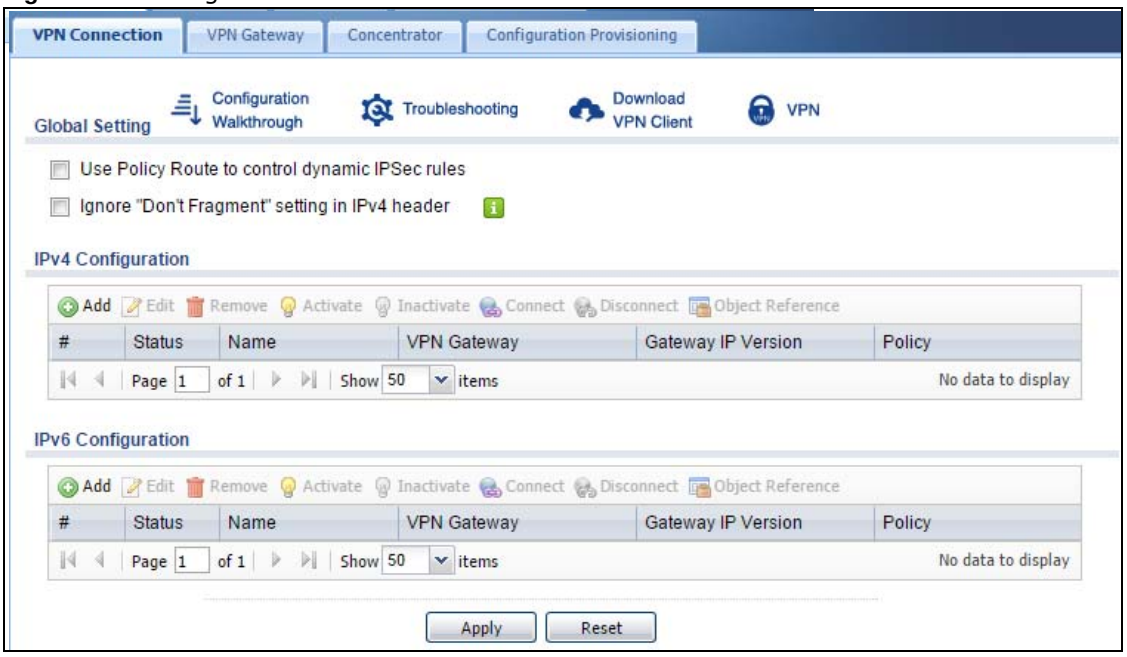
- In any VPN connection, you have to select address objects to specify the local policy and remote policy. You should set up the address objects first.
- In a VPN gateway, you can select an Ethernet interface, virtual Ethernet interface, VLAN interface, or virtual VLAN interface to specify what address the USG uses as its IP address when it establishes the IKE SA. You should set up the interface first.
- In a VPN gateway, you can enable extended authentication. If the USG is in server mode, you should set up the authentication method (AAA server) first. The authentication method specifies how the USG authenticates the remote IPSec router.
- In a VPN gateway, the USG and remote IPSec router can use certificates to authenticate each other. Make sure the USG and the remote IPSec router will trust each other's certificates.

21.2 The VPN Connection Screen

Click Configuration > VPN > IPSec VPN to open the VPN Connection screen. The VPN Connection screen lists the VPN connection policies and their associated VPN gateway(s), and various settings. In addition, it also lets you activate or deactivate and connect or disconnect each VPN connection (each IPSec SA). Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Click on the icons to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting and other information.

Figure 225 Configuration > VPN > IPSec VPN > VPN Connection



Each field is discussed in the following table.

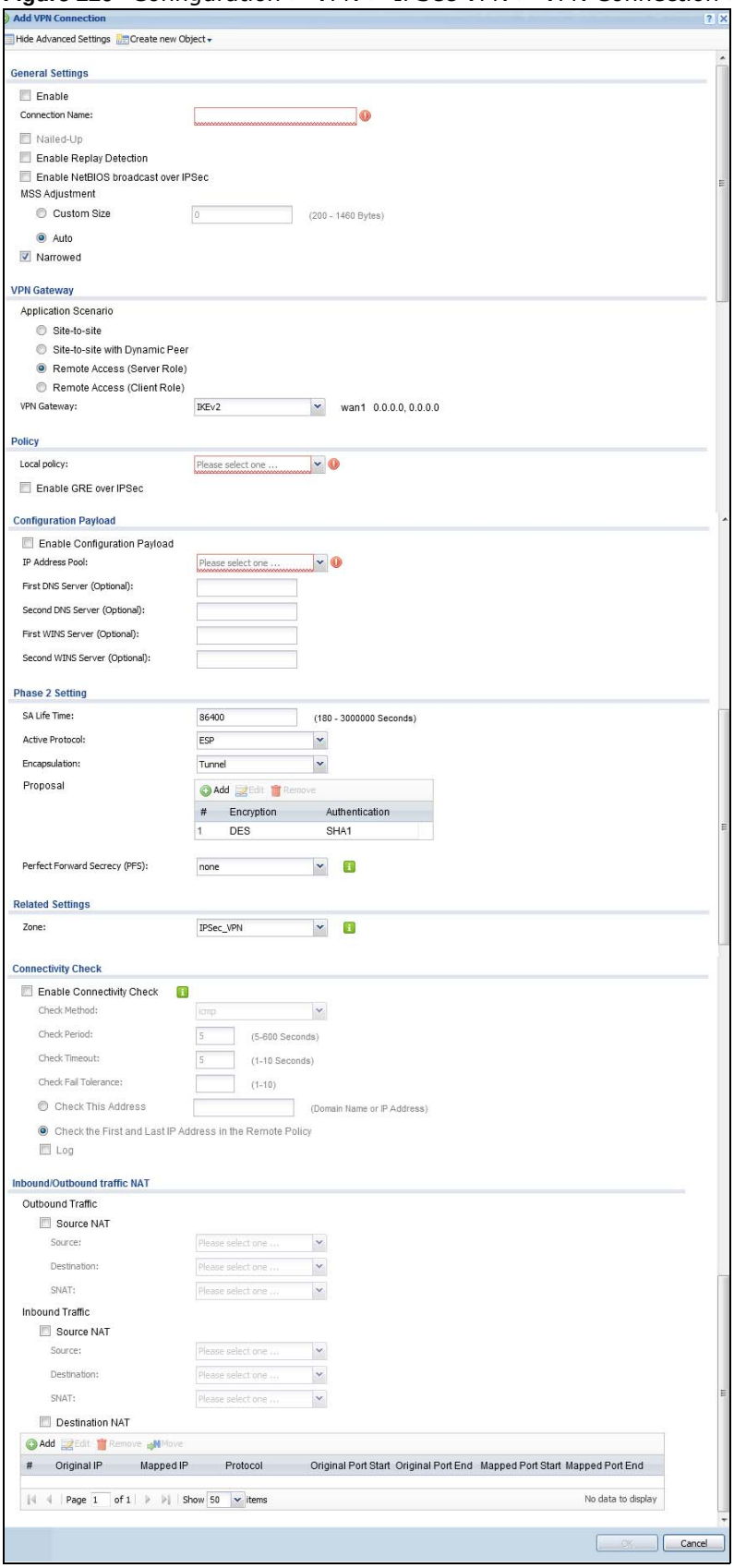
Table 134 Configuration > VPN > IPSec VPN > VPN Connection

LABEL	DESCRIPTION
Global Setting	The following two fields are for all IPSec VPN policies. Click on the VPN icon to go to the ZyXEL VPN Client product page at the ZyXEL website.
Use Policy Route to control dynamic IPSec rules	Select this to be able to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must manually create these policy routes. The USG automatically obtains source and destination addresses for dynamic IPSec rules that do not match any of the policy routes. Clear this to have the USG automatically obtain source and destination addresses for all dynamic IPSec rules.
Ignore "Don't Fragment" setting in packet header	Select this to fragment packets larger than the MTU (Maximum Transmission Unit) that have the "Don't Fragment" bit in the IP header turned on. When you clear this the USG drops packets larger than the MTU that have the "Don't Fragment" bit in the header turned on.
IPv4 / IPv6 Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Connect	To connect an IPSec SA, select it and click Connect.
Disconnect	To disconnect an IPSec SA, select it and click Disconnect.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with a specific connection.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the IPSec SA.
VPN Gateway	This field displays the VPN gateway in use for this VPN connection.
Gateway IP Version	This field displays what IP version the associated VPN gateway(s) is using. An IPv4 gateway may use an IKEv1 or IKEv2 SA. An IPv6 gateway may use IKEv2 only.
Policy	This field displays the local policy and the remote policy, respectively.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

21.2.1 The VPN Connection Add/Edit (IKE) Screen

The VPN Connection Add/ Edit Gateway screen allows you to create a new VPN connection policy or edit an existing one. To access this screen, go to the Configuration > VPN Connection screen (see Section 21.2 on page 338), and click either the Add icon or an Edit icon.

Figure 226 Configuration > VPN > IPSec VPN > VPN Connection > Edit (IKE)



Each field is described in the following table.

Table 135 Configuration > VPN > IPSec VPN > VPN Connection > Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
General Settings	
Enable	Select this check box to activate this VPN connection.
Connection Name	Type the name used to identify this IPSec SA. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Nailed-Up	Select this if you want the USG to automatically renegotiate the IPSec SA when the SA life time expires.
Enable Replay Detection	Select this check box to detect and reject old or duplicate packets to protect against Denial-of-Service attacks.
Enable NetBIOS Broadcast over IPSec	Select this check box if you the USG to send NetBIOS (Network Basic Input/Output System) packets through the IPSec SA. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through IPSec SAs in order to allow local computers to find computers on the remote network and vice versa.
MSS Adjustment	Select Custom Size to set a specific number of bytes for the Maximum Segment Size (MSS) meaning the largest amount of data in a single TCP segment or IP datagram for this VPN connection. Some VPN clients may not be able to use a custom MSS size if it is set too small. In that case those VPN clients will ignore the size set here and use the minimum size that they can use. Select Auto to have the USG automatically set the MSS for this VPN connection.
Narrowed	If the IP range on the USG (local policy) and the local IP range on the remote IPSec router overlap in an IKEv2 SA, then you may select Narrowed to have the SA only apply to the IP addresses in common. Here are some examples. USG (local policy) Remote IPSec router IKEv2 SA-1 192.168.20.0/24 192.168.20.1 ~ 192.168.20.20 Narrowed 192.168.20.1 ~ 192.168.20.20 IKEv2 SA- 2 192.168.30.50 ~ 192.168.30.70 192.168.30.60 ~ 192.168.30.80 Narrowed 192.168.30.60 ~ 192.168.30.70
VPN Gateway	
Application Scenario	Select the scenario that best describes your intended VPN connection. Site-to-site - Choose this if the remote IPSec router has a static IP address or a domain name. This USG can initiate the VPN tunnel. Site-to-site with Dynamic Peer - Choose this if the remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. Remote Access (Server Role) - Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel. Remote Access (Client Role) - Choose this to connect to an IPSec server. This USG is the client (dial-in user) and can initiate the VPN tunnel.

Table 135 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
VPN Gateway	Select the VPN gateway this VPN connection is to use or select Create Object to add another VPN gateway for this VPN connection to use.
Policy	
Local Policy	Select the address corresponding to the local network. Use Create new Object if you need to configure a new one.
Remote Policy	Select the address corresponding to the remote network. Use Create new Object if you need to configure a new one.
Enable GRE over IPSec	Select this to allow traffic using the Generic Routing Encapsulation (GRE) tunneling protocol through an IPSec tunnel.
Policy Enforcement	Clear this to allow traffic with source and destination IP addresses that do not match the local and remote policy to use the VPN tunnel. Leave this cleared for free access between the local and remote networks. Selecting this restricts who can use the VPN tunnel. The USG drops traffic with source and destination IP addresses that do not match the local and remote policy.
Configuration Payload	This is only available when you have created an IKEv2 Gateway and are using Remote Access (Server Role).
Enable Configuration Payload	Select this to have at least have the IP address pool included in the VPN setup data.
IP Address Pool:	Select an address object from the drop-down list box.
First DNS Server (optional)	The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The USG uses these (in the order you specify here) to resolve domain names for VPN. Enter a DNS server's IP address.
Second DNS Server (Optional)	Enter a secondary DNS server's IP address that is checked if the first one is unavailable.
First WINS Server (Optional)	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Second WINS Server (Optional)	Enter a secondary WINS server's IP address that is checked if the first one is unavailable.
Phase 2 Settings	
SA Life Time	Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The USG automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Active Protocol	Select which protocol you want to use in the IPSec SA. Choices are: AH (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select AH, you must select an Authentication algorithm. ESP (RFC 2406) - provides encryption and the same services offered by AH, but its authentication is weaker. If you select ESP, you must select an Encryption algorithm and Authentication algorithm. Both AH and ESP increase processing requirements and latency (delay). The USG and remote IPSec router must use the same active protocol.
Encapsulation	Select which type of encapsulation the IPSec SA uses. Choices are Tunnel - this mode encrypts the IP header information and the data. Transport - this mode only encrypts the data. The USG and remote IPSec router must use the same encapsulation.

Table 135 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the USG accepts from the remote IPSec router for negotiating the IPSec SA.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	This field is applicable when the Active Protocol is ESP. Select which key size and encryption algorithm to use in the IPSec SA. Choices are: NULL - no encryption key or algorithm DES - a 56-bit key with the DES encryption algorithm 3DES - a 168-bit key with the DES encryption algorithm AES128 - a 128-bit key with the AES encryption algorithm AES192 - a 192-bit key with the AES encryption algorithm AES256 - a 256-bit key with the AES encryption algorithm The USG and the remote IPSec router must both have at least one proposal that uses use the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are SHA1, SHA256, SHA512 and MD5. SHA is generally considered stronger than MD5, but it is also slower. The USG and the remote IPSec router must both have a proposal that uses the same authentication algorithm.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: none - disable PFS DH1 - enable PFS and use a 768-bit random number DH2 - enable PFS and use a 1024-bit random number DH5 - enable PFS and use a 1536-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. PFS is ignored in initial IKEv2 authentication but is used when reauthenticating.
Related Settings	
Zone	Select the security zone into which to add this VPN connection policy. Any security rules or settings configured for the selected zone apply to this VPN connection policy.
Connectivity Check	The USG can regularly check the VPN connection to the gateway you specified to make sure it is still available.
Enable Connectivity Check	Select this to turn on the VPN connection check.

Table 135 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
Check Method	Select how the USG checks the connection. The peer must be configured to respond to the method you select. Select icmp to have the USG regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings. Select tcp to have the USG regularly perform a TCP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP connection.
Check Port	This field displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures allowed before the USG disconnects the VPN tunnel. The USG resumes using the first peer gateway address when the VPN connection passes the connectivity check.
Check this Address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check the First and Last IP Address in the Remote Policy	Select this to have the USG check the connection to the first and last IP addresses in the connection's remote policy. Make sure one of these is the peer gateway's LAN IP address.
Log	Select this to have the USG generate a log every time it checks this VPN connection.
Inbound/Outbound traffic NAT	
Outbound Traffic	
Source NAT	This translation hides the source address of computers in the local network. It may also be necessary if you want the USG to route packets from computers outside the local network through the IPSec SA.
Source	Select the address object that represents the original source address (or select Create Object to configure a new one). This is the address object for the computer or network outside the local network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination	Select the address object that represents the original destination address (or select Create Object to configure a new one). This is the address object for the remote network.
SNAT	Select the address object that represents the translated source address (or select Create Object to configure a new one). This is the address object for the local network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Inbound Traffic	
Source NAT	This translation hides the source address of computers in the remote network.
Source	Select the address object that represents the original source address (or select Create Object to configure a new one). This is the address object for the remote network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination	Select the address object that represents the original destination address (or select Create Object to configure a new one). This is the address object for the local network.

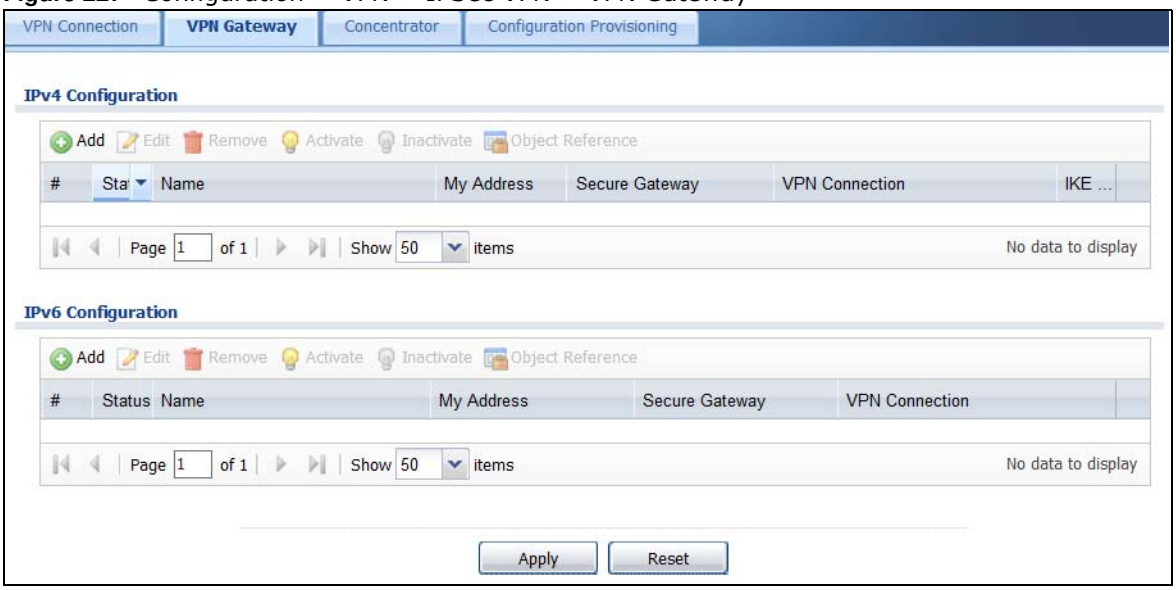
Table 135 Configuration > VPN > IPSec VPN > VPN Connection > Edit (continued)

LABEL	DESCRIPTION
SNAT	Select the address object that represents the translated source address (or select Create Object to configure a new one). This is the address that hides the original source address. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination NAT	This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Move	To change an entry's position in the numbered list, select it and click Move to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
#	This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed.
Original IP	Select the address object that represents the original destination address. This is the address object for the remote network.
Mapped IP	Select the address object that represents the desired destination address. For example, this is the address object for the mail server.
Protocol	Select the protocol required to use this translation. Choices are: TCP, UDP, or All.
Original Port Start / Original Port End	These fields are available if the protocol is TCP or UDP. Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Mapped Port Start / Mapped Port End	These fields are available if the protocol is TCP or UDP. Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard all changes and return to the main VPN screen.

21.3 The VPN Gateway Screen

The VPN Gateway summary screen displays the IPSec VPN gateway policies in the USG, as well as the USG's address, remote IPSec router's address, and associated VPN connections for each one. In addition, it also lets you activate and deactivate each VPN gateway. To access this screen, click Configuration > VPN > Network > IPSec VPN > VPN Gateway. The following screen appears.

Figure 227 Configuration > VPN > IPSec VPN > VPN Gateway



Each field is discussed in the following table. See Section 21.3.1 on page 347 for more information.

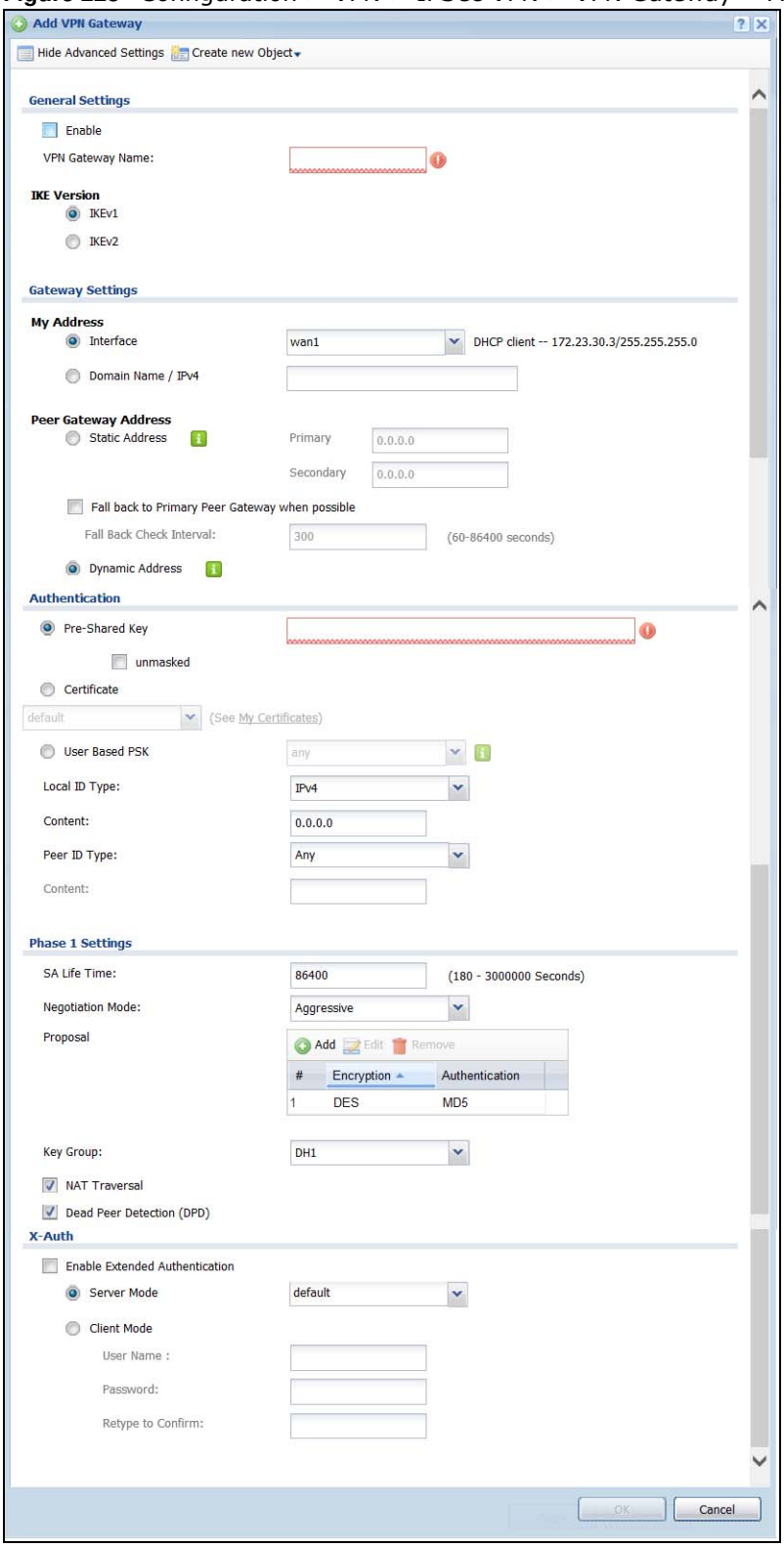
Table 136 Configuration > VPN > IPSec VPN > VPN Gateway

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry. See Section 9.3.2 on page 164 for an example.
#	This field is a sequential value, and it is not associated with a specific VPN gateway.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the VPN gateway
My address	This field displays the interface or a domain name the USG uses for the VPN gateway.
Secure Gateway	This field displays the IP address(es) of the remote IPSec routers.
VPN Connection	This field displays VPN connections that use this VPN gateway.
IKE Version	This field displays whether the gateway is using IKEv1 or IKEv2. IKEv1 applies to IPv4 traffic only. IKEv2 applies to both IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely. See Section 21.1 on page 333 for more information on IKEv1 and IKEv2.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

21.3.1 The VPN Gateway Add/Edit Screen

The VPN Gateway Add/Edit screen allows you to create a new VPN gateway policy or edit an existing one. To access this screen, go to the VPN Gateway summary screen (see Section 21.3 on page 345), and click either the Add icon or an Edit icon.

Figure 228 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit



Each field is described in the following table.

Table 137 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Use to configure any new settings objects that you need to use in this screen.
General Settings	
Enable	Select this to activate the VPN Gateway policy.
VPN Gateway Name	Type the name used to identify this VPN gateway. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IKE Version	
IKEv1 / IKEv2	Select IKEv1 or IKEv2. IKEv1 applies to IPv4 traffic only. IKEv2 applies to both IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely. See Section 21.1 on page 333 for more information on IKEv1 and IKEv2.
Gateway Settings	
My Address	Select how the IP address of the USG in the IKE SA is defined. If you select Interface, select the Ethernet interface, VLAN interface, virtual Ethernet interface, virtual VLAN interface or PPPoE/PPTP interface. The IP address of the USG in the IKE SA is the IP address of the interface. If you select Domain Name / IP, enter the domain name or the IP address of the USG. The IP address of the USG in the IKE SA is the specified IP address or the IP address corresponding to the domain name. 0.0.0.0 is not generally recommended as it has the USG accept IPSec requests destined for any interface address on the USG.
Peer Gateway Address	Select how the IP address of the remote IPSec router in the IKE SA is defined. Select Static Address to enter the domain name or the IP address of the remote IPSec router. You can provide a second IP address or domain name for the USG to try if it cannot establish an IKE SA with the first one. Fall back to Primary Peer Gateway when possible: When you select this, if the connection to the primary address goes down and the USG changes to using the secondary connection, the USG will reconnect to the primary address when it becomes available again and stop using the secondary connection. Users will lose their VPN connection briefly while the USG changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection. In the Fallback Check Interval field, set how often to check if the primary address is available. Select Dynamic Address if the remote IPSec router has a dynamic IP address (and does not use DDNS).
Authentication	Note: The USG and remote IPSec router must use the same authentication method to establish the IKE SA.

Table 137 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Pre-Shared Key	Select this to have the USG and remote IPSec router use a pre-shared key (password) to identify each other when they negotiate the IKE SA. Type the pre-shared key in the field to the right. The pre-shared key can be: • alphanumeric characters or ,;.|`~!@#$%^&*()_+\{}':./<>=-" • pairs of hexadecimal (0-9, A-F) characters, preceded by "0x". Type "0x" at the beginning of a hexadecimal key. For example, "0x0123456789ABCDEF" is in hexadecimal format; "0123456789ABCDEF" is in ASCII format. If you use hexadecimal, you must enter twice as many characters since you need to enter pairs. The USG and remote IPSec router must use the same pre-shared key. Select unmasked to see the pre-shared key in readable plain text.
Certificate	Select this to have the USG and remote IPSec router use certificates to authenticate each other when they negotiate the IKE SA. Then select the certificate the USG uses to identify itself to the remote IPsec router. This certificate is one of the certificates in My Certificates. If this certificate is self-signed, import it into the remote IPsec router. If this certificate is signed by a CA, the remote IPsec router must trust that CA. Note: The IPSec routers must trust each other's certificates. The USG uses one of its Trusted Certificates to authenticate the remote IPSec router's certificate. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.
User-based PSK	User-based PSK (IKEv1 only) generates and manages separate pre-shared keys for every user. This enables multiple users, each with a unique key, to access the same VPN gateway policy with one-to-one authentication and strong encryption. Access can be denied on a per-user basis thus allowing VPN SA user-based policies. Click User-Based PSK then select a user or group object who is allowed VPN SA access using this VPN gateway policy. This is for IKEv1 only.
Local ID Type	This field is read-only if the USG and remote IPSec router use certificates to identify each other. Select which type of identification is used to identify the USG during authentication. Choices are: IPv4 or IPv6 - the USG is identified by an IP address DNS - the USG is identified by a domain name E-mail - the USG is identified by the string specified in this field
Content	This field is read-only if the USG and remote IPSec router use certificates to identify each other. Type the identity of the USG during authentication. The identity depends on the Local ID Type. IP - type an IP address; if you type 0.0.0.0, the USG uses the IP address specified in the My Address field. This is not recommended in the following situations: • There is a NAT router between the USG and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different Local ID Type. DNS - type the fully qualified domain name (FQDN). This value is only used for identification and can be any string that matches the peer ID string. E-mail - the USG is identified by the string you specify here; you can use up to 63 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.

Table 137 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Peer ID Type	Select which type of identification is used to identify the remote IPSec router during authentication. Choices are: IP - the remote IPSec router is identified by an IP address DNS - the remote IPSec router is identified by a domain name E-mail - the remote IPSec router is identified by the string specified in this field Any - the USG does not check the identity of the remote IPSec router If the USG and remote IPSec router use certificates, there is one more choice. Subject Name - the remote IPSec router is identified by the subject name in the certificate
Content	This field is disabled if the Peer ID Type is Any. Type the identity of the remote IPSec router during authentication. The identity depends on the Peer ID Type. If the USG and remote IPSec router do not use certificates, IP - type an IP address; see the note at the end of this description. DNS - type the fully qualified domain name (FQDN). This value is only used for identification and can be any string that matches the peer ID string. E-mail - the remote IPSec router is identified by the string you specify here; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. If the USG and remote IPSec router use certificates, type the following fields from the certificate used by the remote IPSec router. IP - subject alternative name field; see the note at the end of this description. DNS - subject alternative name field E-mail - subject alternative name field Subject Name - subject name (maximum 255 ASCII characters, including spaces) Note: If **Peer ID Type** is **IP**, please read the rest of this section. If you type 0.0.0.0, the USG uses the IP address specified in the Secure Gateway Address field. This is not recommended in the following situations: • There is a NAT router between the USG and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different Peer ID Type.
Phase 1 Settings	
SA Life Time (Seconds)	Type the maximum number of seconds the IKE SA can last. When this time has passed, the USG and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
Negotiation Mode	Select the negotiation mode to use to negotiate the IKE SA. Choices are Main - this encrypts the USG's and remote IPSec router's identities but takes more time to establish the IKE SA Aggressive - this is faster but does not encrypt the identities The USG and the remote IPSec router must use the same negotiation mode.
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the USG accepts from the remote IPSec router for negotiating the IKE SA.

Table 137 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: DES - a 56-bit key with the DES encryption algorithm 3DES - a 168-bit key with the DES encryption algorithm AES128 - a 128-bit key with the AES encryption algorithm AES192 - a 192-bit key with the AES encryption algorithm AES256 - a 256-bit key with the AES encryption algorithm The USG and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are SHA1, SHA256, SHA512 and MD5. SHA is generally considered stronger than MD5, but it is also slower. The remote IPSec router must use the same authentication algorithm.
Key Group	Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are: DH1 - use a 768-bit random number DH2 - use a 1024-bit random number DH5 - use a 1536-bit random number The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
NAT Traversal	Select this if any of these conditions are satisfied. • This IKE SA might be used to negotiate IPSec SAs that use ESP as the active protocol. • There are one or more NAT routers between the USG and remote IPSec router, and these routers do not support IPSec pass-thru or a similar feature. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged. This field applies for IKEv1 only. NAT Traversal is always performed when you use IKEv2.
Dead Peer Detection (DPD)	Select this check box if you want the USG to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If there has been no traffic for at least 15 seconds, the USG sends a message to the remote IPSec router. If the remote IPSec router responds, the USG transmits the data. If the remote IPSec router does not respond, the USG shuts down the IKE SA. If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check (see Section 21.2.1 on page 339). This field applies for IKEv1 only. Dead Peer Detection (DPD) is always performed when you use IKEv2.

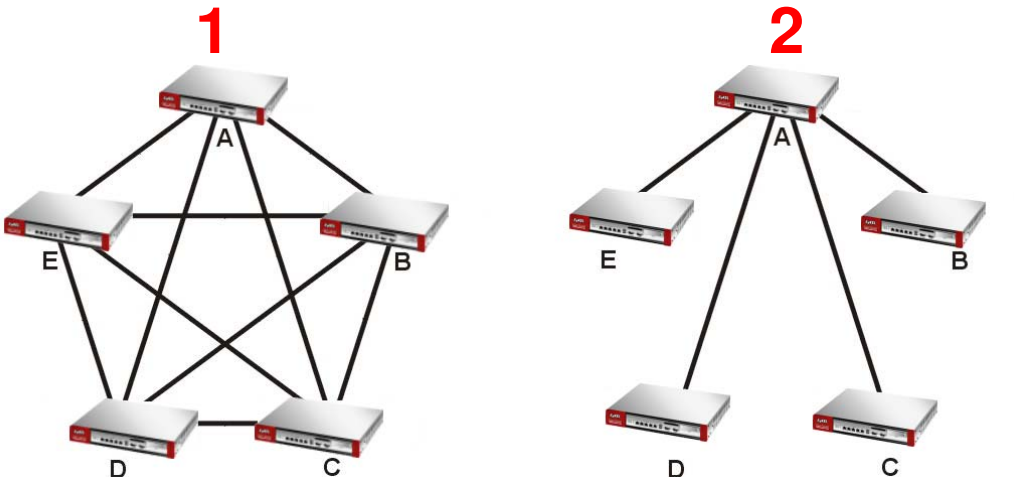
Table 137 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
X Auth / Extended Authentication Protocol	This part of the screen displays X-Auth when using IKEv1 and Extended Authentication Protocol when using IKEv2.
X-Auth	This displays when using IKEv1. When different users use the same VPN tunnel to connect to the USG (telecommuters sharing a tunnel for example), use X-auth to enforce a user name and password check. This way even though telecommuters all know the VPN tunnel's security settings, each still has to provide a unique user name and password.
Enable Extended Authentication	Select this if one of the routers (the USG or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server.
Server Mode	Select this if the USG authenticates the user name and password from the remote IPSec router. You also have to select the authentication method, which specifies how the USG authenticates this information.
Client Mode	Select this radio button if the USG provides a username and password to the remote IPSec router for authentication. You also have to provide the User Name and the Password.
User Name	This field is required if the USG is in Client Mode for extended authentication. Type the user name the USG sends to the remote IPSec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the USG is in Client Mode for extended authentication. Type the password the USG sends to the remote IPSec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Retype to Confirm	Type the exact same password again here to make sure an error was not made when typing it originally.
Extended Authentication Protocol	This displays when using IKEv2. EAP uses a certificate for authentication.
Enable Extended Authentication	Select this if one of the routers (the USG or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server or a certificate.
Server Mode	Select this if the USG authenticates the user name and password from the remote IPSec router. You also have to select an AAA method, which specifies how the USG authenticates this information and who may be authenticated (Allowed User).
Client Mode	Select this radio button if the USG provides a username and password to the remote IPSec router for authentication. You also have to provide the User Name and the Password.
User Name	This field is required if the USG is in Client Mode for extended authentication. Type the user name the USG sends to the remote IPSec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the USG is in Client Mode for extended authentication. Type the password the USG sends to the remote IPSec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Retype to Confirm	Type the exact same password again here to make sure an error was not made when typing it originally.
OK	Click OK to save your settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

21.4 VPN Concentrator

A VPN concentrator combines several IPSec VPN connections into one secure network.

Figure 229 VPN Topologies (Fully Meshed and Hub and Spoke)



In a fully-meshed VPN topology (1 in the figure), there is a VPN connection between every pair of routers. In a hub-and-spoke VPN topology (2 in the figure), there is a VPN connection between each spoke router (B, C, D, and E) and the hub router (A), which uses the VPN concentrator. The VPN concentrator routes VPN traffic between the spoke routers and itself.

A VPN concentrator reduces the number of VPN connections that you have to set up and maintain in the network. You might also be able to consolidate the policy routes in each spoke router, depending on the IP addresses and subnets of each spoke.

However a VPN concentrator is not for every situation. The hub router is a single failure point, so a VPN concentrator is not as appropriate if the connection between spoke routers cannot be down occasionally (maintenance, for example). There is also more burden on the hub router. It receives VPN traffic from one spoke, decrypts it, inspects it to find out to which spoke to route it, encrypts it, and sends it to the appropriate spoke. Therefore, a VPN concentrator is more suitable when there is a minimum amount of traffic between spoke routers.

21.4.1 VPN Concentrator Requirements and Suggestions

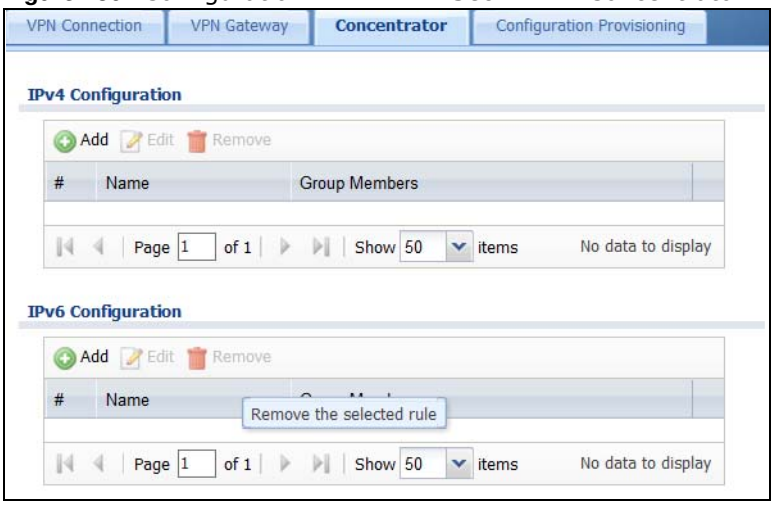
Consider the following when using the VPN concentrator.

- The local IP addresses configured in the VPN rules should not overlap.
- The concentrator must have at least one separate VPN rule for each spoke. In the local policy, specify the IP addresses of the networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule for each spoke.
- To have all Internet access from the spoke routers go through the VPN tunnel, set the VPN rules in the spoke routers to use 0.0.0.0 (any) as the remote IP address.
- Your security policies can still block VPN packets.

21.4.2 VPN Concentrator Screen

The VPN Concentrator summary screen displays the VPN concentrators in the USG. To access this screen, click Configuration > VPN > IPSec VPN > Concentrator.

Figure 230 Configuration > VPN > IPSec VPN > Concentrator



Each field is discussed in the following table. See Section 21.4.3 on page 355 for more information.

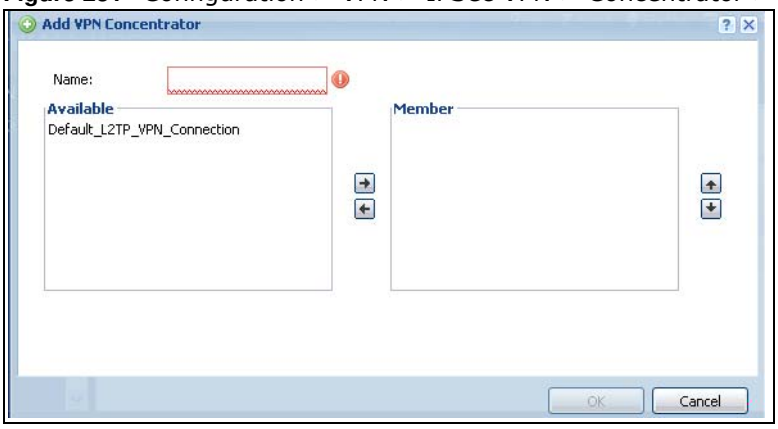
Table 138 Configuration > VPN > IPSec VPN > Concentrator

LABEL	DESCRIPTION
IPv4/IPv6 Configuration	Choose to configure for IPv4 or IPv6 traffic.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific concentrator.
Name	This field displays the name of the VPN concentrator.
Group Members	These are the VPN connection policies that are part of the VPN concentrator.

21.4.3 The VPN Concentrator Add/Edit Screen

Use the VPN Concentrator Add/Edit screen to create or edit a VPN concentrator. To access this screen, go to the VPN Concentrator summary screen (see Section 21.4 on page 354), and click either the Add icon or an Edit icon.

Figure 231 Configuration > VPN > IPSec VPN > Concentrator > Add/Edit



Each field is described in the following table.

Table 139 VPN > IPSec VPN > Concentrator > Add/Edit

LABEL	DESCRIPTION
Name	Enter the name of the concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Member	Select the concentrator's IPSec VPN connection policies. Note: You must disable policy enforcement in each member. See Section 21.2.1 on page 339. IPSec VPN connection policies that do not belong to a VPN concentrator appear under Available. Select any VPN connection policies that you want to add to the VPN concentrator and click the right arrow button to add them. The VPN concentrator's member VPN connections appear under Member. Select any VPN connections that you want to remove from the VPN concentrator, and click the left arrow button to remove them.
OK	Click OK to save your changes in the USG.
Cancel	Click Cancel to exit this screen without saving.

21.5 USG IPSec VPN Client Configuration Provisioning

Use the Configuration > VPN > IPSec VPN > Configuration Provisioning screen to configure who can retrieve VPN rule settings from the USG using the USG IPSec VPN Client. In the USG IPSec VPN Client, you just need to enter the IP address of the USG to get all the VPN rule settings automatically. You do not need to manually configure all rule settings in the USG IPSec VPN client.

VPN rules for the USG IPSec VPN Client have certain restrictions. They must *not* contain the following settings:

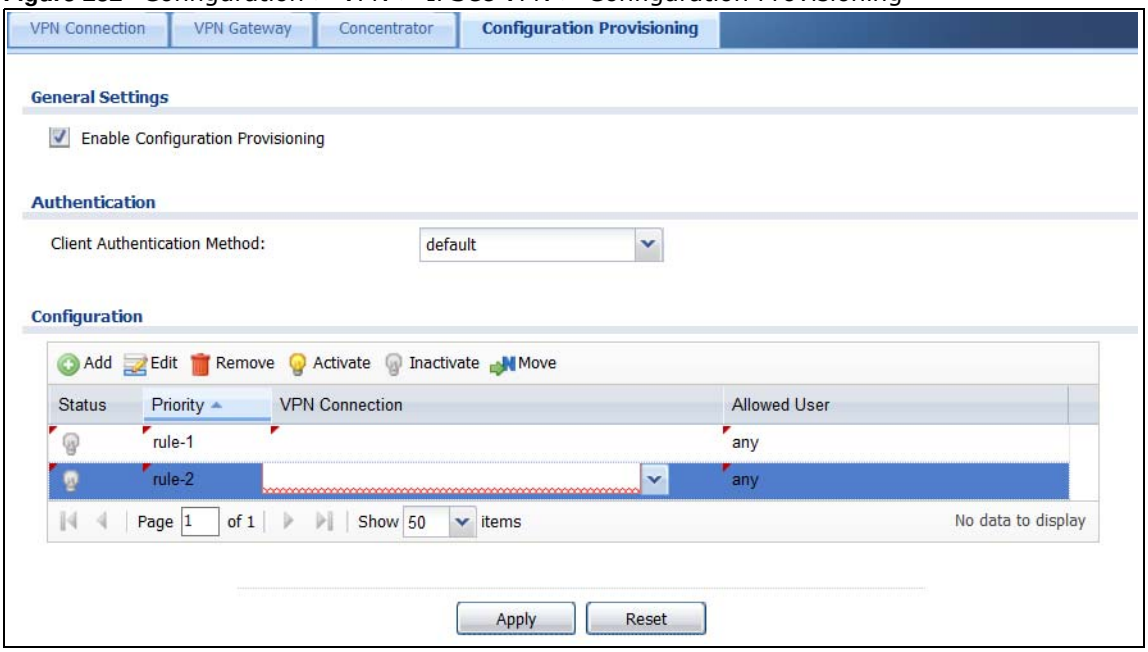
- AH active protocol
- NULL encryption
- SHA512 authentication
- A subnet or range remote policy

The following VPN Gateway rules configured on the USG cannot be provisioned to the IPSec VPN Client:

- IPv4 rules with IKEv2 version
- IPv4 rules with User-based PSK authentication
- IPv6 rules

In the USG Quick Setup wizard, you can use the VPN Settings for Configuration Provisioning wizard to create a VPN rule that will not violate these restrictions.

Figure 232 Configuration > VPN > IPSec VPN > Configuration Provisioning



Each field is discussed in the following table.

Table 140 Configuration > VPN > IPSec VPN > Configuration Provisioning

LABEL	DESCRIPTION
Enable Configuration Provisioning	Select this for users to be able to retrieve VPN rule settings using the USG IPSec VPN client.
Client Authentication Method	Choose how users should be authenticated. They can be authenticated using the local database on the USG or an external authentication database such as LDAP, Active Directory or RADIUS. default is a method you configured in Object > Auth Method. You may configure multiple methods there. If you choose the local database on the USG, then configure users using the Object > User/ Group screen. If you choose LDAP, Active Directory or RADIUS authentication servers, then configure users on the respective server.
Configuration	When you add or edit a configuration provisioning entry, you are allowed to set the VPN Connection and Allowed User fields. Duplicate entries are not allowed. You cannot select the same VPN Connection and Allowed User pair in a new entry if the same pair exists in a previous entry. You can bind different rules to the same user, but the USG will only allow VPN rule setting retrieval for the first match found.

Table 140 Configuration > VPN > IPSec VPN > Configuration Provisioning (continued)

LABEL	DESCRIPTION
Add	Click Add to bind a configured VPN rule to a user or group. Only that user or group may then retrieve the specified VPN rule settings. If you click Add without selecting an entry in advance then the new entry appears as the first entry. Entry order is important as the USG searches entries in the order listed here to find a match. After a match is found, the USG stops searching. If you want to add an entry as number three for example, then first select entry 2 and click Add. To reorder an entry, use Move.
Edit	Select an existing entry and click Edit to change its settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate. Make sure that Enable Configuration Provisioning is also selected.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	Use Move to reorder a selected entry. Select an entry, click Move, type the number where the entry should be moved, press <ENTER>, then click Apply.
Status	This icon shows if the entry is active (yellow) or not (gray). VPN rule settings can only be retrieved when the entry is activated (and Enable Configuration Provisioning is also selected).
Priority	Priority shows the order of the entry in the list. Entry order is important as the USG searches entries in the order listed here to find a match. After a match is found the USG stops searching.
VPN Connection	This field shows all configured VPN rules that match the rule criteria for the USG IPSec VPN client. Select a rule to bind to the associated user or group.
Allowed User	Select which user or group of users is allowed to retrieve the associated VPN rule settings using the USG IPSec VPN client. A user may belong to a number of groups. If entries are configured for different groups, the USG will allow VPN rule setting retrieval based on the first match found. Users of type admin or limited-admin are not allowed.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

21.6 IPSec VPN Background Information

Here is some more detailed IPSec VPN background information.

IKE SA Overview

The IKE SA provides a secure connection between the USG and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines how many. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Note: Both routers must use the same negotiation mode.

These modes are discussed in more detail in Negotiation Mode on page 362. Main mode is used in various examples in the rest of this section.

The USG supports IKEv1 and IKEv2. See Section 21.1 on page 333 for more information.

IP Addresses of the USG and Remote IPSec Router

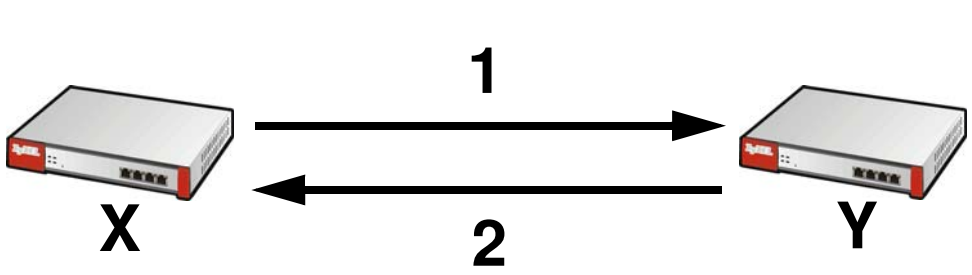
To set up an IKE SA, you have to specify the IP addresses of the USG and remote IPSec router. You can usually enter a static IP address or a domain name for either or both IP addresses. Sometimes, your USG might offer another alternative, such as using the IP address of a port or interface, as well.

You can also specify the IP address of the remote IPSec router as 0.0.0.0. This means that the remote IPSec router can have any IP address. In this case, only the remote IPSec router can initiate an IKE SA because the USG does not know the IP address of the remote IPSec router. This is often used for telecommuters.

IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the USG and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated next.

Figure 233 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal



The USG sends one or more proposals to the remote IPSec router. (In some devices, you can only set up one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the USG wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the USG. If the remote IPSec router rejects all of the proposals, the USG and remote IPSec router cannot establish an IKE SA.

Note: Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

In most USGs, you can select one of the following encryption algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Some USGs also offer stronger forms of AES that apply 192-bit or 256-bit keys to 128-bit blocks of data.

In most USGs, you can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

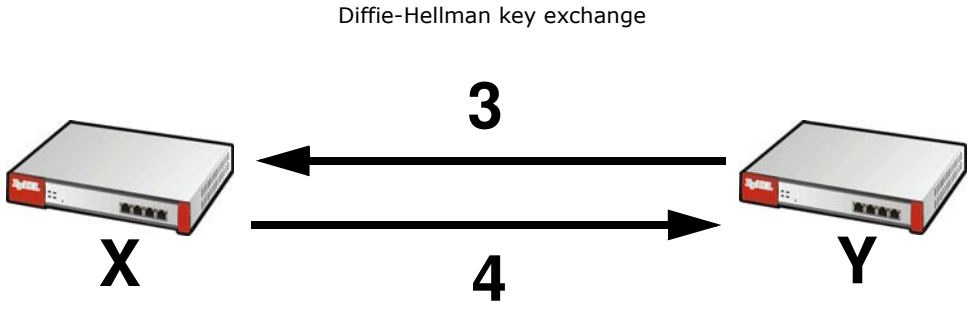
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
- SHA256 (Secure Hash Algorithm) produces a 256-bit digest to authenticate packet data.
- SHA512 (Secure Hash Algorithm) produces a 512-bit digest to authenticate packet data.

See Diffie-Hellman (DH) Key Exchange on page 360 for more information about DH key groups.

Diffie-Hellman (DH) Key Exchange

The USG and the remote IPSec router use DH public-key cryptography to establish a shared secret. The shared secret is then used to generate encryption keys for the IKE SA and IPSec SA. In main mode, this is done in steps 3 and 4, as illustrated next.

Figure 234 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



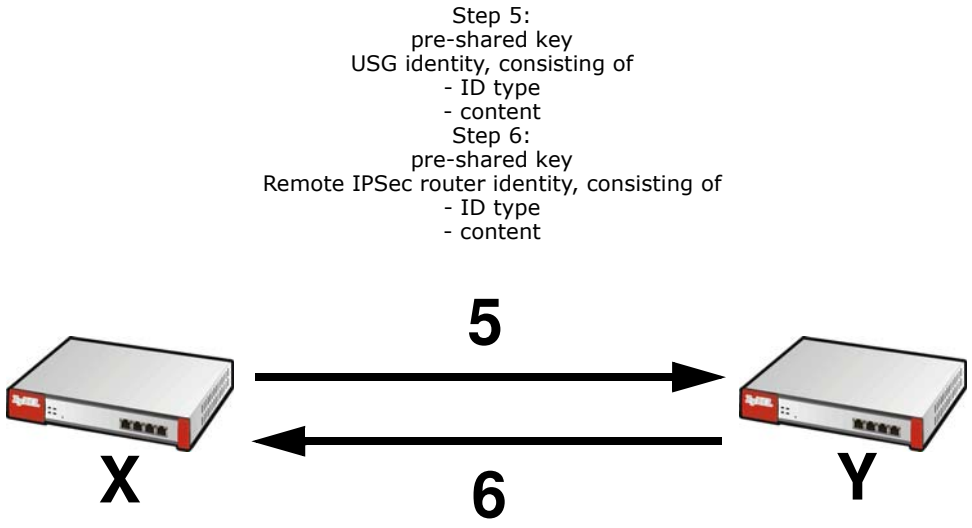
DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

Authentication

Before the USG and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the USG and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. The identities are also encrypted using the encryption algorithm and encryption key the USG and remote IPSec router selected in previous steps.

Figure 235 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication (continued)



You have to create (and distribute) a pre-shared key. The USG and remote IPSec router use it in the authentication process, though it is not actually transmitted or exchanged.

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

Router identity consists of ID type and content. The ID type can be domain name, IP address, or e-mail address, and the content is a (properly-formatted) domain name, IP address, or e-mail address. The content is only used for identification. Any domain name or e-mail address that you enter does not have to actually exist. Similarly, any domain name or IP address that you enter does not have to correspond to the USG's or remote IPSec router's properties.

The USG and the remote IPSec router have their own identities, so both of them must store two sets of information, one for themselves and one for the other router. Local ID type and content refers to the ID type and content that applies to the router itself, and peer ID type and content refers to the ID type and content that applies to the other router.

Note: The USG's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.

For example, in Table 141 on page 361, the USG and the remote IPSec router authenticate each other successfully. In contrast, in Table 142 on page 362, the USG and the remote IPSec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

Table 141 VPN Example: Matching ID Type and Content

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

Table 142 VPN Example: Mismatching ID Type and Content

USG	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.20	Peer ID content: tom@yourcompany.com

It is also possible to configure the USG to ignore the identity of the remote IPSec router. In this case, you usually set the peer ID type to Any. This is less secure, so you should only use this if your USG provides another way to check the identity of the remote IPSec router (for example, extended authentication) or if you are troubleshooting a VPN tunnel.

Additional Topics for IKE SA

This section provides more information about IKE SA.

Negotiation Mode

There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1 - 2: The USG sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the USG.

Steps 3 - 4: The USG and the remote IPSec router exchange pre-shared keys for authentication and participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

Steps 5 - 6: Finally, the USG and the remote IPSec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

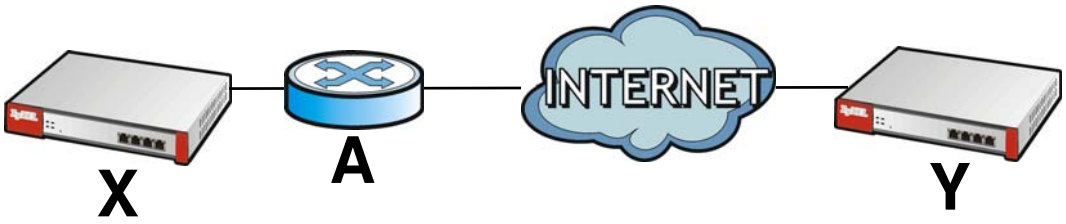
In contrast, aggressive mode only takes three steps to establish an IKE SA. Aggressive mode does not provide as much security because the identity of the USG and the identity of the remote IPSec router are not encrypted. It is usually used in remote-access situations, where the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication. For example, the remote IPSec router may be a telecommuter who does not have a static IP address.

VPN, NAT, and NAT Traversal

In the following example, there is another router (A) between router X and router Y.

Figure 236 VPN/NAT Example

If router A does NAT, it might change the IP addresses, port numbers, or both. If router X and router Y try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.



Most routers like router A now have an IPSec pass-thru feature. This feature helps router A recognize VPN packets and route them appropriately. If router A has this feature, router X and router Y can establish a VPN tunnel as long as the active protocol is ESP. (See Active Protocol on page 364 for more information about active protocols.)

If router A does not have an IPSec pass-thru or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router X and router Y add an extra header to the IKE SA and IPSec SA packets. If you configure router A to forward these packets unchanged, router X and router Y can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the USG and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the USG and remote IPSec router support.

X-Auth / Extended Authentication

X-Auth / Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters.

In extended authentication, one of the routers (the USG or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the USG to provide a user name and password to the remote IPSec router, or you can set up the USG to check a user name and password that is provided by the remote IPSec router.

If you use extended authentication, it takes four more steps to establish an IKE SA. These steps occur at the end, regardless of the negotiation mode (steps 7-10 in main mode, steps 4-7 in aggressive mode).

Certificates

It is possible for the USG and remote IPSec router to authenticate each other with certificates. In this case, you do not have to set up the pre-shared key, local identity, or remote identity because the certificates provide this information instead.

- Instead of using the pre-shared key, the USG and remote IPSec router check the signatures on each other's certificates. Unlike pre-shared keys, the signatures do not have to match.
- The local and peer ID type and content come from the certificates.

Note: You must set up the certificates for the USG and remote IPSec router first.

IPSec SA Overview

Once the USG and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

Note: The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

Local Network and Remote Network

In an IPSec SA, the local network, the one(s) connected to the USG, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPSec router, may be called the remote policy.

Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

Note: The USG and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the USG and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

Note: The USG and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 237 VPN: Transport and Tunnel Mode Encapsulation

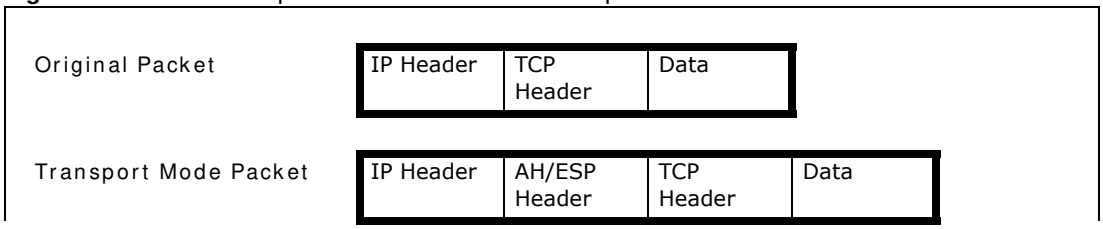
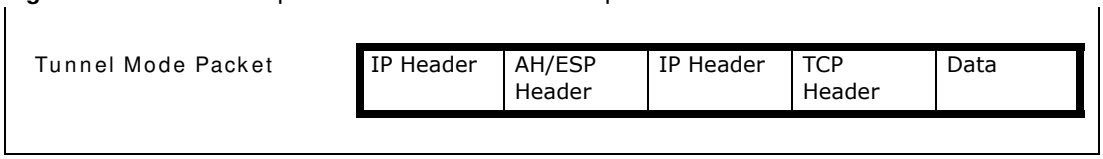


Figure 237 VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the USG uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the USG or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the USG or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the USG includes part of the original IP header when it encapsulates the packet. With ESP, however, the USG does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see IKE SA Proposal on page 359), except that you also have the choice whether or not the USG and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the USG and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the USG and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

PFS is ignored in initial IKEv2 authentication but is used when reauthenticating.

Additional Topics for IPSec SA

This section provides more information about IPSec SA in your USG.

Authentication and the Security Parameter Index (SPI)

For authentication, the USG and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

Note: The USG and remote IPSec router must use the same SPI.

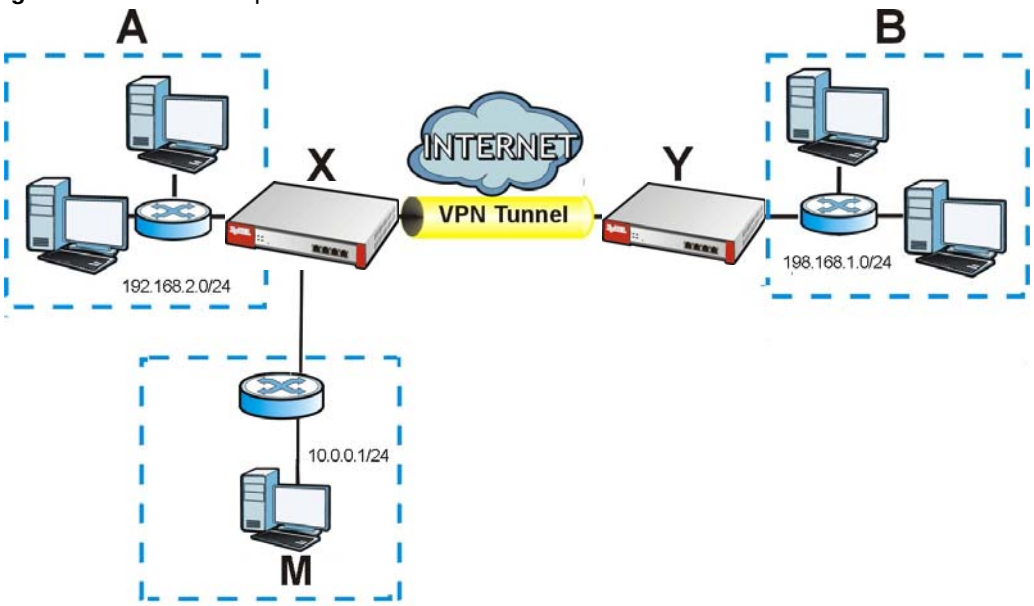
NAT for Inbound and Outbound Traffic

The USG can translate the following types of network addresses in IPSec SA.

- Source address in outbound packets - this translation is necessary if you want the USG to route packets from computers outside the local network through the IPSec SA.
- Source address in inbound packets - this translation hides the source address of computers in the remote network.
- Destination address in inbound packets - this translation is used if you want to forward packets (for example, mail) from the remote network to a specific computer (like the mail server) in the local network.

Each kind of translation is explained below. The following example is used to help explain each one.

Figure 238 VPN Example: NAT for Inbound and Outbound Traffic



Source Address in Outbound Packets (Outbound Traffic, Source NAT)

This translation lets the USG route packets from computers that are not part of the specified local network (local policy) through the IPSec SA. For example, in Figure 238 on page 366, you have to configure this kind of translation if you want computer M to establish a connection with any computer in the remote network (B). If you do not configure it, the remote IPSec router may not route messages for computer M through the IPSec SA because computer M's IP address is not part of its local policy.

To set up this NAT, you have to specify the following information:

- Source - the original source address; most likely, computer M's network.
- Destination - the original destination address; the remote network (B).
- SNAT - the translated source address; the local network (A).

Source Address in Inbound Packets (Inbound Traffic, Source NAT)

You can set up this translation if you want to change the source address of computers in the remote network. To set up this NAT, you have to specify the following information:

- Source - the original source address; the remote network (B).

- Destination - the original destination address; the local network (A).
- SNAT - the translated source address; a different IP address (range of addresses) to hide the original source address.

Destination Address in Inbound Packets (Inbound Traffic, Destination NAT)

You can set up this translation if you want the USG to forward some packets from the remote network to a specific computer in the local network. For example, in Figure 238 on page 366, you can configure this kind of translation if you want to forward mail from the remote network to the mail server in the local network (A).

You have to specify one or more rules when you set up this kind of NAT. The USG checks these rules similar to the way it checks rules for a security policy. The first part of these rules define the conditions in which the rule apply.

- Original IP - the original destination address; the remote network (B).
- Protocol - the protocol [TCP, UDP, or both] used by the service requesting the connection.
- Original Port - the original destination port or range of destination ports; in Figure 238 on page 366, it might be port 25 for SMTP.

The second part of these rules controls the translation when the condition is satisfied.

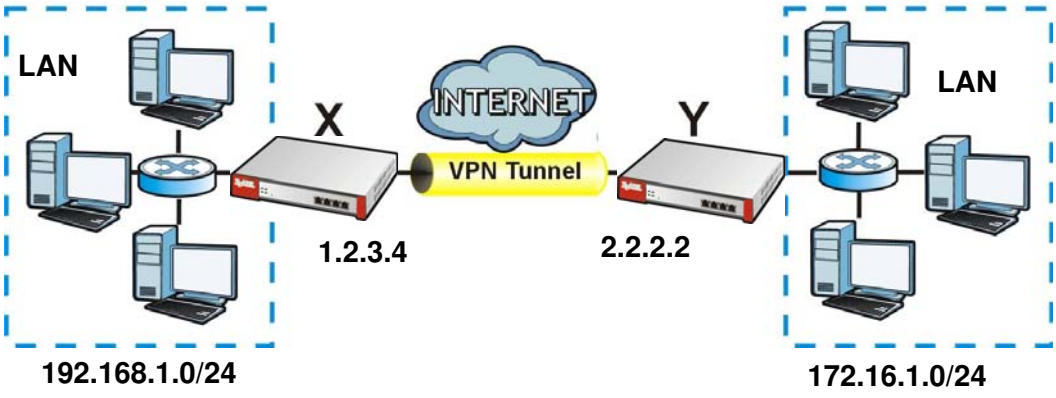
- Mapped IP - the translated destination address; in Figure 238 on page 366, the IP address of the mail server in the local network (A).
- Mapped Port - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

IPSec VPN Example Scenario

Here is an example site-to-site IPSec VPN scenario.

Figure 239 Site-to-site IPSec VPN Example



22

SSL VPN

22.1 Overview

Use SSL VPN to allow users to use a web browser for secure remote user login. The remote users do not need a VPN router or VPN client software.

22.1.1 What You Can Do in this Chapter

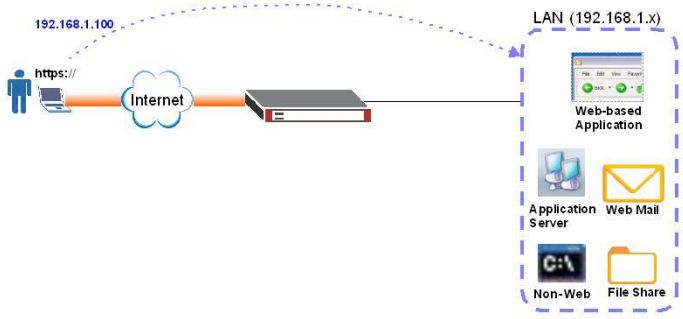
- Use the VPN > SSL VPN > Access Privilege screens (see Section 22.2 on page 369) to configure SSL access policies.
- Use the Click VPN > SSL VPN > Global Setting screen (see Section 22.3 on page 373) to set the IP address of the USG (or a gateway device) on your network for full tunnel mode access, enter access messages or upload a custom logo to be displayed on the remote user screen.
- Use the VPN > SSL VPN > SecuExtender screen (see Section 22.4 on page 375) to update and check the current and latest version of the Security Extender.

22.1.2 What You Need to Know

Full Tunnel Mode

In full tunnel mode, a virtual connection is created for remote users with private IP addresses in the same subnet as the local network. This allows them to access network resources in the same way as if they were part of the internal network.

Figure 240 Network Access Mode: Full Tunnel Mode



SSL Access Policy

An SSL access policy allows the USG to perform the following tasks:

- limit user access to specific applications or file sharing server on the network.
- allow user access to specific networks.

- assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

SSL Access Policy Objects

The SSL access policies reference the following objects. If you update this information, in response to changes, the USG automatically propagates the changes through the SSL policies that use the object(s). When you delete an SSL policy, the objects are not removed.

Table 143 Objects

OBJECT TYPE	OBJECT SCREEN	DESCRIPTION
User Accounts	User Account/ User Group	Configure a user account or user group to which you want to apply this SSL access policy.
Application	SSL Application	Configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access.
IP Pool	Address	Configure an address object that defines a range of private IP addresses to assign to user computers so they can access the internal network through a VPN connection.
Server Addresses	Address	Configure address objects for the IP addresses of the DNS and WINS servers that the USG sends to the VPN connection users.
VPN Network	Address	Configure an address object to specify which network segment users are allowed to access through a VPN connection.

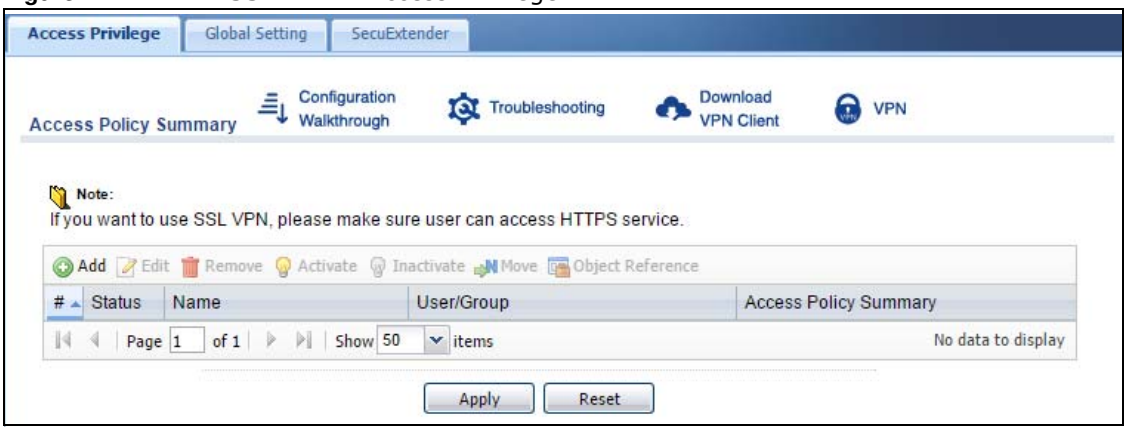
You cannot delete an object that is referenced by an SSL access policy. To delete the object, you must first unassociate the object from the SSL access policy.

22.2 The SSL Access Privilege Screen

Click VPN > SSL VPN to open the Access Privilege screen. This screen lists the configured SSL access policies.

Click on the icons to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting and other information.

Figure 241 VPN > SSL VPN > Access Privilege



The following table describes the labels in this screen.

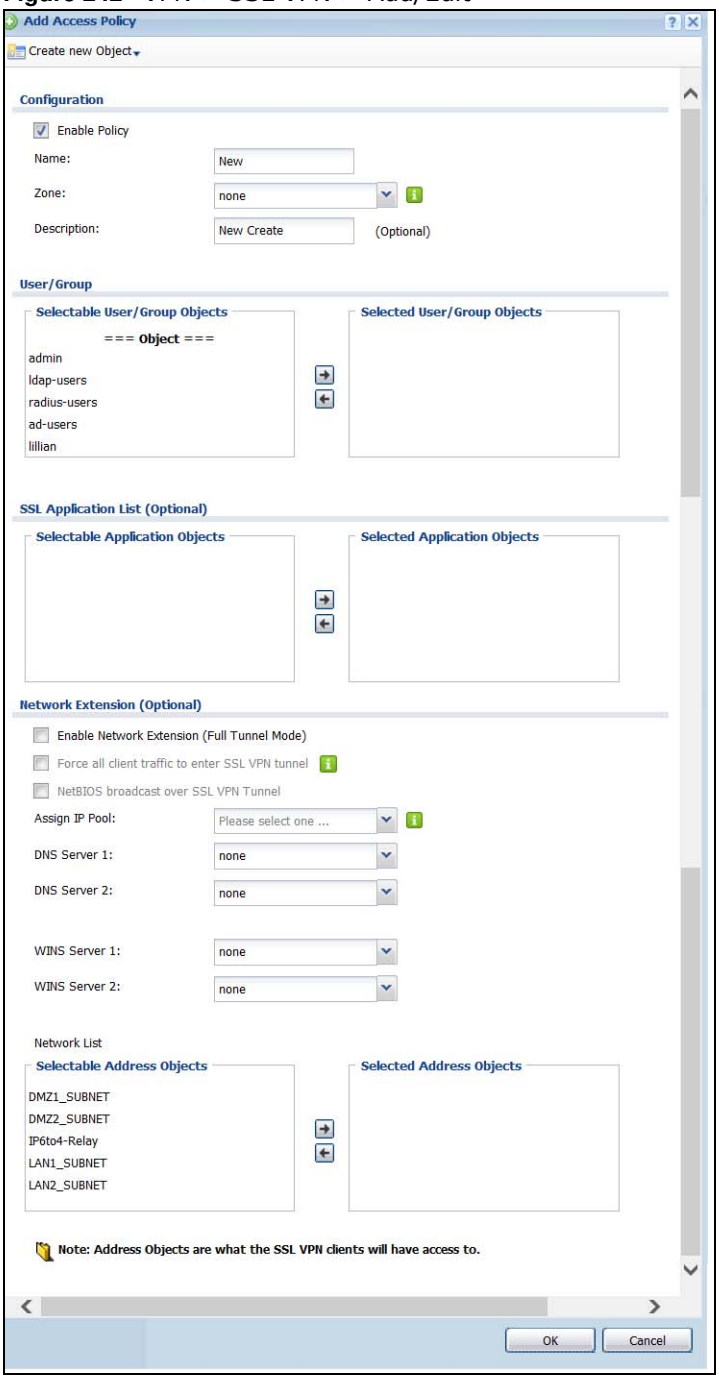
Table 144 VPN > SSL VPN > Access Privilege

LABEL	DESCRIPTION
Access Policy Summary	This screen shows a summary of SSL VPN policies created. Click on the VPN icon to go to the ZyXEL VPN Client product page at the ZyXEL website.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	To move an entry to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the interface.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This field displays the index number of the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the descriptive name of the SSL access policy for identification purposes.
User/Group	This field displays the user account or user group name(s) associated to an SSL access policy. This field displays up to three names.
Access Policy Summary	This field displays details about the SSL application object this policy uses including its name, type, and address.
Apply	Click Apply to save the settings.
Reset	Click Reset to discard all changes.

22.2.1 The SSL Access Privilege Policy Add/Edit Screen

To create a new or edit an existing SSL access policy, click the Add or Edit icon in the Access Privilege screen.

Figure 242 VPN > SSL VPN > Add/Edit



The following table describes the labels in this screen.

Table 145 VPN > SSL VPN > Access Privilege > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Configuration	
Enable Policy	Select this option to activate this SSL access policy.

Table 145 VPN > SSL VPN > Access Privilege > Add/Edit (continued)

LABEL	DESCRIPTION
Name	Enter a descriptive name to identify this policy. You can enter up to 31 characters (“a-z”, A-Z”, “0-9”) with no spaces allowed.
Zone	Select the zone to which to add this SSL access policy. You use zones to apply security settings such as security policy and remote management.
Description	Enter additional information about this SSL access policy. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").
User/Group	The Selectable User/ Group Objects list displays the name(s) of the user account and/or user group(s) to which you have not applied an SSL access policy yet. To associate a user or user group to this SSL access policy, select a user account or user group and click the right arrow button to add to the Selected User/ Group Objects list. You can select more than one name. To remove a user or user group, select the name(s) in the Selected User/ Group Objects list and click the left arrow button. Note: Although you can select admin and limited-admin accounts in this screen, they are reserved for device configuration only. You cannot use them to access the SSL VPN portal.
SSL Application List (Optional)	The Selectable Application Objects list displays the name(s) of the SSL application(s) you can select for this SSL access policy. To associate an SSL application to this SSL access policy, select a name and click the right arrow button to add to the Selected Application Objects list. You can select more than one application. To remove an SSL application, select the name(s) in the Selected Application Objects list and click the left arrow button. Note: To allow access to shared files on a Windows 7 computer, within Windows 7 you must enable sharing on the folder and also go to the **Network and Sharing Center**’s **Advanced sharing settings** and turn on the current network profile’s file and printer sharing.
Network Extension (Optional)	
Enable Network Extension	Select this option to create a VPN tunnel between the authenticated users and the internal network. This allows the users to access the resources on the network as if they were on the same local network. This includes access to resources not supported by SSL application objects. For example this lets users Telnet to the internal network even though the USG does not have SSL application objects for Telnet. Clear this option to disable this feature. Users can only access the applications as defined by the VPN tunnel’s selected SSL application settings and the remote user computers are not made to be a part of the local network.
Force all client traffic to SSL VPN tunnel	Select this to send all traffic from the SSL VPN clients through the SSL VPN tunnel. This replaces the default gateway of the SSL VPN clients with the SSL VPN gateway.
NetBIOS broadcast over SSL VPN Tunnel	Select this to search for a remote computer and access its applications as if it was in a Local Area Network. The user can find a computer not only by its IP adress but also by computer name.
Assign IP Pool	Define a separate pool of IP addresses to assign to the SSL users. Select it here. The SSL VPN IP pool should not overlap with IP addresses on the USG's local networks (LAN and DMZ for example), the SSL user's network, or the networks you specify in the SSL VPN Network List.
DNS/WINS Server 1..2	Select the name of the DNS or WINS server whose information the USG sends to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses.

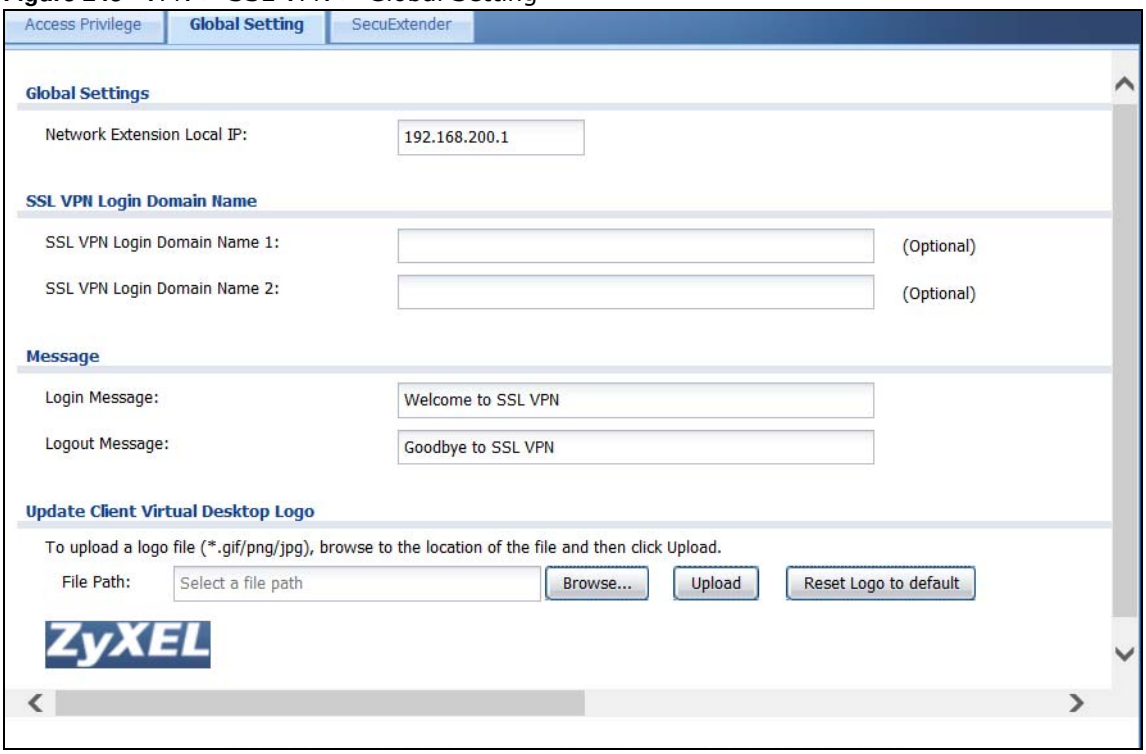
Table 145 VPN > SSL VPN > Access Privilege > Add/Edit (continued)

LABEL	DESCRIPTION
Network List	To allow user access to local network(s), select a network name in the Selectable Address Objects list and click the right arrow button to add to the Selected Address Objects list. You can select more than one network. To block access to a network, select the network name in the Selected Address Objects list and click the left arrow button.
OK	Click OK to save the changes and return to the main Access Privilege screen.
Cancel	Click Cancel to discard all changes and return to the main Access Privilege screen.

22.3 The SSL Global Setting Screen

Click VPN > SSL VPN and click the Global Setting tab to display the following screen. Use this screen to set the IP address of the USG (or a gateway device) on your network for full tunnel mode access, enter access messages or upload a custom logo to be displayed on the remote user screen.

Figure 243 VPN > SSL VPN > Global Setting



The following table describes the labels in this screen.

Table 146 VPN > SSL VPN > Global Setting

LABEL	DESCRIPTION
Global Setting	
Network Extension Local IP	Specify the IP address of the USG (or a gateway device) for full tunnel mode SSL VPN access. Leave this field to the default settings unless it conflicts with another interface.

Table 146 VPN > SSL VPN > Global Setting (continued)

LABEL	DESCRIPTION
SSL VPN Login Domain Name	
SSL VPN Login Domain Name 1/ 2	Specify a full domain name for users to use for SSL VPN login. The domain name must be registered to one of the USG's IP addresses or be one of the USG's DDNS entries. You can specify up to two domain names so you could use one domain name for each of two WAN ports. For example, www.zyxel.com is a fully qualified domain name where "www" is the host. The USG displays the normal login screen without the button for logging into the Web Configurator.
Message	
Login Message	Specify a message to display on the screen when a user logs in and an SSL VPN connection is established successfully. You can enter up to 60 characters (0-9, a-z, A-Z, '()+,/:=?;!*#@$_%-") with spaces allowed.
Logout Message	Specify a message to display on the screen when a user logs out and the SSL VPN connection is terminated successfully. You can enter up to 60 characters (0-9, a-z, A-Z, '()+,/:=?;!*#@$_%-") with spaces allowed.
Update Client Virtual Desktop Logo	You can upload a graphic logo to be displayed on the web browser on the remote user computer. The ZyXEL company logo is the default logo. Specify the location and file name of the logo graphic or click Browse to locate it. Note: The logo graphic must be GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The USG automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.
Browse	Click Browse to locate the graphic file on your computer.
Upload	Click Upload to transfer the specified graphic file from your computer to the USG.
Reset Logo to Default	Click Reset Logo to Default to display the ZyXEL company logo on the remote user's web browser.
Apply	Click Apply to save the changes and/or start the logo file upload process.
Reset	Click Reset to return the screen to its last-saved settings.

22.3.1 How to Upload a Custom Logo

Follow the steps below to upload a custom logo to display on the remote user SSL VPN screens.

1 Click VPN > SSL VPN and click the Global Setting tab to display the configuration screen.

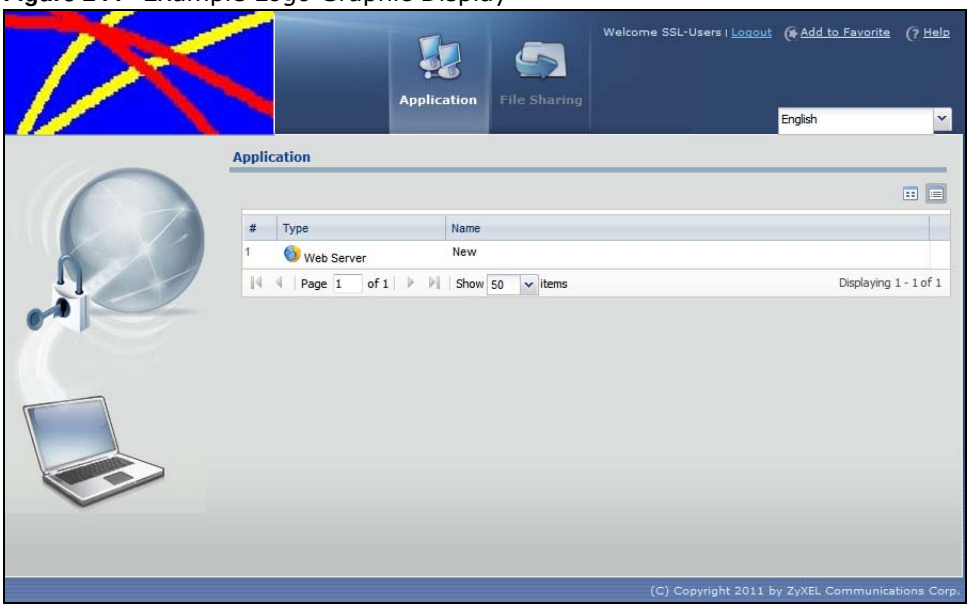
2 Click Browse to locate the logo graphic. Make sure the file is in GIF, JPG, or PNG format.

3 Click Apply to start the file transfer process.

4 Log in as a user to verify that the new logo displays properly.

The following shows an example logo on the remote user screen.

Figure 244 Example Logo Graphic Display



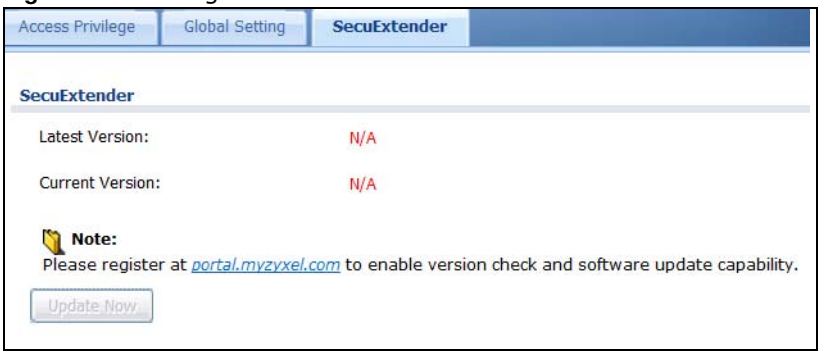
22.4 USG SecuExtender

The USG automatically loads the USG SecuExtender client program to your computer after a successful login to an SSL VPN tunnel with network extension support enabled. The USG SecuExtender lets you:

- Access servers, remote desktops and manage files as if you were on the local network.
- Use applications like e-mail, file transfer, and remote desktop programs directly without using a browser. For example, you can use Outlook for e-mail instead of the USG's web-based e-mail.
- Use applications, even proprietary applications, for which the USG does not offer SSL application objects.

The applications must be installed on your computer. For example, to use the VNC remote desktop program, you must have the VNC client installed on your computer. Please refer to the SecuExtender chapter for details.

Figure 245 Configuration > VPN > SSL VPN > SecuExtender.



The following table describes the labels in this screen.

Table 147 Configuration > VPN > SSL VPN > SecuExtender

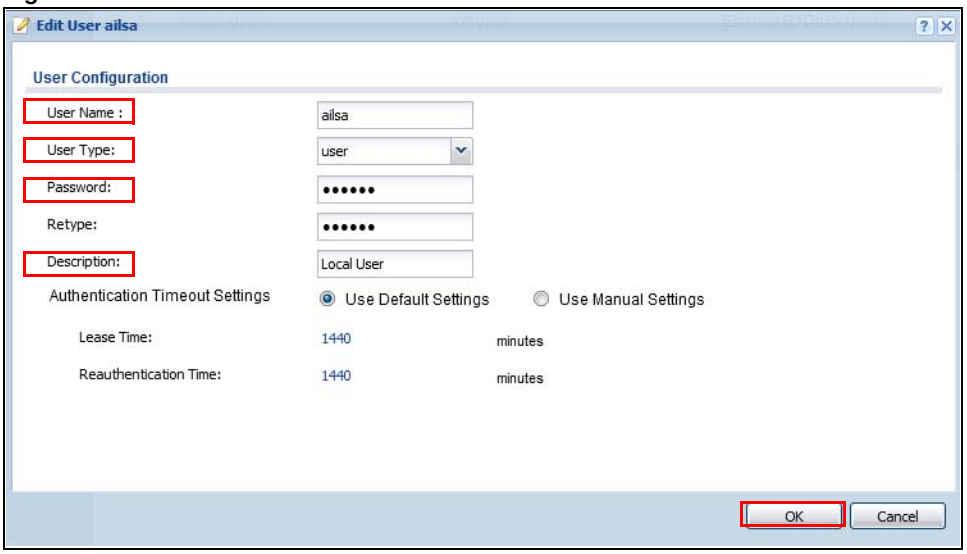
LABEL	DESCRIPTION
Latest Version	This displays the latest version of the USG Security SecuExtender that is available.
Current Version	This displays the current version of SecuExtender that is installed in the USG.
Note:	You need to register first at portal.myzyxel.com to download the latest version of SecuExtender.
Update Now	The USG periodically checks if there's a later version of SecuExtender at the portal. The Update Now button is enabled when thre is.Click Update Now to get the latest version of SecuExtender.

22.4.1 Example: Configure USG for SecuExtender

Make these configurations on the USG to allow the remote user to access resources behind the USG using SecuExtender. These steps can be performed in any order.

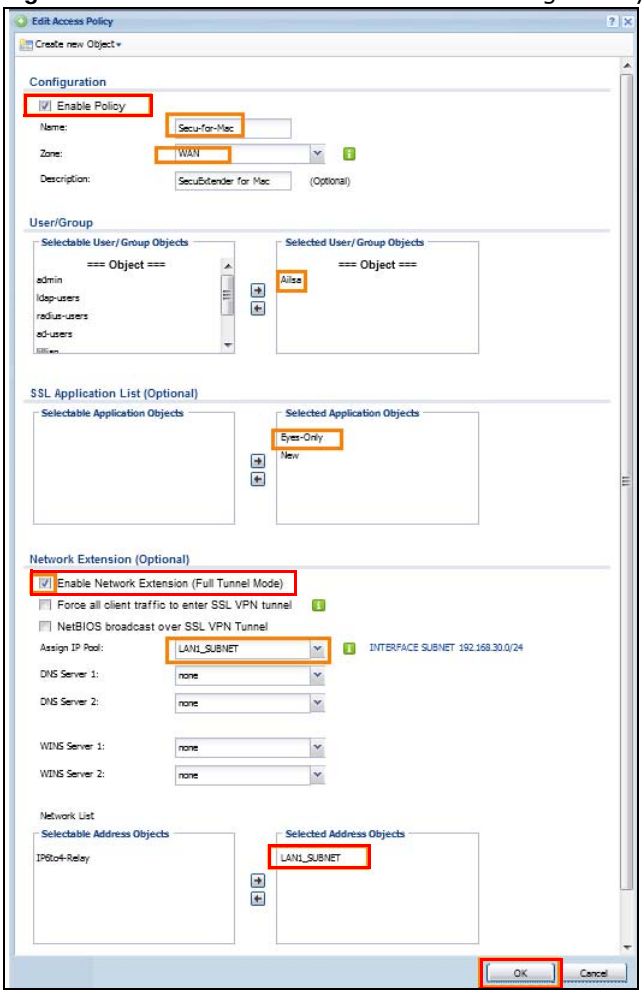
1 Create a user that can log into the USG. Using the USG web configurator, go to Configuration > Object > User > Add and substitute your information for the information shown in the following example.

Figure 246 Create a User



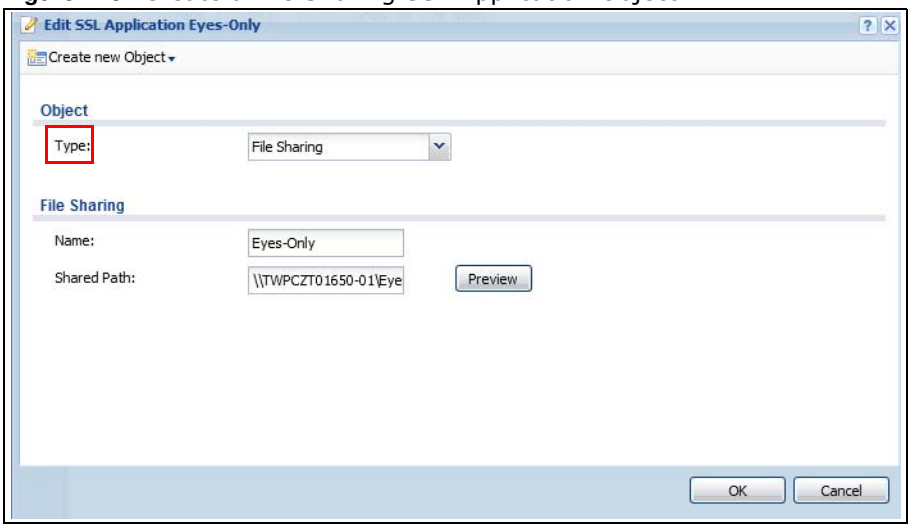
2 Next create an SSL VPN Access Privilege policy substituting your information for the information shown in the following example. Using the USG web configurator, go to Configuration > VPN > SSL VPN > Access Privilege > Add.

Figure 247 Create an SSL VPN Access Privilege Policy

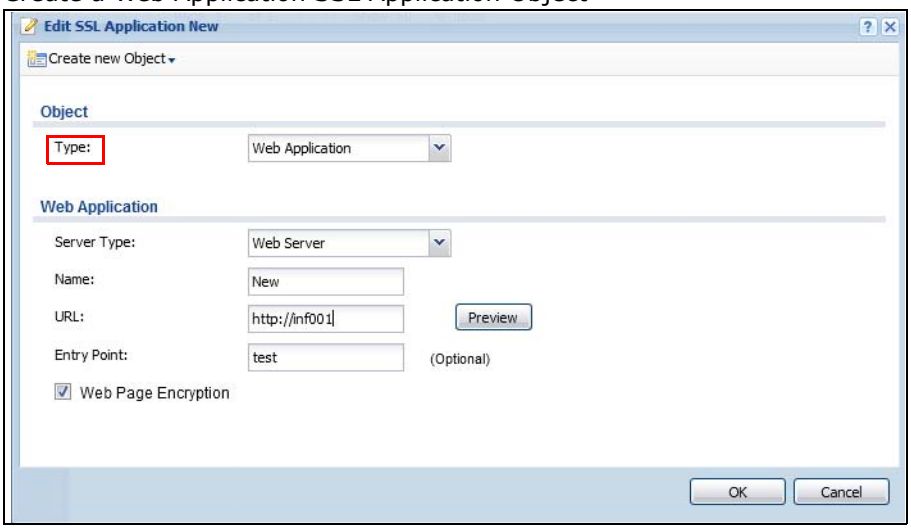


3 Then create File Sharing and Web Application SSL Application objects. Using the USG web configurator, go to Configuration > Object > SSL Application > Add and select the Type accordingly. Substitute your information for the information shown in the following example.

Figure 248 Create a File Sharing SSL Application Object



Create a Web Application SSL Application Object



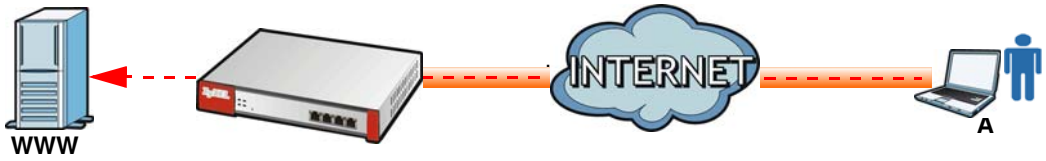
23

SSL User Screens

23.1 Overview

This chapter introduces the remote user SSL VPN screens. The following figure shows a network example where a remote user (A) logs into the USG from the Internet to access the web server (WWW) on the local network.

Figure 249 Network Example



23.1.1 What You Need to Know

The USG can use SSL VPN to provide secure connections to network resources such as applications, files, intranet sites or e-mail through a web-based interface and using Microsoft Outlook Web Access (OWA).

Network Resource Access Methods

As a remote user, you can access resources on the local network using one of the following methods.

- Using a supported web browser

  Once you have successfully logged in through the USG, you can access intranet sites, web-based applications, or web-based e-mails using one of the supported web browsers.
- Using the USG SecuExtender client

  Once you have successfully logged into the USG, if the SSL VPN access policy has network extension enabled the USG automatically loads the USG SecuExtender client program to your computer. With the USG SecuExtender, you can access network resources, remote desktops and manage files as if you were on the local network. See Chapter 24 on page 392 for more on the USG SecuExtender.

System Requirements

Here are the browser and computer system requirements for remote user access.

- Windows 7 (32 or 64-bit), Vista (32 or 64-bit), 2003 (32-bit), XP (32-bit), or 2000 (32-bit)
- Internet Explorer 7 and above or Firefox 1.5 and above

- Using RDP requires Internet Explorer
- Sun's Runtime Environment (JRE) version 1.6 or later installed and enabled.

Required Information

A remote user needs the following information from the network administrator to log in and access network resources.

- the domain name or IP address of the USG
- the login account user name and password
- if also required, the user name and/or password to access the network resource

Certificates

The remote user's computer establishes an HTTPS connection to the USG to access the login screen. If instructed by your network administrator, you must install or import a certificate (provided by the USG or your network administrator).

Finding Out More

See Chapter 22 on page 368 for how to configure SSL VPN on the USG.

23.2 Remote SSL User Login

This section shows you how to access and log into the network through the USG. Example screens for Internet Explorer are shown.

1 Open a web browser and enter the web site address or IP address of the USG. For example, "http://sslvpn.mycompany.com".

Figure 250 Enter the Address in a Web Browser



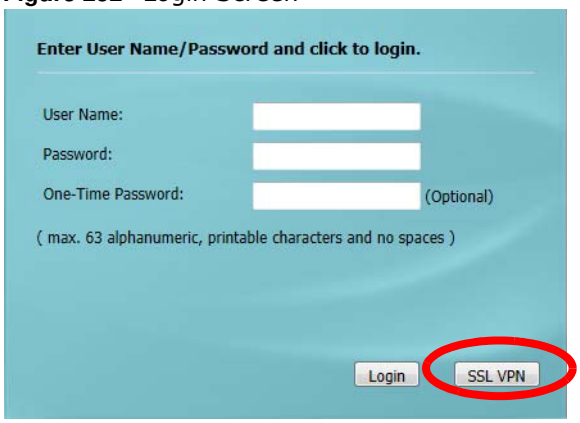
2 Click OK or Yes if a security screen displays.

Figure 251 Login Security Screen



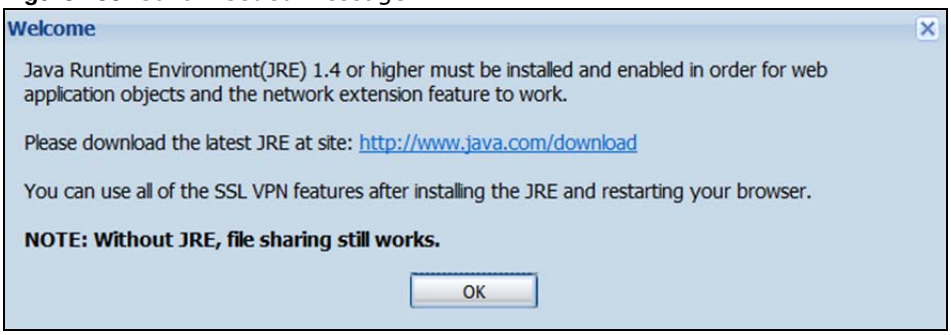
3 A login screen displays. Enter the user name and password of your login account. If a token password is also required, enter it in the One-Time Password field. Click SSL VPN to log in and establish an SSL VPN connection to the network to access network resources.

Figure 252 Login Screen



4 Your computer starts establishing a secure connection to the USG after a successful login. This may take up to two minutes. If you get a message about needing Java, download and install it and restart your browser and re-login. If a certificate warning screen displays, click OK, Yes or Continue.

Figure 253 Java Needed Message



5 The USG tries to install the SecuExtender client. As shown next, you may have to click some pop-ups to get your browser to allow the installation.

Figure 254 ActiveX Object Installation Blocked by Browser

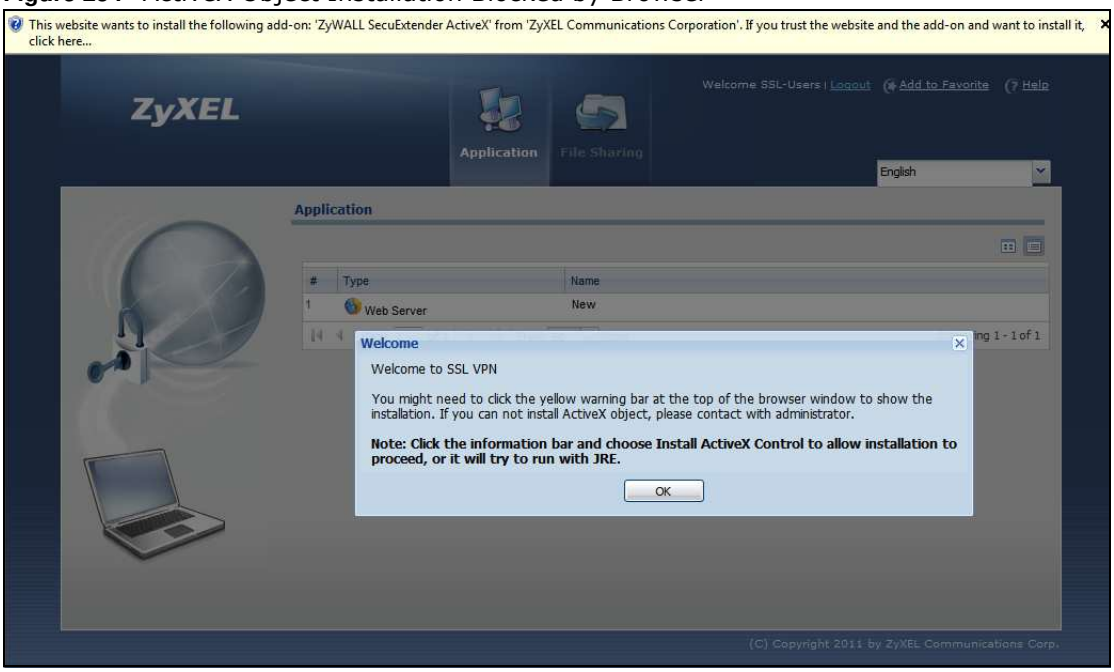
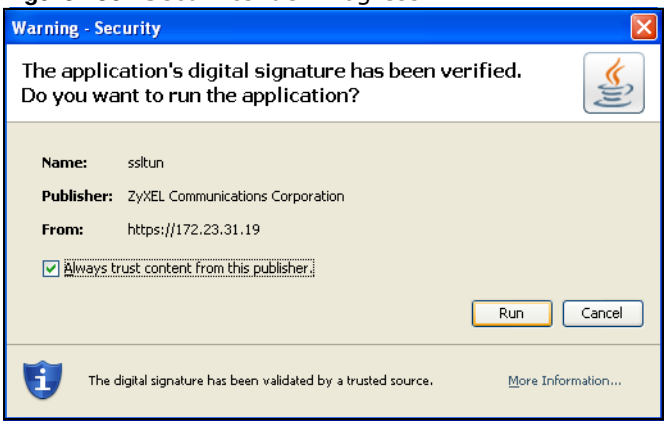


Figure 255 SecuExtender Blocked by Internet Explorer



6 The USG tries to run the "ssltun" application. You may need to click something to get your browser to allow this. In Internet Explorer, click Run.

Figure 256 SecuExtender Progress



7 Click Next to use the setup wizard to install the SecuExtender client on your computer.

Figure 257 SecuExtender Progress



8 If a screen like the following displays, click Continue Anyway to finish installing the SecuExtender client on your computer.

Figure 258 Installation Warning



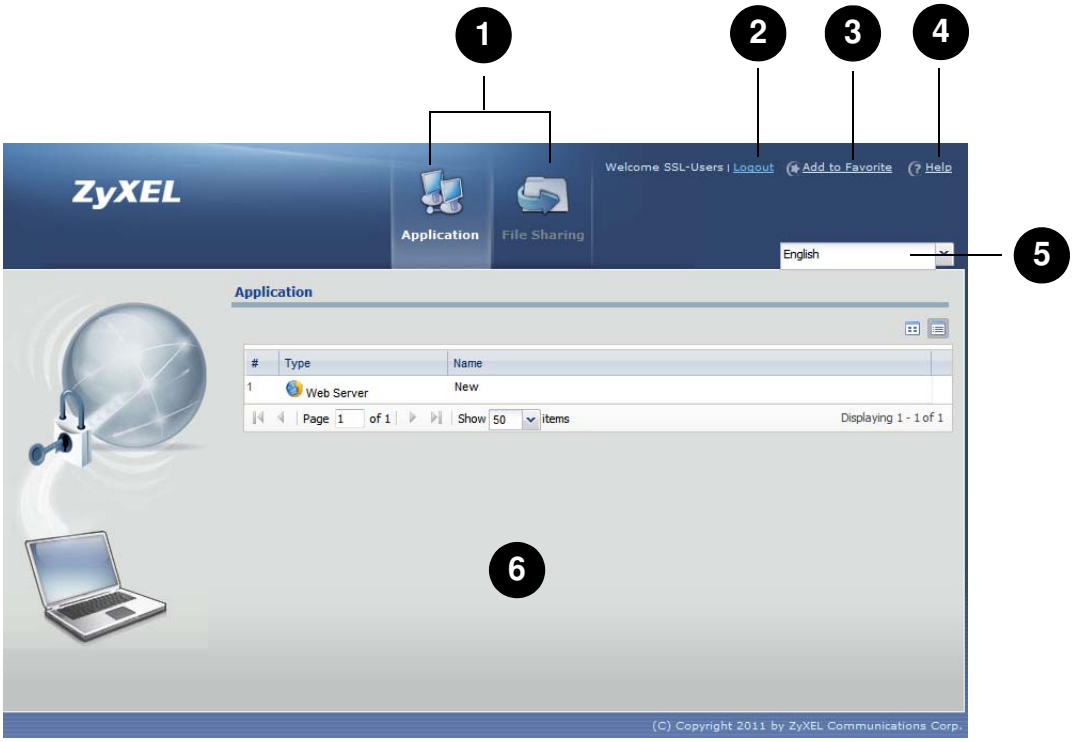
9 The Application screen displays showing the list of resources available to you. See Figure 259 on page 384 for a screen example.

Note: Available resource links vary depending on the configuration your network administrator made.

23.3 The SSL VPN User Screens

This section describes the main elements in the remote user screens.

Figure 259 Remote User Screen



The following table describes the various parts of a remote user screen.

Table 148 Remote User Screen Overview

#	DESCRIPTION
1	Click on a menu tab to go to the Application or File Sharing screen.
2	Click this icon to log out and terminate the secure connection.
3	Click this icon to create a bookmark to the SSL VPN user screen in your web browser.
4	Click this icon to display the on-line help window.
5	Select your preferred language for the interface.
6	This part of the screen displays a list of the resources available to you. In the Application screen, click on a link to access or display the access method. In the File Sharing screen, click on a link to open a file or directory.

23.4 Bookmarking the USG

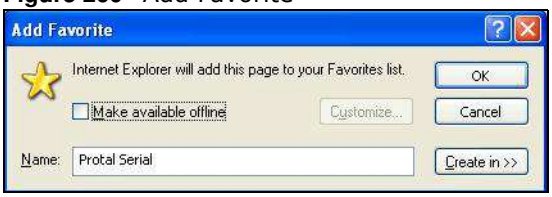
You can create a bookmark of the USG by clicking the Add to Favorite icon. This allows you to access the USG using the bookmark without having to enter the address every time.

1 In any remote user screen, click the Add to Favorite icon.

2 A screen displays. Accept the default name in the Name field or enter a descriptive name to identify this link.

3 Click OK to create a bookmark in your web browser.

Figure 260 Add Favorite



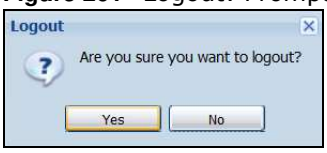
23.5 Logging Out of the SSL VPN User Screens

To properly terminate a connection, click on the Logout icon in any remote user screen.

1 Click the Logout icon in any remote user screen.

2 A prompt window displays. Click OK to continue.

Figure 261 Logout: Prompt



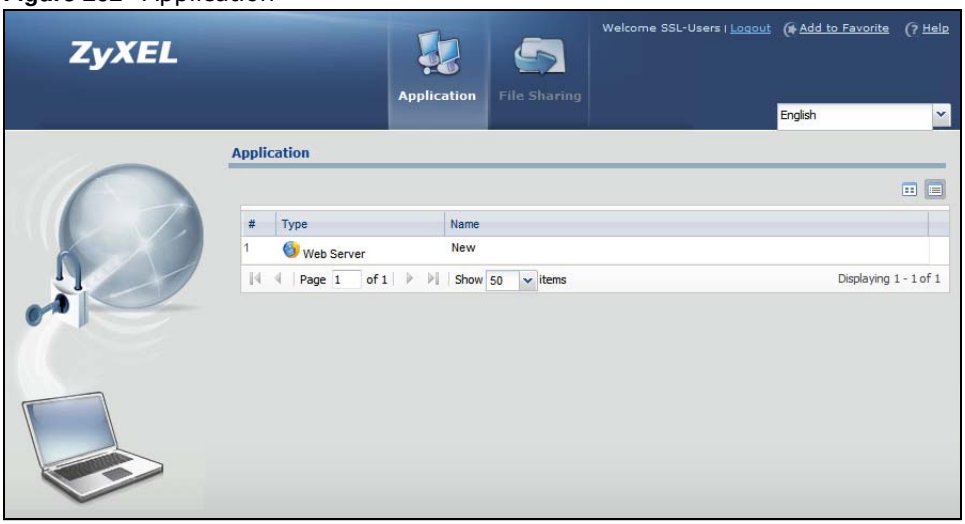
23.6 SSL User Application Screen

Use the Application tab's screen to access web-based applications (such as web sites and e-mail) on the network through the SSL VPN connection. Which applications you can access depends on the USG's configuration.

The Name field displays the descriptive name for an application. The Type field displays wether the application is a web site (Web Server) or web-based e-mail using Microsoft Outlook Web Access (OWA).

To access a web-based application, simply click a link in the Application screen to display the web screen in a separate browser window.

Figure 262 Application



23.7 SSL User File Sharing

The File Sharing screen lets you access files on a file server through the SSL VPN connection. Use it to display and access shared files/folders on a file server.

You can also perform the following actions:

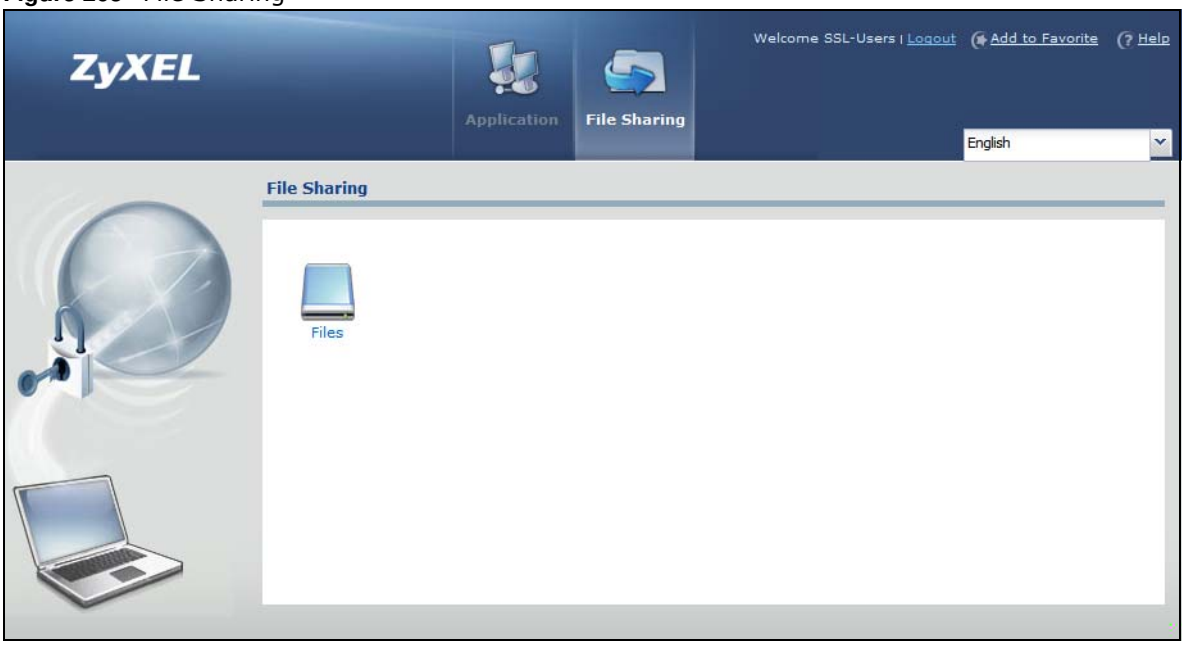
- Access a folder.
- Open a file (if your web browser cannot open the file, you are prompted to download it).
- Save a file to your computer.
- Create a new folder.
- Rename a file or folder.
- Delete a file or folder.
- Upload a file.

Note: Available actions you can perform in the File Sharing screen vary depending on the rights granted to you on the file server.

23.7.1 The Main File Sharing Screen

The first File Sharing screen displays the name(s) of the shared folder(s) available. The following figure shows an example with one file share.

Figure 263 File Sharing



23.7.2 Opening a File or Folder

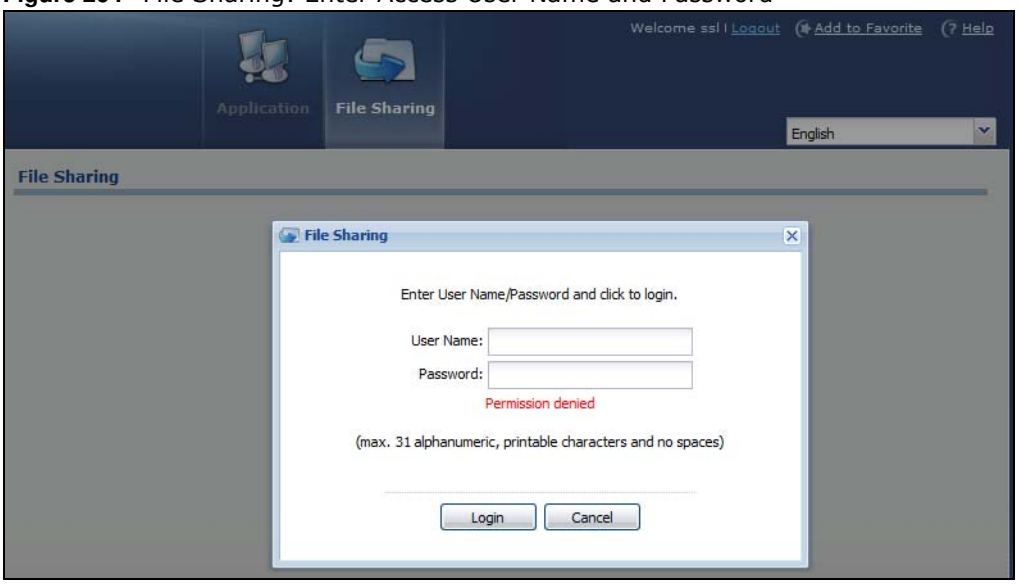
You can open a file if the file extension is recognized by the web browser and the associated application is installed on your computer.

1 Log in as a remote user and click the File Sharing tab.

2 Click on a file share icon.

3 If an access user name and password are required, a screen displays as shown in the following figure. Enter the account information and click Login to continue.

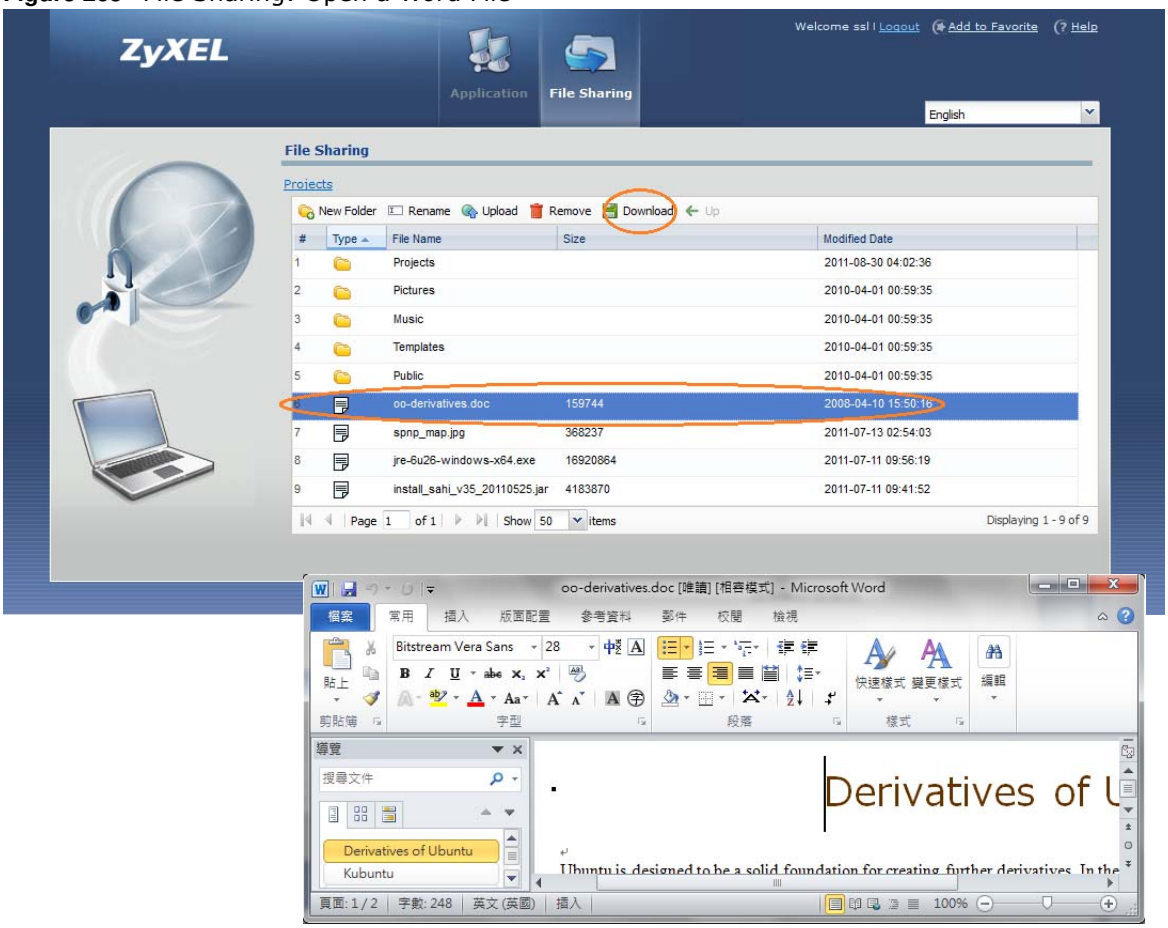
Figure 264 File Sharing: Enter Access User Name and Password



4 A list of files/folders displays. Double click a file to open it in a separate browser window or select a file and click Download to save it to your computer. You can also click a folder to access it.

For this example, click on a .doc file to open the Word document.

Figure 265 File Sharing: Open a Word File



23.7.3 Downloading a File

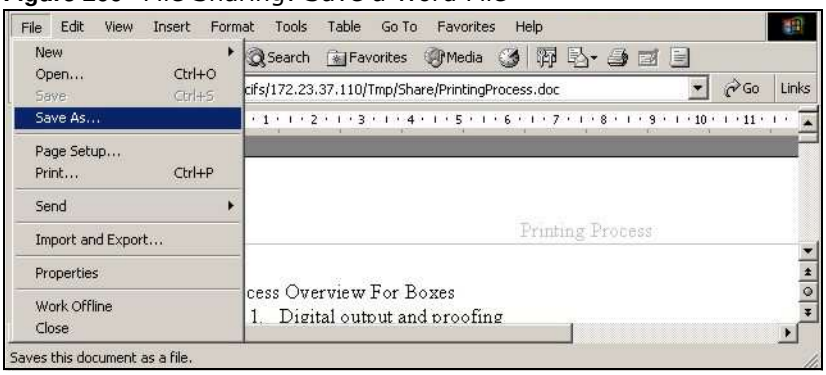
You are prompted to download a file which cannot be opened using a web browser.

Follow the on-screen instructions to download and save the file to your computer. Then launch the associated application to open the file.

23.7.4 Saving a File

After you have opened a file in a web browser, you can save a copy of the file by clicking File > Save As and following the on-screen instructions.

Figure 266 File Sharing: Save a Word File



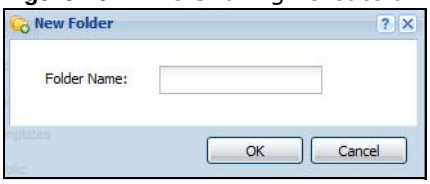
23.7.5 Creating a New Folder

To create a new folder in the file share location, click the New Folder icon.

Specify a descriptive name for the folder. You can enter up to 356 characters. Then click Add.

Note: Make sure the length of the folder name does not exceed the maximum allowed on the file server.

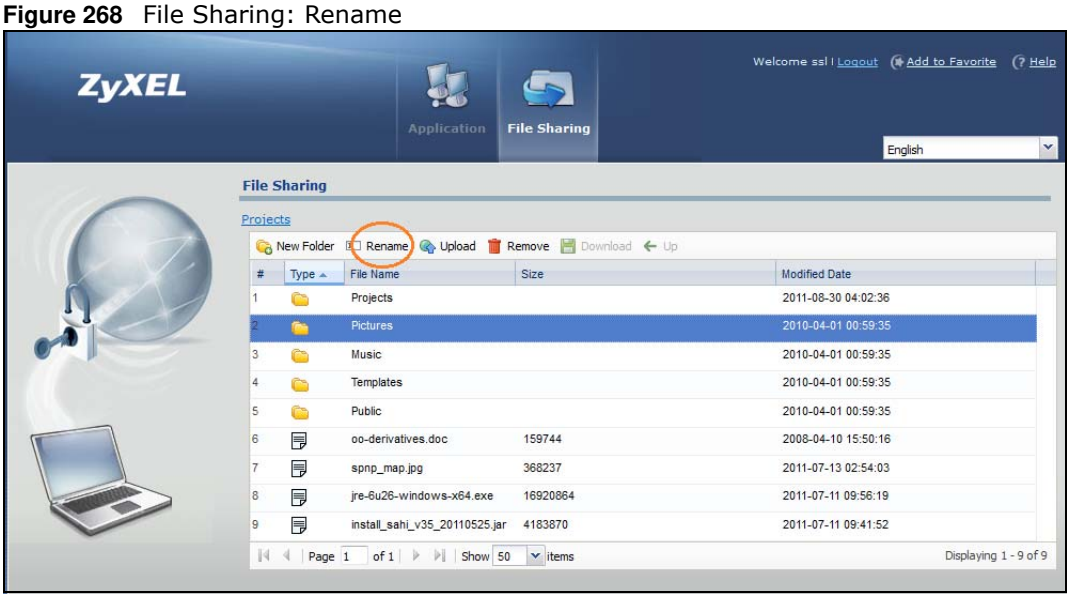
Figure 267 File Sharing: Create a New Folder



23.7.6 Renaming a File or Folder

To rename a file or folder, select a file or folder and click the Rename icon.

Figure 268 File Sharing: Rename



A popup window displays. Specify the new name and/or file extension in the field provided. You can enter up to 356 characters. Then click Apply.

Note: Make sure the length of the name does not exceed the maximum allowed on the file server.
You may not be able to open a file if you change the file extension.

Figure 269 File Sharing: Rename



23.7.7 Deleting a File or Folder

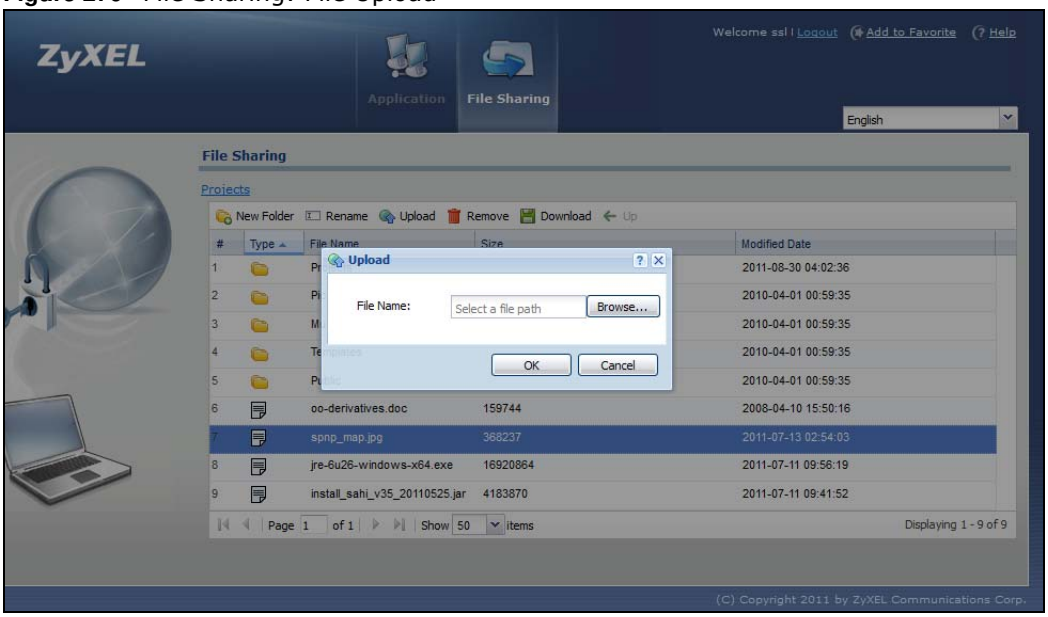
Click the Delete icon next to a file or folder to remove it.

23.7.8 Uploading a File

Follow the steps below to upload a file to the file server.

1. Log into the remote user screen and click the File Sharing tab.
2. Click Upload and specify the location and/or name of the file you want to upload. Or click Browse to locate it.
3. Click OK to send the file to the file server.
4. After the file is uploaded successfully, you should see the name of the file and a message in the screen.

Figure 270 File Sharing: File Upload



Note: Uploading a file with the same name and file extension replaces the existing file on the file server. No warning message is displayed.

24

USG SecuExtender (Windows)

The USG automatically loads the USG SecuExtender for Windows client program to your computer after a successful login to an SSL VPN tunnel with network extension support enabled.

Note: For information on using the USG SecuExtender for Mac client program, please see its User's Guide at the download library on the ZyXEL website.

The USG SecuExtender (Windows) lets you:

- Access servers, remote desktops and manage files as if you were on the local network.
- Use applications like e-mail, file transfer, and remote desktop programs directly without using a browser. For example, you can use Outlook for e-mail instead of the USG's web-based e-mail.
- Use applications, even proprietary applications, for which the USG does not offer SSL application objects.

The applications must be installed on your computer. For example, to use the VNC remote desktop program, you must have the VNC client installed on your computer.

24.1 The USG SecuExtender Icon

The USG SecuExtender icon color indicates the SSL VPN tunnel's connection status.

Figure 271 USG SecuExtender Icon

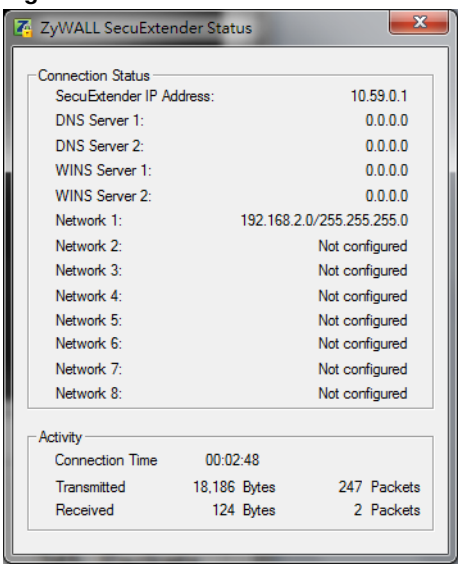


- Green: the SSL VPN tunnel is connected. You can connect to the SSL application and network resources. You can also use another application to access resources behind the USG.
- Gray: the SSL VPN tunnel's connection is suspended. This means the SSL VPN tunnel is connected, but the USG SecuExtender will not send any traffic through it until you right-click the icon and resume the connection.
- Red: the SSL VPN tunnel is not connected. You cannot connect to the SSL application and network resources.

24.2 Status

Right-click the USG SecuExtender icon in the system tray and select Status to open the Status screen. Use this screen to view the USG SecuExtender's connection status and activity statistics.

Figure 272 USG SecuExtender Status



The following table describes the labels in this screen.

Table 149 USG SecuExtender Status

LABEL	DESCRIPTION
Connection Status	
SecuExtender IP Address	This is the IP address the USG assigned to this remote user computer for an SSL VPN connection.
DNS Server 1/2	These are the IP addresses of the DNS server and backup DNS server for the SSL VPN connection. DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. Your computer uses the DNS server specified here to resolve domain names for resources you access through the SSL VPN connection.
WINS Server 1/2	These are the IP addresses of the WINS (Windows Internet Naming Service) and backup WINS servers for the SSL VPN connection. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Network 1~8	These are the networks (including netmask) that you can access through the SSL VPN connection.
Activity	
Connected Time	This is how long the computer has been connected to the SSL VPN tunnel.
Transmitted	This is how many bytes and packets the computer has sent through the SSL VPN connection.
Received	This is how many bytes and packets the computer has received through the SSL VPN connection.

24.3 View Log

If you have problems with the USG SecuExtender, customer support may request you to provide information from the log. Right-click the USG SecuExtender icon in the system tray and select Log to open a notepad file of the USG SecuExtender's log.

Figure 273 USG SecuExtender Log Example

```
################################################################################
##############
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Build Datetime: Feb 24 2009/
10:25:07
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG]   rasphone.pbk: C:\Documents and
Settings\11746\rasphone.pbk
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG]   SecuExtender.log:
C:\Documents and Settings\11746\SecuExtender.log
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Check Parameters
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Connect to 172.23.31.19:443/
10444
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Parameter is OK
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Checking System status...
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Checking service (first) ...
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  SecuExtender Helper is running
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  System is OK
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG]   Connect to 2887196435/443
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Handshake LoopCounter: 0
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  611 bytes of handshake data
received
```

24.4 Suspend and Resume the Connection

When the USG SecuExtender icon in the system tray is green, you can right-click the icon and select Suspend Connection to keep the SSL VPN tunnel connected but not send any traffic through it until you right-click the icon and resume the connection.

24.5 Stop the Connection

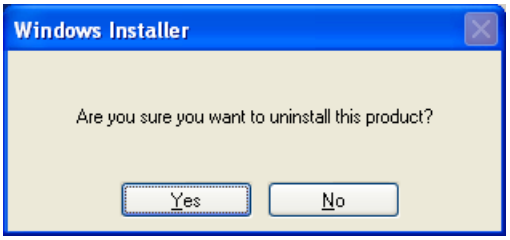
Right-click the icon and select Stop Connection to disconnect the SSL VPN tunnel.

24.6 Uninstalling the USG SecuExtender

Do the following if you need to remove the USG SecuExtender.

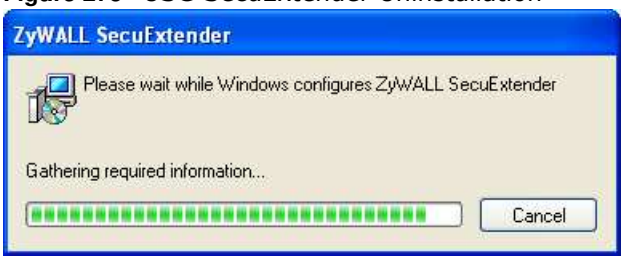
1. Click start > All Programs > ZyXEL > USG SecuExtender > Uninstall ZyWALL SecuExtender.
2. In the confirmation screen, click Yes.

Figure 274 Uninstalling the USG SecuExtender Confirmation



3 Windows uninstalls the USG SecuExtender.

Figure 275 USG SecuExtender Uninstallation



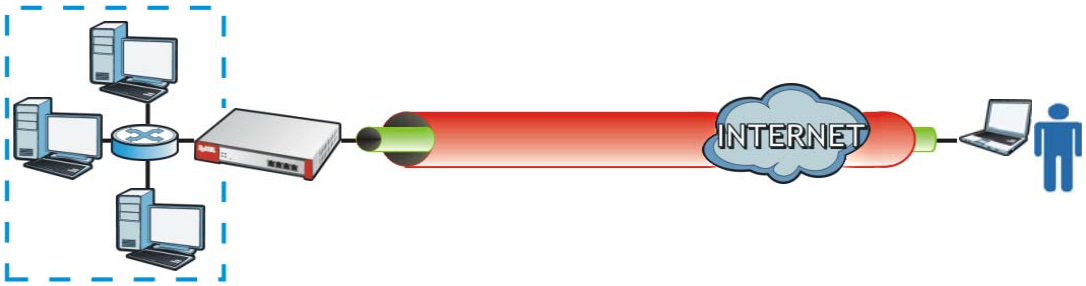
25

L2TP VPN

25.1 Overview

L2TP VPN uses the L2TP and IPSec client software included in remote users' Android, iOS, Windows or Mac OS X operating systems for secure connections to the network behind the USG. The remote users do not need their own IPSec gateways or third-party VPN client software.

Figure 276 L2TP VPN Overview



25.1.1 What You Can Do in this Chapter

- Use the L2TP VPN screen (see Section 25.2 on page 397) to configure the USG's L2TP VPN settings.
- Use the VPN Setup Wizard screen in Quick Setup (Chapter 4 on page 50) to configure the USG's L2TP VPN settings.

25.1.2 What You Need to Know

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first and then an L2TP tunnel is built inside it. See Chapter 21 on page 333 for information on IPSec VPN.

IPSec Configuration Required for L2TP VPN

You must configure an IPSec VPN connection prior to proper L2TP VPN usage (see Chapter 25 on page 396 for details). The IPSec VPN connection must:

- Be enabled.
- Use transport mode.
- Use Pre-Shared Key authentication.
- Use a VPN gateway with the Secure Gateway set to 0.0.0.0 if you need to allow L2TP VPN clients to connect from more than one IP address.

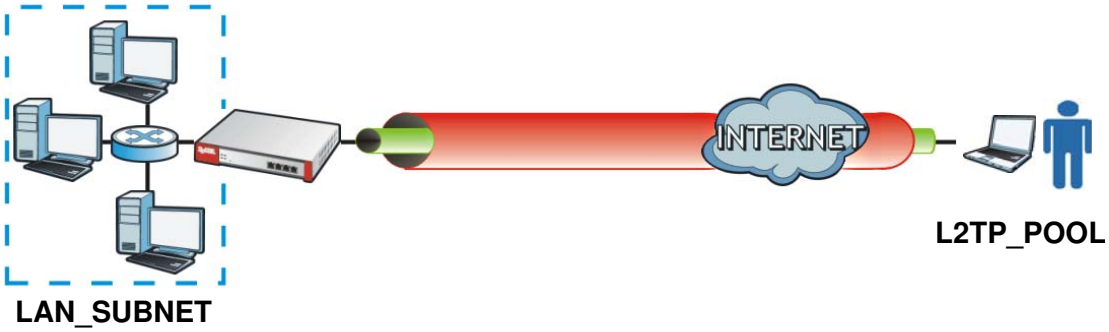
Using the Quick Setup VPN Setup Wizard

The VPN Setup Wizard is an easy and convenient way to configure the L2TP VPN settings. Click Configuration > Quick Setup > VPN Setup > VPN Settings for L2TP VPN Settings to get started.

Policy Route

The Policy Route for return traffic (from LAN to L2TP clients) is automatically created when USG adds a new L2TP connection, allowing users access the resources on a network without additional configuration. However, if some of the traffic from the L2TP clients needs to go to the Internet, you will need to create a policy route to send that traffic from the L2TP tunnels out through a WAN trunk. This task can be easily performed by clicking the Allow L2TP traffic through WAN checkbox at Quick Setup > VPN Setup > Allow L2TP traffic through WAN.

Figure 277 Policy Route for L2TP VPN



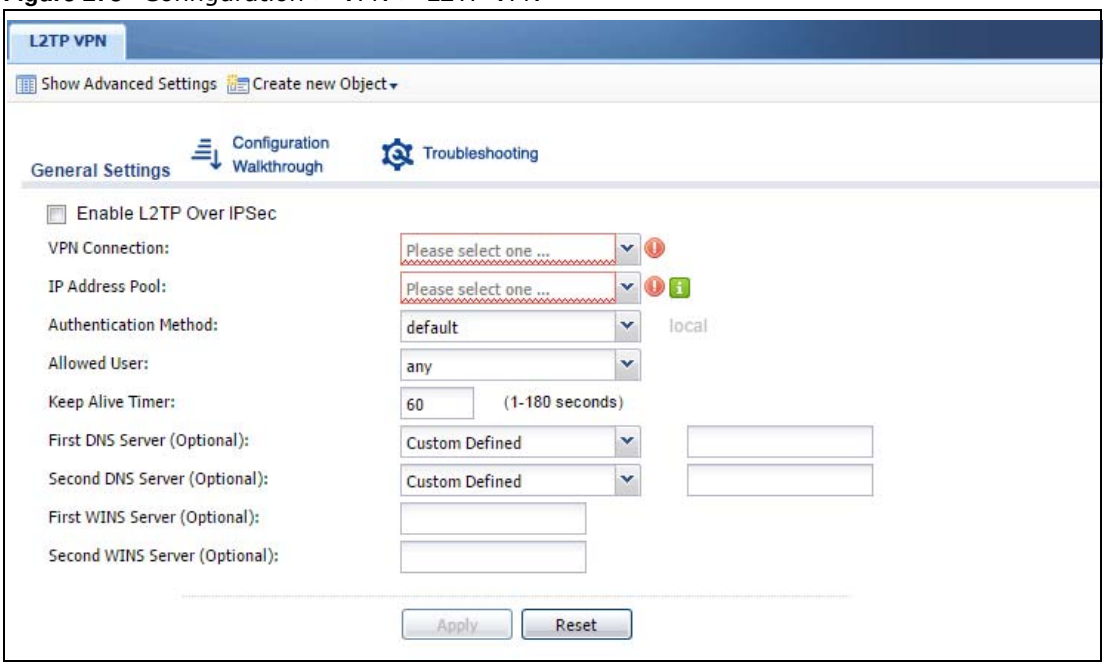
25.2 L2TP VPN Screen

Click Configuration > VPN > L2TP VPN to open the following screen. Use this screen to configure the USG's L2TP VPN settings.

Note: Disconnect any existing L2TP VPN sessions before modifying L2TP VPN settings. The remote users must make any needed matching configuration changes and re-establish the sessions using the new settings.

Click on the icons to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting, and other information.

Figure 278 Configuration > VPN > L2TP VPN



The following table describes the fields in this screen.

Table 150 Configuration > VPN > L2TP VPN

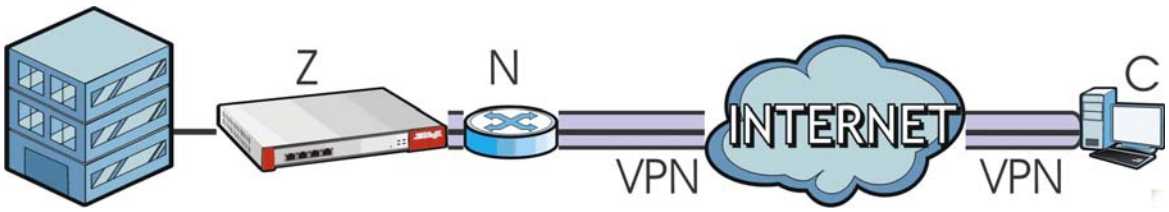
LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable L2TP Over IPSec	Use this field to turn the USG's L2TP VPN function on or off.
VPN Connection	Select the IPSec VPN connection the USG uses for L2TP VPN. All of the configured VPN connections display here, but the one you use must meet the requirements listed in IPSec Configuration Required for L2TP VPN on page 396. Note: Modifying this VPN connection (or the VPN gateway that it uses) disconnects any existing L2TP VPN sessions.
IP Address Pool	Select the pool of IP addresses that the USG uses to assign to the L2TP VPN clients. Use Create new Object if you need to configure a new pool of IP addresses. This should not conflict with any WAN, LAN, DMZ or WLAN subnet even if they are not in use.
Authentication Method	Select how the USG authenticates a remote user before allowing access to the L2TP VPN tunnel. The authentication method has the USG check a user's user name and password against the USG's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these.
Authentication Server Certificate	Select the certificate to use to identify the USG for L2TP VPN connections. You must have certificates already configured in the My Certificates screen. The certificate is used with the EAP, PEAP, and MSCHAPv2 authentication protocols.

Table 150 Configuration > VPN > L2TP VPN (continued)

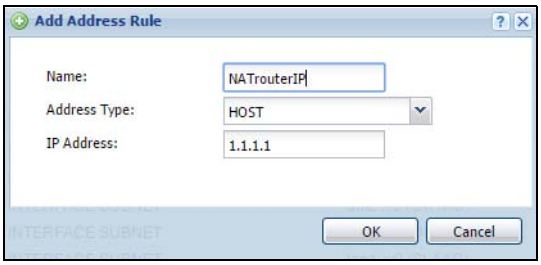
LABEL	DESCRIPTION
Allowed User	The remote user must log into the USG to use the L2TP VPN tunnel. Select a user or user group that can use the L2TP VPN tunnel. Use Create new Object if you need to configure a new user account. Otherwise, select any to allow any user with a valid account and password on the USG to log in.
Keep Alive Timer	The USG sends a Hello message after waiting this long without receiving any traffic from the remote user. The USG disconnects the VPN tunnel if the remote user does not respond.
First DNS Server, Second DNS Server	Specify the IP addresses of DNS servers to assign to the remote users. You can specify these IP addresses two ways. Custom Defined - enter a static IP address. From ISP - use the IP address of a DNS server that another interface received from its DHCP server.
First WINS Server, Second WINS Server	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Type the IP addresses of up to two WINS servers to assign to the remote users. You can specify these IP addresses two ways.
Apply	Click Apply to save your changes in the USG.
Reset	Click Reset to return the screen to its last-saved settings.

25.2.1 Example: L2TP and USG Behind a NAT Router

If the USG (Z) is behind a NAT router (N), then do the following for remote clients (C) to access the network behind the USG (Z) using L2TP over IPv4.



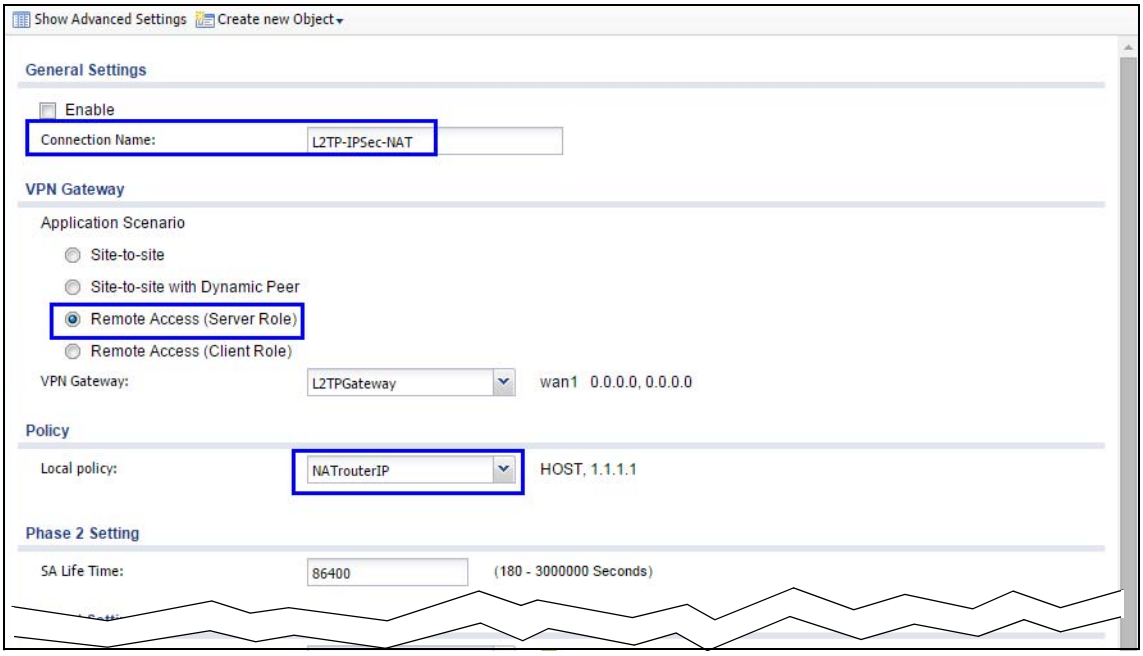
1 Create an address object in Configuration > Object > Address for the WAN IP address of the NAT router.



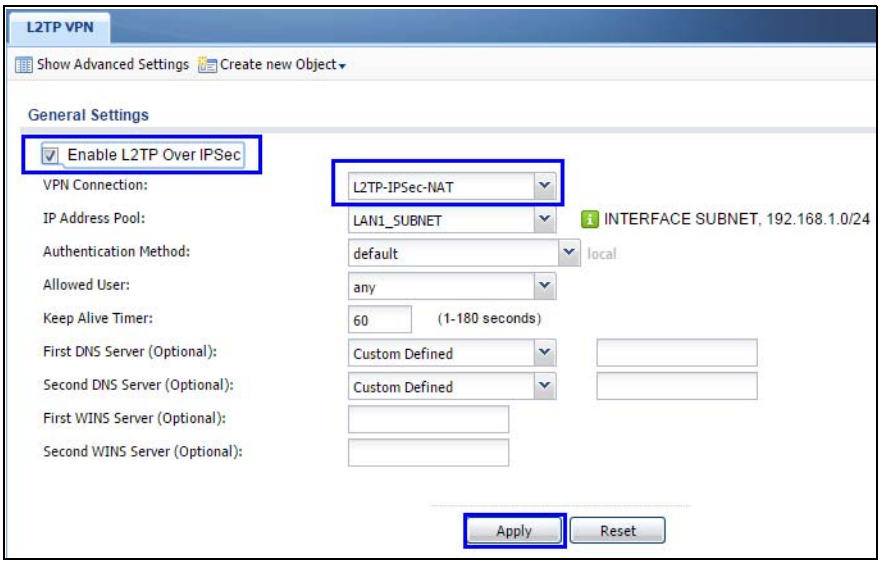
2 Go to Configuration > VPN > IPSec VPN > VPN Connection and click Add for IPv4 Configuration to create a new VPN connection.

3 Select Remote Access (Server Role) as the VPN scenario for the remote client.

4 Select the NAT router WAN IP address object as the Local Policy.



5 Go to Configuration > VPN > L2TP VPN and select the VPN Connection just configured.



26

BWM (Bandwidth Management)

26.1 Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

26.1.1 What You Can Do in this Chapter

Use the BWM screens (see Section 26.2 on page 405) to control bandwidth for services passing through the USG, and to identify the conditions that define the bandwidth control.

26.1.2 What You Need to Know

When you allow a service, you can restrict the bandwidth it uses. It controls TCP and UDP traffic. Use policy routes to manage other types of traffic (like ICMP).

Note: Bandwidth management in policy routes has priority over TCP and UDP traffic policies.

If you want to use a service, make sure both the security policy allow the service's packets to go through the USG.

Note: The USG checks security policies before it checks bandwidth management rules for traffic going through the USG.

Bandwidth management examines every TCP and UDP connection passing through the USG. Then, you can specify, by port, whether or not the USG continues to route the connection.

BWM Type

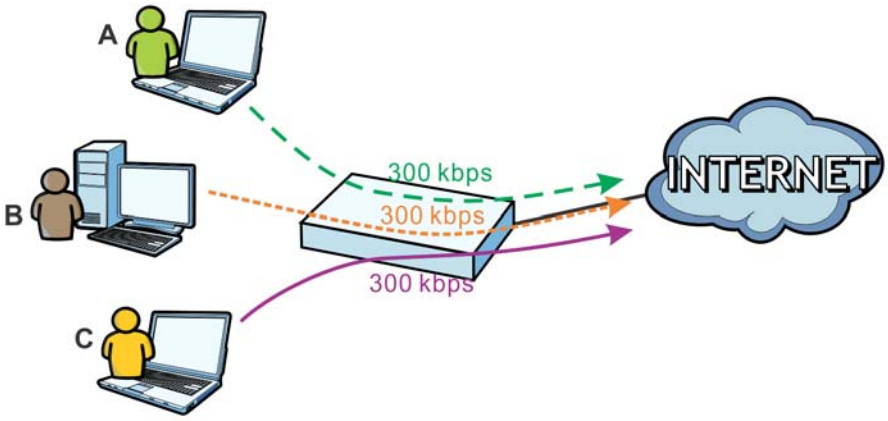
The USG supports three types of bandwidth management: Shared, Per user and Per-Source-IP.

The Shared BWM type is selected by default in a bandwidth management rule. All matched taffic shares the bandwidth configured in the rule.

If the BWM type is set to Per user in a rule, each user that matches the rule can use up to the configured bandwidth by his/her own.

Select the Per-Source-IP type when you want to set the maximum bandwidth for traffic from an individual source IP address.

In the following example, you configure a Per user bandwidth management rule for radius-users to limit outgoing traffic to 300 kbs. Then all radius-users (A, B and C) can send 300 kbps of traffic.



DiffServ and DSCP Marking

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

Connection and Packet Directions

Bandwidth management looks at the connection direction, that is, from which interface the connection was initiated and to which interface the connection is going.

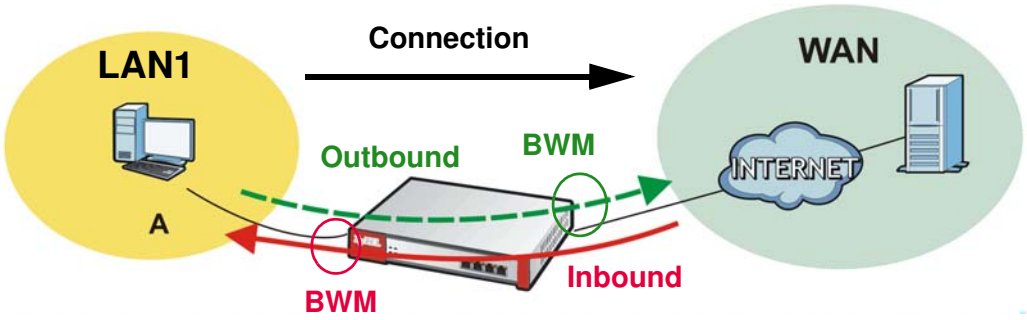
A connection has outbound and inbound packet flows. The USG controls the bandwidth of traffic of each flow as it is going out through an interface or VPN tunnel.

- The outbound traffic flows from the connection initiator to the connection responder.
- The inbound traffic flows from the connection responder to the connection initiator.

For example, a LAN1 to WAN connection is initiated from LAN1 and goes to the WAN.

- Outbound traffic goes from a LAN1 device to a WAN device. Bandwidth management is applied before sending the packets out a WAN interface on the USG.
- Inbound traffic comes back from the WAN device to the LAN1 device. Bandwidth management is applied before sending the traffic out a LAN1 interface.

Figure 279 LAN1 to WAN Connection and Packet Directions

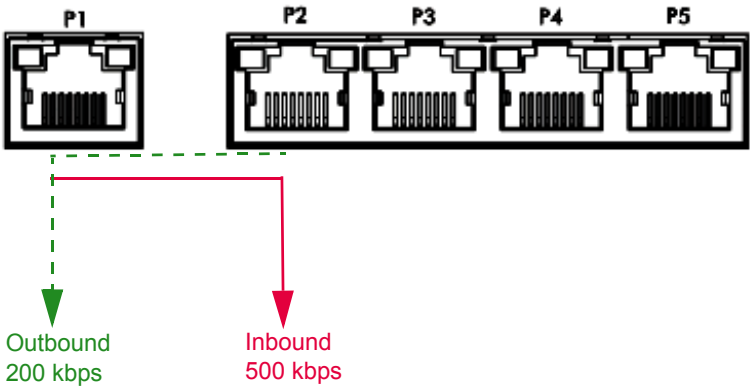


Outbound and Inbound Bandwidth Limits

You can limit an application's outbound or inbound bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. When you apply a bandwidth limit to outbound or inbound traffic, each member of the out-going zone can send up to the limit. Take a LAN1 to WAN policy for example.

- Outbound traffic is limited to 200 kbps. The connection initiator is on the LAN1 so outbound means the traffic traveling from the LAN1 to the WAN. Each of the WAN zone's two interfaces can send the limit of 200 kbps of traffic.
- Inbound traffic is limited to 500 kbs. The connection initiator is on the LAN1 so inbound means the traffic traveling from the WAN to the LAN1.

Figure 280 LAN1 to WAN, Outbound 200 kbps, Inbound 500 kbps



Bandwidth Management Priority

- The USG gives bandwidth to higher-priority traffic first, until it reaches its configured bandwidth rate.
- Then lower-priority traffic gets bandwidth.
- The USG uses a fairness-based (round-robin) scheduler to divide bandwidth among traffic flows with the same priority.
- The USG automatically treats traffic with bandwidth management disabled as priority 7 (the lowest priority).

Maximize Bandwidth Usage

Maximize bandwidth usage allows applications with maximize bandwidth usage enabled to "borrow" any unused bandwidth on the out-going interface.

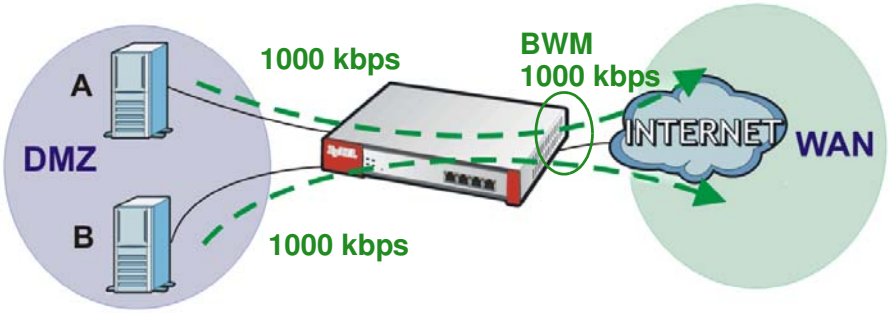
After each application gets its configured bandwidth rate, the USG uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.

Unused bandwidth is divided equally. Higher priority traffic does not get a larger portion of the unused bandwidth.

Bandwidth Management Behavior

The following sections show how bandwidth management behaves with various settings. For example, you configure DMZ to WAN policies for FTP servers A and B. Each server tries to send 1000 kbps, but the WAN is set to a maximum outgoing speed of 1000 kbps. You configure policy A for server A's traffic and policy B for server B's traffic.

Figure 281 Bandwidth Management Behavior



Configured Rate Effect

In the following table the configured rates total less than the available bandwidth and maximize bandwidth usage is disabled, both servers get their configured rate.

Table 151 Configured Rate Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	No	1	300 kbps
B	200 kbps	No	1	200 kbps

Priority Effect

Here the configured rates total more than the available bandwidth. Because server A has higher priority, it gets up to it's configured rate (800 kbps), leaving only 200 kbps for server B.

Table 152 Priority Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	800 kbps	Yes	1	800 kbps
B	1000 kbps	Yes	2	200 kbps

Maximize Bandwidth Usage Effect

With maximize bandwidth usage enabled, after each server gets its configured rate, the rest of the available bandwidth is divided equally between the two. So server A gets its configured rate of 300 kbps and server B gets its configured rate of 200 kbps. Then the USG divides the remaining bandwidth (1000 - 500 = 500) equally between the two (500 / 2 = 250 kbps for each). The priority has no effect on how much of the unused bandwidth each server gets.

So server A gets its configured rate of 300 kbps plus 250 kbps for a total of 550 kbps. Server B gets its configured rate of 200 kbps plus 250 kbps for a total of 450 kbps.

Table 153 Maximize Bandwidth Usage Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	Yes	1	550 kbps
B	200 kbps	Yes	2	450 kbps

Priority and Over Allotment of Bandwidth Effect

Server A has a configured rate that equals the total amount of available bandwidth and a higher priority. You should regard extreme over allotment of traffic with different priorities (as shown here) as a configuration error. Even though the USG still attempts to let all traffic get through and not be lost, regardless of its priority, server B gets almost no bandwidth with this configuration.

Table 154 Priority and Over Allotment of Bandwidth Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	1000 kbps	Yes	1	999 kbps
B	1000 kbps	Yes	2	1 kbps

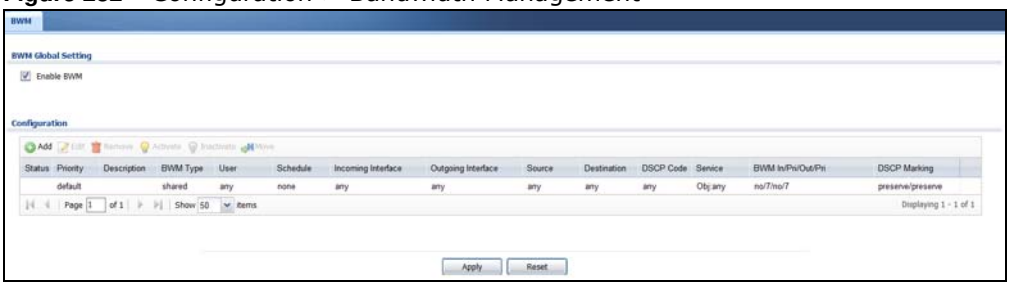
26.2 The Bandwidth Management Screen

The Bandwidth management screens control the bandwidth allocation for TCP and UDP traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions, similar to the sequence of rules used by firewalls, to specify how the USG handles the DSCP value and allocate bandwidth for the matching packets.

Click Configuration > BWM to open the following screen. This screen allows you to enable/disable bandwidth management and add, edit, and remove user-defined bandwidth management policies.

The default bandwidth management policy is the one with the priority of "default". It is the last policy the USG checks if traffic does not match any other bandwidth management policies you have configured. You cannot remove, activate, deactivate or move the default bandwidth management policy.

Figure 282 Configuration > Bandwidth Management



The following table describes the labels in this screen. See Section 26.2.1 on page 407 for more information as well.

Table 155 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Enable BWM	Select this check box to activate management bandwidth.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	To change an entry's position in the numbered list, select it and click Move to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The status icon is not available for the default bandwidth management policy.
Priority	This field displays a sequential value for each bandwidth management policy and it is not associated with a specific setting. This field displays default for the default bandwidth management policy.
Description	This field displays additional information about this policy.
BWM Type	This field displays the below types of BWM: • Shared, when the policy is set for all matched traffic • Per User, when the policy is set for an individual user or a user group • Per-Source-IP, when the policy is set for a source IP
User	This is the type of user account to which the policy applies. If any displays, the policy applies to all user accounts.
Schedule	This is the schedule that defines when the policy applies. none means the policy always applies.
Incoming Interface	This is the source interface of the traffic to which this policy applies.
Outgoing Interface	This is the destination interface of the traffic to which this policy applies.
Source	This is the source address or address group for whom this policy applies. If any displays, the policy is effective for every source.
Destination	This is the destination address or address group for whom this policy applies. If any displays, the policy is effective for every destination.

Table 155 Configuration > Bandwidth Management

LABEL	DESCRIPTION
DSCP Code	These are the DSCP code point values of incoming and outgoing packets to which this policy applies. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. any means all DSCP value or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic The "af" options stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences.
Service Type	App and the service name displays if you selected Application Object for the service type. An Application Object is a pre-defined service. Obj and the service name displays if you selected Service Object for the service type. A Service Object is a customized pre-defined service or another service. Mouse over the service object name to view the corresponding IP protocol number.
BWM In/Pri/Out/Pri	This field shows the amount of bandwidth the traffic can use. In - This is how much inbound bandwidth, in kilobits per second, this policy allows the matching traffic to use. Inbound refers to the traffic the USG sends to a connection's initiator. If no displays here, this policy does not apply bandwidth management for the inbound traffic. Out - This is how much outgoing bandwidth, in kilobits per second, this policy allows the matching traffic to use. Outbound refers to the traffic the USG sends out from a connection's initiator. If no displays here, this policy does not apply bandwidth management for the outbound traffic. Pri - This is the priority for the incoming (the first Pri value) or outgoing (the second Pri value) traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The USG ignores this number if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.
DSCP Marking	This is how the USG handles the DSCP value of the incoming and outgoing packets that match this policy. In - Inbound, the traffic the USG sends to a connection's initiator. Out - Outbound, the traffic the USG sends out from a connection's initiator. If this field displays a DSCP value, the USG applies that DSCP value to the route's outgoing packets. preserve means the USG does not modify the DSCP value of the route's outgoing packets. default means the USG sets the DSCP value of the route's outgoing packets to 0. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

26.2.1 The Bandwidth Management Add/Edit Screen

The Configuration > Bandwidth Management Add/Edit screen allows you to create a new condition or edit an existing one.

802.1P Marking

Use 802.1P to prioritize outgoing traffic from a VLAN interface. The Priority Code is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest.

Table 156 Single Tagged 802.1Q Frame Format

			DA	SA	TPID	Priority	VID	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame

Table 157 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame
TPID	Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

The following table is a guide to types of traffic for the priority code.

Table 158 Priority Code and Types of Traffic

PRIORITY	TRAFFIC TYPES
0 (lowest)	Background
1	Best Effort
2	Excellent Effort
3	Critical Applications
4	Video, less than 100 ms latency and jitter
5	Voice, less than 10 ms latency and jitter
6	Internetwork Control
7 (highest)	Network Control

To access this screen, go to the Configuration > Bandwidth Management screen (see Section 26.2 on page 405), and click either the Add icon or an Edit icon.

Figure 283 Configuration > Bandwidth Management > Edit (For the Default Policy)

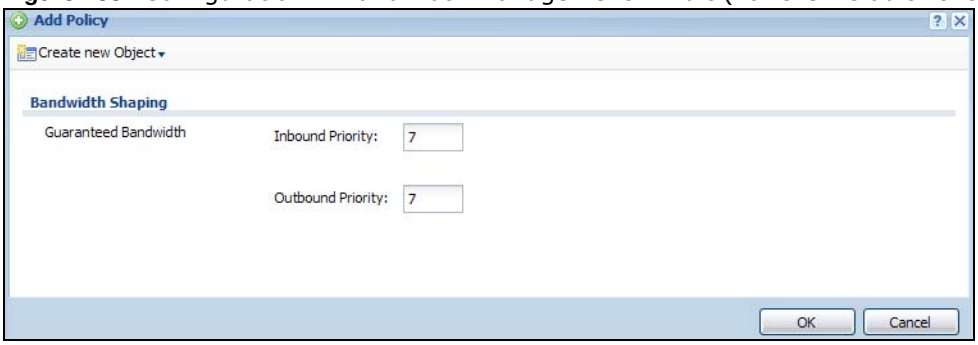
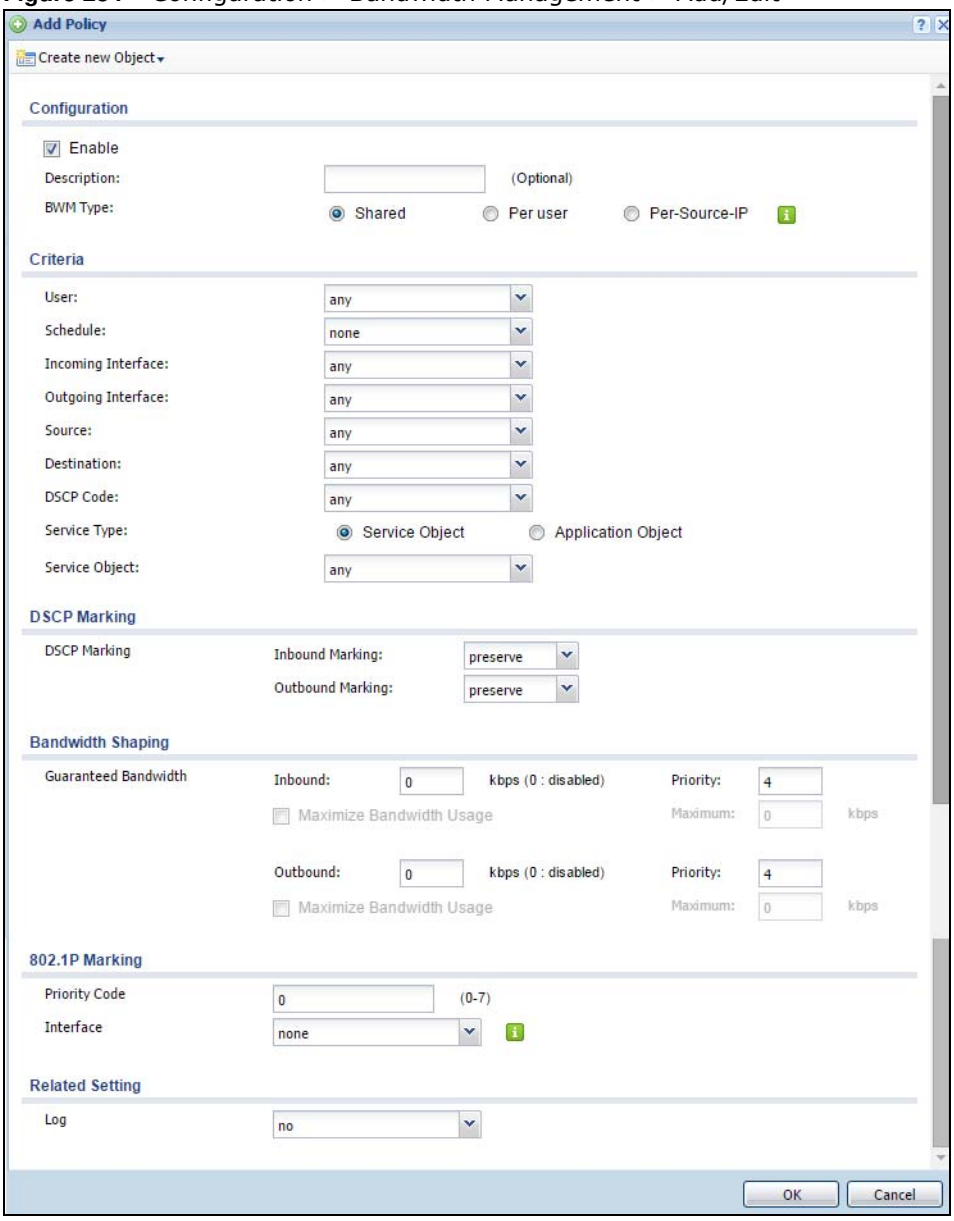


Figure 284 Configuration > Bandwidth Management > Add/Edit



The following table describes the labels in this screen.

Table 159 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Configuration	
Enable	Select this check box to turn on this policy.
Description	Enter a description of this policy. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Criteria	Use this section to configure the conditions of traffic to which this policy applies.

Table 159 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
BWM Type	This field displays the below types of BWM rule: • Shared, when the policy is set for all users • Per User, when the policy is set for an individual user or a user group • Per Source IP, when the policy is set for a source IP
User	Select a user name or user group to which to apply the policy. Use Create new Object if you need to configure a new user account. Select any to apply the policy for every user.
Schedule	Select a schedule that defines when the policy applies or select Create Object to configure a new one. Otherwise, select none to make the policy always effective.
Incoming Interface	Select the source interface of the traffic to which this policy applies.
Outgoing Interface	Select the destination interface of the traffic to which this policy applies.
Source	Select a source address or address group for whom this policy applies. Use Create new Object if you need to configure a new one. Select any if the policy is effective for every source.
Destination	Select a destination address or address group for whom this policy applies. Use Create new Object if you need to configure a new one. Select any if the policy is effective for every destination.
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select User Defined to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. any means all DSCP value or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point.
Service Type	Select Service Object if you want a specific service (defined in a service object) to which the policy applies.
Service Object	This field is available if you selected Service Object as the service type. Select a service or service group to identify the type of traffic to which this policy applies. any means all services.
DSCP Marking	Set how the USG handles the DSCP value of the incoming and outgoing packets that match this policy. Inbound refers to the traffic the USG sends to a connection's initiator. Outbound refers to the traffic the USG sends out from a connection's initiator. Select one of the pre-defined DSCP values to apply or select User Defined to specify another DSCP value. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. Select preserve to have the USG keep the packets' original DSCP value. Select default to have the USG set the DSCP value of the packets to 0.
Bandwidth Shaping	Configure these fields to set the amount of bandwidth the matching traffic can use.

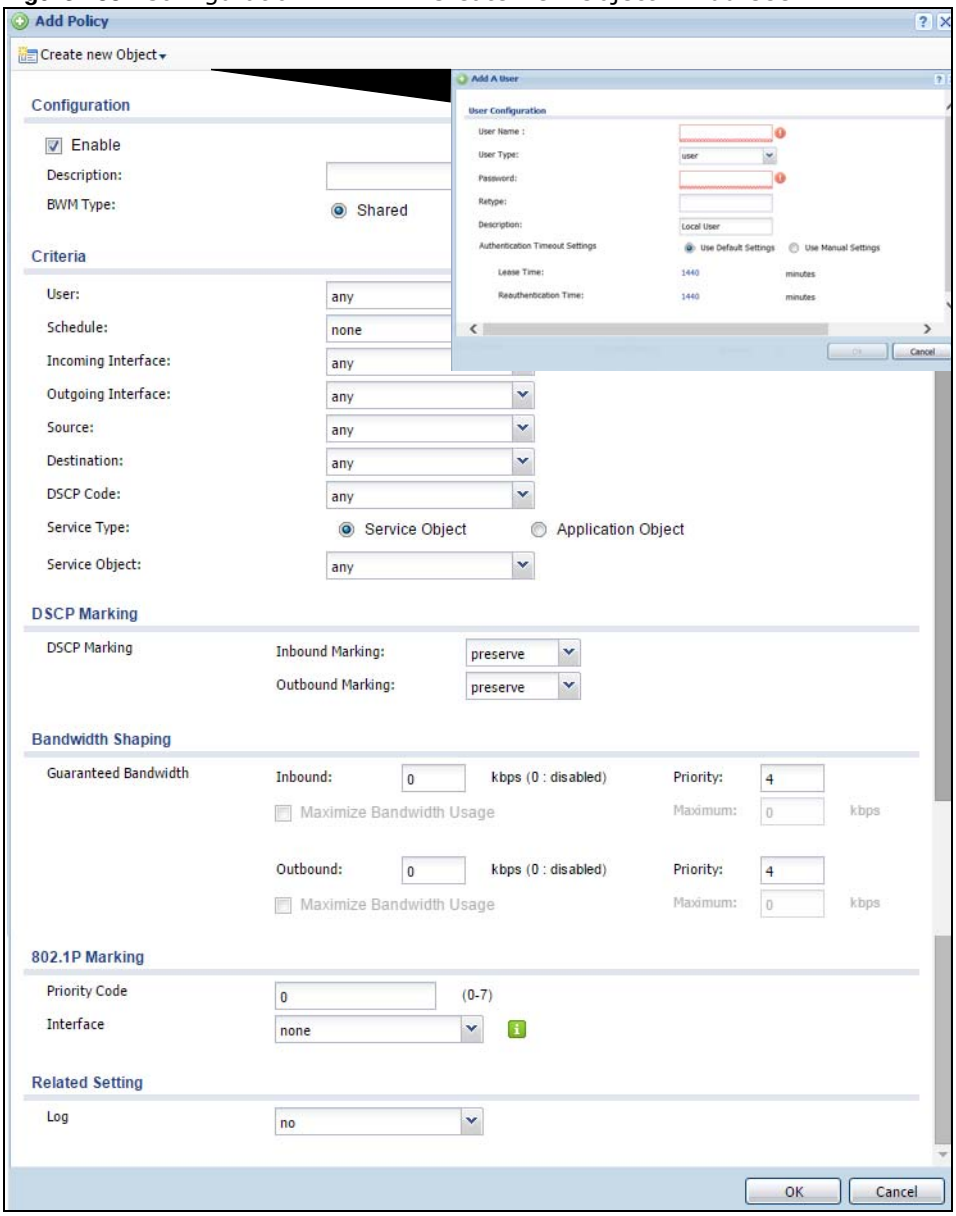
Table 159 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
Inbound kbps	Type how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use. Inbound refers to the traffic the USG sends to a connection's initiator. If you enter 0 here, this policy does not apply bandwidth management for the matching traffic that the USG sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Outbound kbps	Type how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use. Outbound refers to the traffic the USG sends out from a connection's initiator. If you enter 0 here, this policy does not apply bandwidth management for the matching traffic that the USG sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Priority	This field displays when the inbound or outbound bandwidth management is not set to 0. Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The USG uses a fairness-based (round-robin) scheduler to divide bandwidth between traffic flows with the same priority. The number in this field is ignored if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.
Maximize Bandwidth Usage	This field displays when the inbound or outbound bandwidth management is not set to 0 and the BWM Type is set to Shared. Enable maximize bandwidth usage to let the traffic matching this policy "borrow" all unused bandwidth on the out-going interface. After each application or type of traffic gets its configured bandwidth rate, the USG uses the fairness-based scheduler to divide any unused bandwidth on the out-going interface among applications and traffic types that need more bandwidth and have maximize bandwidth usage enabled.
Maximum	If you did not enable Maximize Bandwidth Usage, then type the maximium unused bandwidth that traffic matching this policy is allowed to "borrow" on the out-going interface (in Kbps), here.
802.1P Marking	Use 802.1P to prioritize outgoing traffic from a VLAN interface.
Priority Code	This is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest. See Table 158 on page 408. The setting configured here overwrites existing priority settings.
Interface	Choose a VLAN interface to which to apply the priority level for matching frames.
Related Setting	
Log	Select whether to have the USG generate a log (log), log and alert (log alert) or neither (no) when any traffic matches this policy.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

26.2.1.1 Adding Objects for the BWM Policy

Objects are parameters to which the Policy rules are built upon. There are three kinds of objects you can add/edit for the BWM policy, they are User, Schedule and Address objects. Click Configuration > BWM > Add > Create New Object > Add User to see the following screen.

Figure 285 Configuration >BWM > Create New Object > Add User



The following table describes the fields in the above screen.

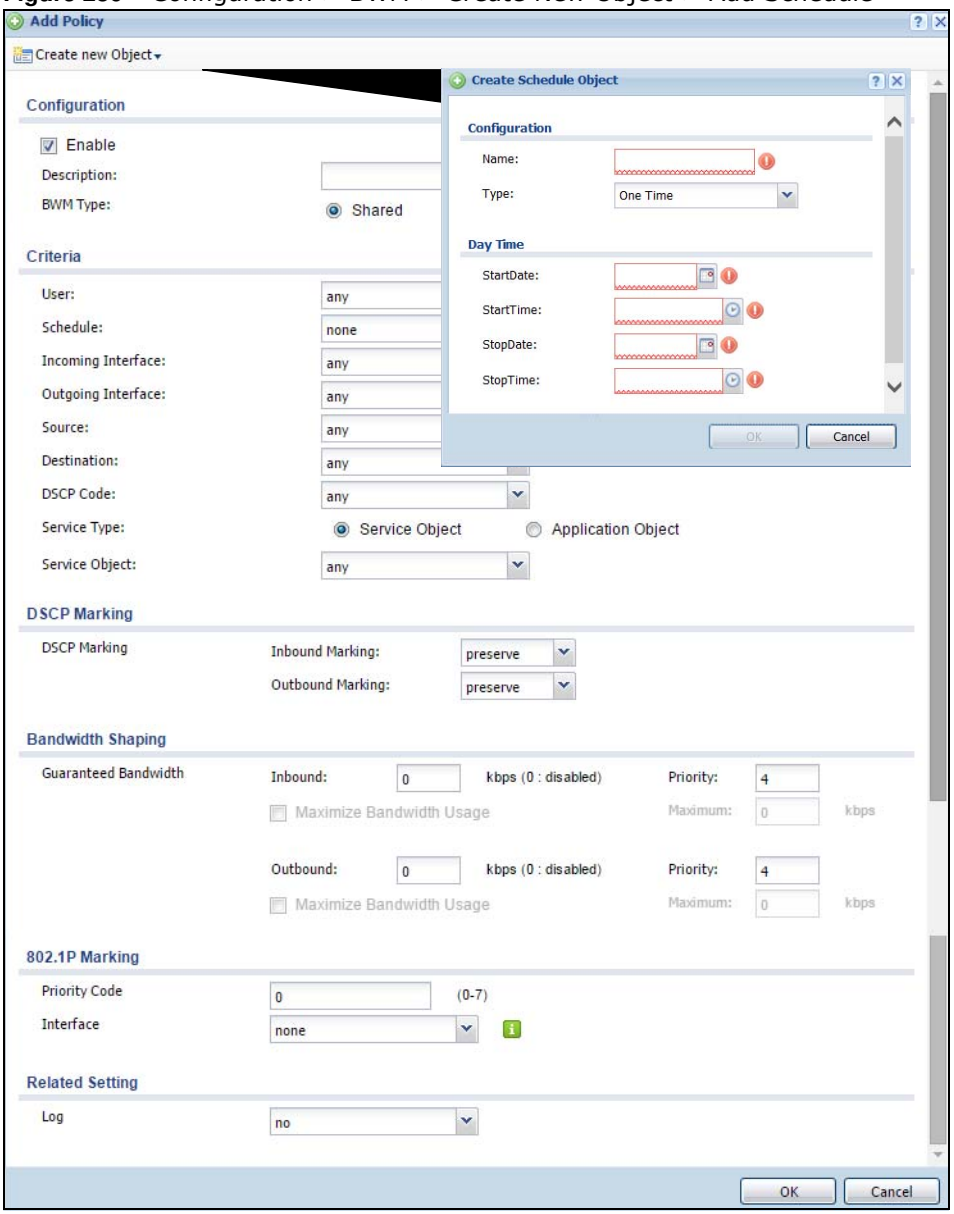
Table 160 Configuration > BWM > Create New Object > Add User

LABEL	DESCRIPTION
User Name	Type a user or user group object name of the rule.
User Type	Select a user type from the drop down menu. The user types are Admin, Limited admin, User, Guest, Ext-user, Ext-group-user.

Table 160 Configuration > BWM > Create New Object > Add User

LABEL	DESCRIPTION
Password	Type a password for the user object. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()), and it can be up to eight characters long.
Retype	Retype the password to confirm.
Description	Enter a description for this user object. It is not used elsewhere. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Authentication Timeout Settings	Choose either Use Default setting option, which shows the default Lease Time of 1,440 minutes and Reauthentication Time of 1,440 minutes or you can enter them manually by choosing Use Manual Settings option.
Lease Time	This shows the Lease Time setting for the user, by default it is 1,440 minutes.
Reauthentication Time	This shows the Reauthentication Time for the user, by default it is 1,440 minutes.
OK	Click OK to save the setting.
Cancel	Click Cancel to abandon this screen.

Figure 286 Configuration > BWM > Create New Object > Add Schedule

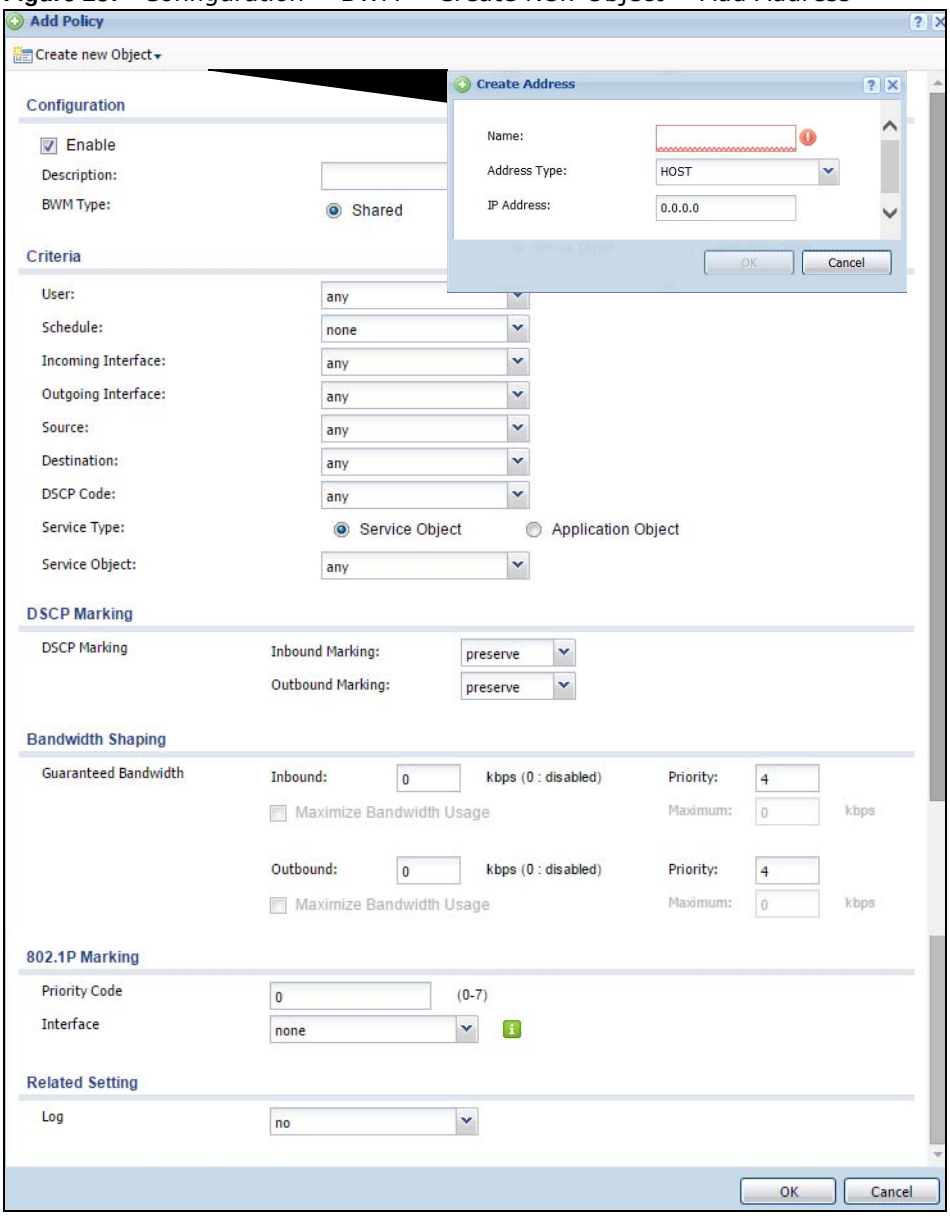


The following table describes the fields in the above screen.

Table 161 Configuration > BWM > Create New Object > Add Schedule

LABEL	DESCRIPTION
Name	Enter a name for the schedule object of the rule.
Type	Select an option from the drop down menu for the schedule object. It will show One Time or Recurring.
Start Date	Click the icon menu on the right to choose a Start Date for the schedule object.
Start Time	Click the icon menu on the right to choose a Start Time for the schedule object.
Stop Date	Click the icon menu on the right to choose a Stop Date for schedule object.
Stop Time	Click the icon menu on the right to choose a Stop Time for the schedule object.

Figure 287 Configuration > BWM > Create New Object > Add Address



The following table describes the fields in the above screen.

Table 162 Configuration > BWM > Create New Object > Add Address

LABEL	DESCRIPTION
Name	Enter a name for the Address object of the rule.
Address Type	Select an Address Type from the drop down menu on the right. The Address Types are Host, Range, Subnet, Interface IP, Interface Subnet, and Interface Gateway.
IP Address	Enter an IP address for the Address object.
OK	Click OK to save the setting.
Cancel	Click Cancel to abandon the setting.

27

Content Filtering

27.1 Overview

Use the content filtering feature to control access to specific web sites or web content.

27.1.1 What You Can Do in this Chapter

- Use the Filter Profile screens (Section Figure 289 on page 421) to set up content filtering profiles.
- Use the Trusted Web Sites screens (Section 27.4 on page 431) to create a common list of good (allowed) web site addresses.
- Use the Forbidden Web Sites screens (Section 27.5 on page 432) to create a common list of bad (blocked) web site addresses.

27.1.2 What You Need to Know

Content Filtering

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. It can also block access to specific categories of web site content. You can create different content filter policies for different addresses, schedules, users or groups and content filter profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

Content Filtering Policies

A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filter profile.
- Use address and/or user/group objects to define to whose web access to apply the content filter profile.
- Apply a content filter profile that you have custom-tailored.

Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

- Category-based Blocking

  The USG can block access to particular categories of web site content, such as pornography or racial intolerance.

- Restrict Web Features

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

- Customize Web Site Access

  You can specify URLs to which the USG blocks access. You can alternatively block access to all URLs except ones that you specify. You can also have the USG block access to URLs that contain particular keywords.

Content Filtering Configuration Guidelines

When the USG receives an HTTP request, the content filter searches for a policy that matches the source address and time (schedule). The content filter checks the policies in order (based on the policy numbers). When a matching policy is found, the content filter allows or blocks the request depending on the settings of the filtering profile specified by the policy. Some requests may not match any policy. The USG allows the request if the default policy is not set to block. The USG blocks the request if the default policy is set to block.

External Web Filtering Service

When you register for and enable the external web filtering service, your USG accesses an external database that has millions of web sites categorized based on content. You can have the USG block, block and/or log access to web sites based on these categories.

Keyword Blocking URL Checking

The USG checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the USG checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the USG would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

Finding Out More

- See Section 27.6 on page 433 for content filtering background/technical information.

27.1.3 Before You Begin

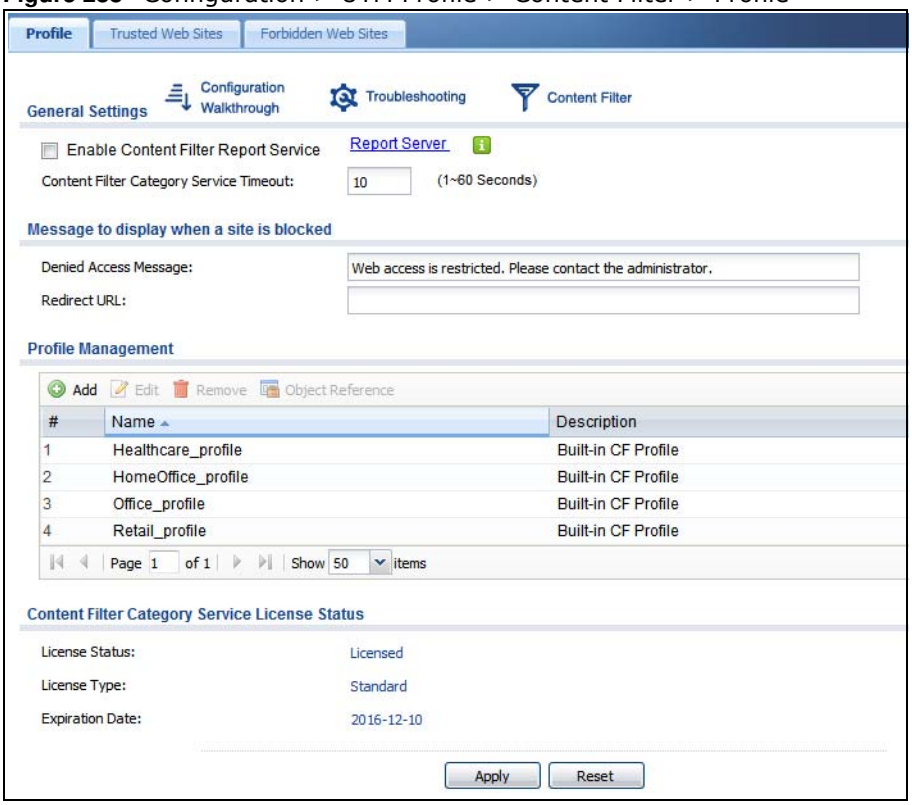
- You must configure an address object, a schedule object and a filtering profile before you can set up a content security policy.
- You must have Content Filtering license in order to use the function.subscribe to use the external database content filtering (see the Licensing > Registration screens).

27.2 Content Filter Profile Screen

Click Configuration > UTM Profile> Content Filter > Profile to open the Content Filter Profile screen. Use this screen to enable content filtering, view and order your list of content filter policies, create a denial of access message or specify a redirect URL and check your external web filtering service registration status.

Click on the icons to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting and other information.

Figure 288 Configuration > UTM Profile > Content Filter > Profile



The following table describes the labels in this screen.

Table 163 Configuration > UTM Profile > Content Filter > Profile

LABEL	DESCRIPTION
General Settings	
Enable Content Filter Report Service	Select this check box to have the USG collect category-based content filtering statistics.
Report Server	Click this link to choose where your USG is registered: myZyXEL.com or myZyXEL.com 2.0. Choose myZyXEL.com 2.0 for a model in this series.
Content Filter Category Service Timeout	Specify the allowable time period in seconds for accessing the external web filtering service's server.

Table 163 Configuration > UTM Profile > Content Filter > Profile (continued)

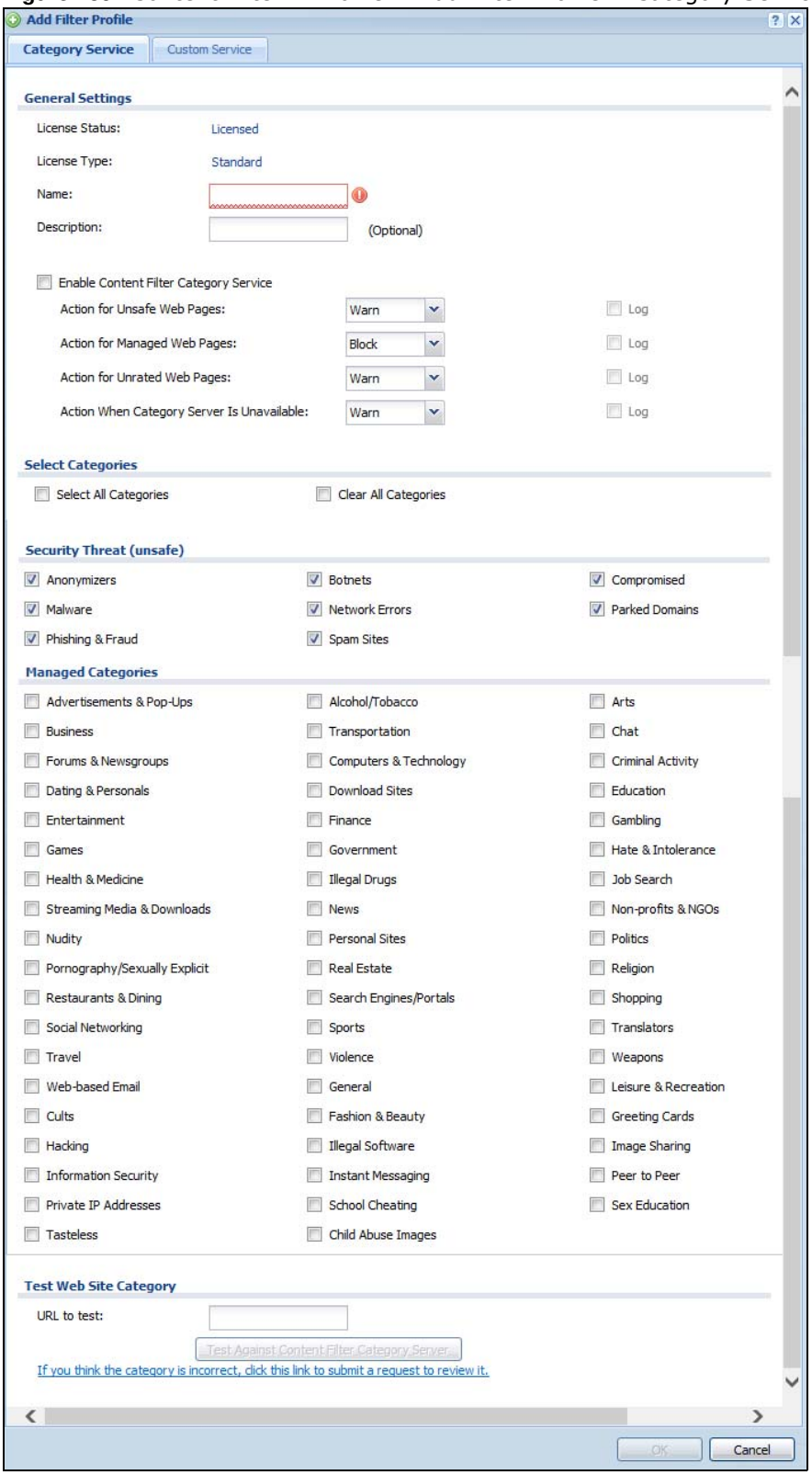
LABEL	DESCRIPTION
Denied Access Message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the Redirect URL field. In this case if the content filter blocks access to a web page, the USG just opens the web page you specified without showing a denied access message.
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Profile Management	
Add	Click Add to create a new content filter rule.
Edit	Click Edit to make changes to a content filter rule.
Remove	Click Remove the delete a content filter rule.
Object Reference	Select an entry and click Object References to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This column lists the index numbers of the content filter profile.
Name	This column lists the names of the content filter profile rule.
Description	This column lists the description of the content filter profile rule.
Reference	This displays the number of times an Object Reference is used in a rule.
License Status	This read-only field displays the status of your content-filtering database service registration. Not Licensed displays if you have not successfully registered and activated the service. Expired displays if your subscription to the service has expired. Licensed displays if you have successfully registered the USG and activated the service. You can view content filter reports after you register the USG and activate the subscription service in the Registration screen.
License Type	This read-only field displays what kind of service registration you have for the content-filtering database. None displays if you have not successfully registered and activated the service. Standard displays if you have successfully registered the USG and activated the service. Trial displays if you have successfully registered the USG and activated the trial service subscription.
Expiration Date	This field displays the date your service license expires.
Register Now	This link appears if you have not registered for the service or the service has expired. Click this link to go to the screen where you can register for the service.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

27.3 Content Filter Profile Add or Edit Screen

Click Configuration > UTM > Content Filter > Profile > Add or Edit to open the Add Filter Profile screen. Configure Category Service and Custom Service tabs.

27.3.1 Content Filter Add Profile Category Service

Figure 289 Content Filter > Profile > Add Filter Profile > Category Service



The following table describes the labels in this screen.

Table 164 Configuration > UTM Profile> Content Filter > Profile > Add > Category Service

LABEL	DESCRIPTION
License Status	This read-only field displays the status of your content-filtering database service registration. Not Licensed displays if you have not successfully registered and activated the service. Expired displays if your subscription to the service has expired. Licensed displays if you have successfully registered the USG and activated the service. You can view content filter reports after you register the USG and activate the subscription service in the Registration screen.
License Type	This read-only field displays what kind of service registration you have for the content-filtering database. None displays if you have not successfully registered and activated the service. Standard displays if you have successfully registered the USG and activated the standard content filtering service. Trial displays if you have successfully registered the USG and activated the trial service subscription.
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Enable Content Filter Category Service	Enable external database content filtering to have the USG check an external database to find to which category a requested web page belongs. The USG then blocks or forwards access to the web page depending on the configuration of the rest of this page.
Action for Unsafe Web Pages	Select Pass to allow users to access web pages that match the unsafe categories that you select below. Select Block to prevent users from accessing web pages that match the unsafe categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page. Select Warn to display a warning message before allowing users to access web pages that match the unsafe categories that you select below. Select Log to record attempts to access web pages that match the unsafe categories that you select below.

Table 164 Configuration > UTM Profile> Content Filter > Profile > Add > Category Service

LABEL	DESCRIPTION
Action for Managed Web Pages	Select Pass to allow users to access web pages that match the other categories that you select below. Select Block to prevent users from accessing web pages that match the other categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page. Select Log to record attempts to access web pages that match the other categories that you select below.
Action for Unrated Web Pages	Select Pass to allow users to access web pages that the external web filtering service has not categorized. Select Block to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page. Select Warn to display a warning message before allowing users to access web pages that the external web filtering service has not categorized. Select Log to record attempts to access web pages that are not categorized.
Action When Category Server Is Unavailable	Select Pass to allow users to access any requested web page if the external content filtering database is unavailable. Select Block to block access to any requested web page if the external content filtering database is unavailable. Select Warn to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable. The following are possible causes for the external content filtering server not being available: • There is no response from the external content filtering server within the time period specified in the Content Filter Server Unavailable Timeout field. • The USG is not able to resolve the domain name of the external content filtering database. • There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid"). Select Log to record attempts to access web pages that occur when the external content filtering database is unavailable.
Select Categories	
Select All Categories	Select this check box to restrict access to all site categories listed below.
Clear All Categories	Select this check box to clear the selected categories below.
Security Threat (unsafe)	Theese are the categories of web pages that are known to pose a threat to users or their computers.
Anonymizers	Sites and proxies that act as an intermediary for surfing to other Web sites in an anonymous fashion, whether to circumvent Web filtering or for other reasons. For example, blog.go2.tw, anonymizer.com, www.qu365.com.
Botnets	Sites that use bots (zombies) including command-and-control sites.
Compromised	Sites that have been compromised by someone other than the site owner in order to install malicious programs without the user's knowledge. Includes sites that may be vulnerable to a particular high-risk attack. For example, www.wokoo.net, movie.sx.zj.cn.

Table 164 Configuration > UTM Profile> Content Filter > Profile > Add > Category Service

LABEL	DESCRIPTION
Malware	Sites that install unwanted software on a user's computer with the intent to enable third-party monitoring or make system changes without the user's consent. For example, www.tqlkg.com, aladel.net.
Network Errors	Sites that do not resolve to any IP address.
Parked Domains	Sites that are inactive, typically reserved for later use. They most often do not contain their own content, may simply say "under construction," "purchase this domain," or display advertisements. For example, www.moemoon.com, artlin.net, img.sedoparking.com.
Phishing & Fraud	Sites that are used for deceptive or fraudulent purposes (e.g. phishing), such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials. For example, optimizedby.rmxads.com, 218.1.71.226/.../e3b.
Spam Sites	Sites that have been promoted through spam techniques. For example, img.tongji.linezing.com, banner.chinesegamer.net.
Managed Categories	These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content. You must have the Category Service content filtering license to filter these categories. See the next table for category details.
Test Web Site Category	
URL to test	You can check which category a web page belongs to. Enter a web site URL in the text box. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active.
If you think the category is incorrect	Click this link to see the category recorded in the USG's content filtering database for the web page you specified (if the database has an entry for it).
Test Against Content Filter Category Server	Click this button to see the category recorded in the external content filter server's database for the web page you specified.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

The following table describes the managed categories.

Table 165 Managed Category Descriptions

CATEGORY	DESCRIPTION
Advertisements & Pop-Ups	Sites that provide advertising graphics or other ad content files such as banners and pop-ups. For example, pagead2.googlesyndication.com, ad.yieldmanager.com.
Alcohol & Tobacco	Sites that promote or sell alcohol- or tobacco-related products or services. For example, www.drinks.com.tw, www.p9.com.tw, beer.ttl.com.tw.
Arts	Sites with artistic content or relating to artistic institutions such as theaters, museums, galleries, dance companies, photography, and digital graphic resources. For example, www.npm.gov.tw, www.nmh.gov.tw.
Business	Sites that provide business related information such as corporate Web sites. Information, services, or products that help businesses of all sizes to do their day-to-day commercial activities. For example, www.kinkos.com, www.proctorgamble.com, www.bbb.org.
Chat	Sites that enable web-based exchange of realtime messages through chat services or chat rooms. For example, me.sohu.com, blufiles.storage.live.com.

Table 165 Managed Category Descriptions (continued)

Child Abuse Images	Sites that portray or discuss children in sexual or other abusive acts. For example, a.uuzhijia.info.
Computers & Technology	Sites that contain information about computers, software, hardware, IT, peripheral and computer services, such as product reviews, discussions, and IT news. For example, www.informationsecurity.com.tw, blog.ithome.com.tw.
Criminal Activity	Sites that offer advice on how to commit illegal or criminal activities, or to avoid detection. These can include how to commit murder, build bombs, pick locks, etc. Also includes sites with information about illegal manipulation of electronic devices, hacking, fraud and illegal distribution of software. For example, www.hackbase.com, jia.hackbase.com, ad.adver.com.tw.
Cults	Sites relating to non-traditional religious practice typically known as "cults," that is, considered to be false, unorthodox, extremist, or coercive, with members often living under the direction of a charismatic leader. For example, www.churchofsatan.com, www.ccya.org.tw.
Dating & Personals	Sites that promote networking for interpersonal relationships such as dating and marriage. Includes sites for match-making, online dating, spousal introduction. For example, www.i-part.com.tw, www.imatchi.com.
Download Sites	Sites that contain downloadable software, whether shareware, freeware, or for a charge. Includes peer-to-peer sites. For example, www.hotdl.com, toget.pchome.com.tw, www.azroo.com.
Education	Sites sponsored by educational institutions and schools of all types including distance education. Includes general educational and reference materials such as dictionaries, encyclopedias, online courses, teaching aids and discussion guides. For example, www.tfam.museum, www.lksf.org, www.1980.org.tw..
Entertainment	Sites related to television, movies, music and video (including video on demand), such as program guides, celebrity sites, and entertainment news. For example, www.ctitv.com.tw, www.hboasia.com, www.startv.com.tw.
Fashion & Beauty	Sites concerning fashion, jewelry, glamour, beauty, modeling, cosmetics or related products or services. Includes product reviews, comparisons, and general consumer information. For example, women.sohu.com, baodian.women.sohu.com.
Finance	Sites related to banking, finance, payment or investment, including banks, brokerages, online stock trading, stock quotes, fund management, insurance companies, credit unions, credit card companies, and so on. For example, www.concords.com.tw, www.polaris.com.tw, www.bochk.com.
Forums & Newsgroups	Sites for sharing information in the form of newsgroups, forums, bulletin boards. For example, ck101.com, my.xuite.net, ptt.cc.
Gambling	Sites that offer or are related to online gambling, lottery, casinos and betting agencies involving chance. For example, www.taiwanlottery.com.tw, www.i-win.com.tw, www.hkjc.com.
Games	Sites relating to computer or other games, information about game producers, or how to obtain cheat codes. Game-related publication sites. For example, www.gamer.com.tw, www.wowtaiwan.com.tw, tw.lineage.gamania.com.
General	Sites that do not clearly fall into other categories, for example, blank Web pages. For example, bs.serving-sys.com, simg.sinajs.cn, i0.itc.cn.
Government	Sites run by governmental organizations, departments, or agencies, including police departments, fire departments, customs bureaus, emergency services, civil defense, counterterrorism organizations, military and hospitals. For example, www.ey.gov.tw, www.whitehouse.gov, www.npa.gov.tw.
Greeting cards	Sites that allow people to send and receive greeting cards and postcards. For example, www.e-card.com.tw, card.ivy.net.tw.

Table 165 Managed Category Descriptions (continued)

Hacking	Sites that promote or give advice about how to gain unauthorized access to proprietary computer systems, for the purpose of stealing information, perpetrating fraud, creating viruses, or committing other illegal activity related to theft of digital information. For example, www.hackbase.com, www.chinahacker.com.
Hate & Intolerance	Sites that promote a supremacist political agenda, encouraging oppression of people or groups of people based on their race, religion, gender, age, disability, sexual orientation or nationality. For example, www.racist-jokes.com, aryan-nations.org, whitepower.com.
Health & Medicine	Sites containing information pertaining to health, healthcare services, fitness and well-being, including information about medical equipment, hospitals, drugstores, nursing, medicine, procedures, prescription medications, etc. For example, www.lksf.org, www.ohayo.com.tw.
Illegal Drug	Sites with information on the purchase, manufacture, and use of illegal or recreational drugs and their paraphernalia, and misuse of prescription drugs and other compounds For example, www.cannabis.net, www.amphetamines.com.
Illegal Software	Sites that illegally distribute software or copyrighted materials such as movies or music, software cracks, illicit serial numbers, illegal license key generators. For example, www.zhaokey.com.cn, www.tiansha.net.
Image Sharing	Sites that host digital photographs and images, online photo albums and digital photo exchanges. For example, photo.pchome.com.tw, photo.xuite.net, photobucket.com.
Information Security	Sites that provide legitimate information about data protection, including newly discovered vulnerabilities and how to block them. For example, www.informationsecurity.com.tw, www.itis.tw.
Instant Messaging	Sites that enable logging in to instant messaging services such as ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, and the like. For example, www.meebo.com, www.aim.com, www. ebuddy.com.
Job Search	Sites containing job listings, career information, assistance with job searches (such as resume writing, interviewing tips, etc.), employment agencies or head hunters. For example, www.104.com.tw, www.1111.com.tw, www.yes123.com.tw.
Leisure & Recreation	Sites relating to recreational activities and hobbies including zoos, public recreation centers, pools, amusement parks, and hobbies such as gardening, literature, arts & crafts, home improvement, home d?cor, family, etc. For example, tpbg.tfri.gov.tw, tw.fashion.yahoo.com, www.relaxtimes.com.tw.
News	Sites covering news and current events such as newspapers, newswire services, personalized news services, broadcasting sites, and magazines. For example, www.tvbs.com.tw?Awww.ebc.net.tw?Awww.iset.com.tw.
Non-profits & NGOs	Sites devoted to clubs, communities, unions, and non-profit organizations. Many of these groups exist for educational or charitable purposes. For example, www.tzuchi.org.tw, web.redcross.org.tw, www.lksf.org.
Nudity	Sites that contain full or partial nudity that are not necessarily overtly sexual in intent. Includes sites that advertise or sell lingerie, intimate apparel, or swimwear. For example, www.easyshop.com.tw, www.faster-swim.com.tw, image.baidu.com.
Peer-to-Peer	Sites that enable direct exchange of files between users without dependence on a central server. For example, www.eyny.com.
Personal Sites	Sites about or hosted by personal individuals, including those hosted on commercial sites. For example, blog.yam.com, www.wretch.cc, blog.xuite.net.
Politics	Sites that promote political parties or political advocacy, or provide information about political parties, interest groups, elections, legislation or lobbying. Also includes sites that offer legal information and advice. For example, www.kmt.org.tw, www.dpp.org.tw, cpc.people.com.cn.

Table 165 Managed Category Descriptions (continued)

Pornography/Sexually Explicit	Sites that contain explicit sexual content. Includes adult products such as sex toys, CD-ROMs, and videos, adult services such as videoconferencing, escort services, and strip clubs, erotic stories and textual descriptions of sexual acts. For example, www.dvd888.com, www.18center.com, blog.sina.com.tw.
Private IP Addresses	Sites that are private IP addresses as defined in RFC 1918, that is, hosts that do not require access to hosts in other enterprises (or require just limited access) and whose IP address may be ambiguous between enterprises but are well defined within a certain enterprise. For example, 172.21.20.123, 192.168.35.62.
Real Estate	Sites relating to commercial or residential real estate services, including renting, purchasing, selling or financing homes, offices, etc. For example, www.sinyi.com.tw, www.yungching.com.tw, house.focus.cn.
Religion	Sites that deal with faith, human spirituality or religious beliefs, including sites of churches, synagogues, mosques and other houses of worship. For example, www.fgs.org.tw, www.twtaoism.net, www.fhl.net.
Restaurants & Dining	Sites that list, review, promote or advertise food, dining or catering services. Includes sites for recipes, cooking instruction and tips, food products, and wine advisors. For example, www.jogoya.com.tw, www.dintaifung.com.tw, www2.pizzahut.com.tw.
School Cheating	Sites that promote unethical practices such as cheating or plagiarism by providing test answers, written essays, research papers, or term papers. For example, www.zydk788.com, www.huafengksw.com.
Search Engines & Portals	Sites enabling the searching of the Web, newsgroups, images, directories, and other online content. Includes portal and directory sites such as white/yellow pages. For example, tw.yahoo.com, www.pchome.com.tw, www.google.com.tw.
Sex Education	Sites relating to sex education, including subjects such as respect for partner, abortion, gay and lesbian lifestyle, contraceptives, sexually transmitted diseases, and pregnancy. For example, apps.rockyou.com, www.howmama.com.tw, www.mombaby.com.tw.
Shopping	Sites for online shopping, catalogs, online ordering, auctions, classified ads. Excludes shopping for products and services exclusively covered by another category such as health & medicine. For example, shopping.pchome.com.tw, buy.yahoo.com.tw, www.tkec.com.tw.
Social Networking	Sites that enable social networking for online communities of various topics, for friendship, dating, or professional reasons. For example, www.facebook.com, www.flickr.com, www.groups.google.com.
Sports	Sites relating to sports teams, fan clubs, scores and sports news. Relates to all sports, whether professional or recreational. For example, www.yankees.com, www.nba.com, mlb.mlb.com.
Streaming Media & Downloads	Sites that deliver streaming content, such as Internet radio, Internet TV or MP3 and live or archived media download sites. Includes fan sites, or official sites run by musicians, bands, or record labels. For example, www.youtube.com, pfp.sina.com.cn, my.xunlei.com.
Tasteless	Sites with offensive or tasteless content such as bathroom humor or profanity. For example, comedycentral.com, dilbert.com.
Translators	Sites that translate Web pages or phrases from one language to another. These sites may be used to attempt to bypass a filtering system. For example, translate.google.com.tw, www.smartlinkcorp.com, translation.paralink.com.
Transportation	Sites that provide information about motor vehicles such as cars, motorcycles, boats, trucks, RVs and the like. Includes manufacturer sites, dealerships, review sites, pricing, , online purchase sites, enthusiasts clubs, etc. For example, www.toyota.com.tw, www.ford.com.tw, www.sym.com.tw.

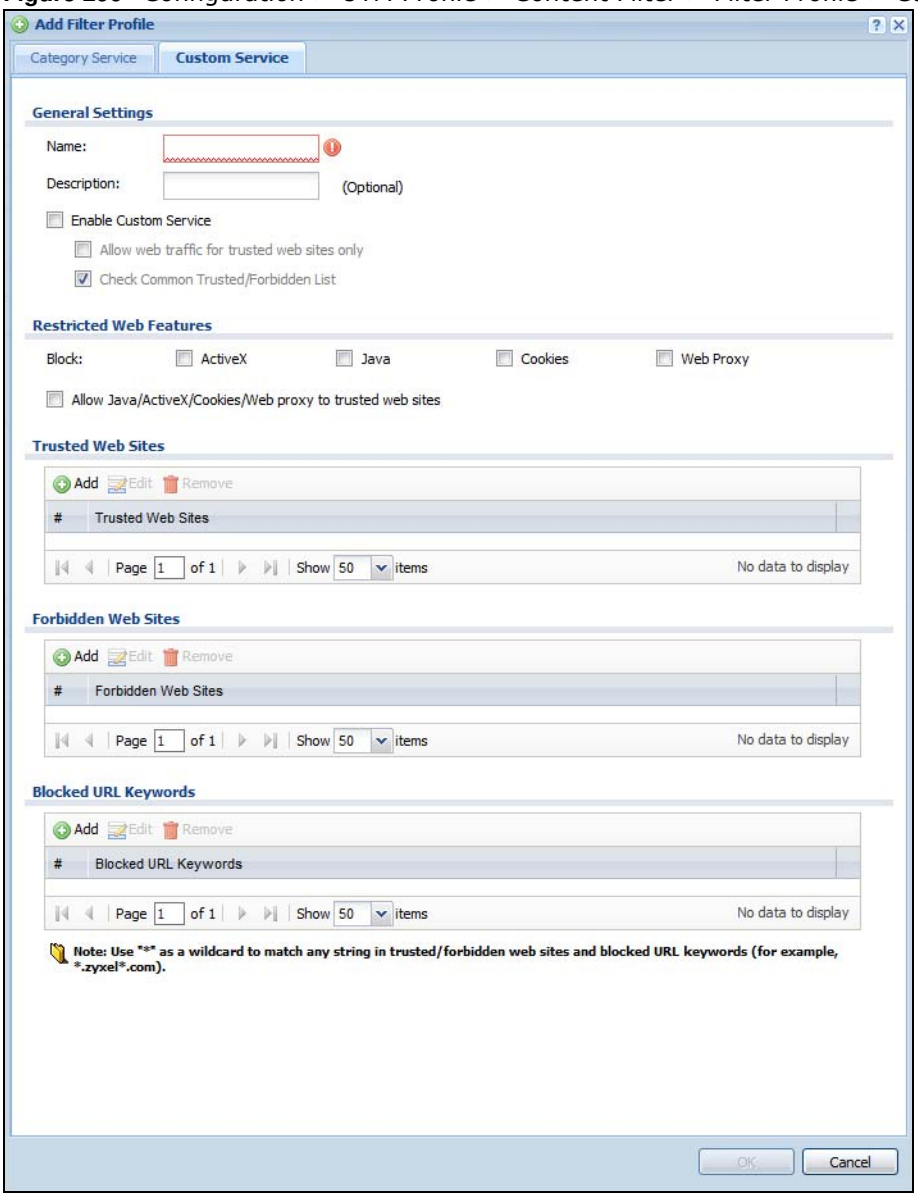
Table 165 Managed Category Descriptions (continued)

Travel	Sites that provide travel and tourism information or online booking of travel services such as airlines, accommodations, car rentals. Includes regional or city information sites. For example, www.startravel.com.tw, taipei.grand.hyatt.com.tw, www.car-plus.com.tw.
Unknown	Unknown For example, www.669.com.tw, www.appleballoon.com.tw, www.uimco.com.tw.
Violence	Sites that contain images or text depicting or advocating physical assault against humans, animals, or institutions. Sites of a particularly gruesome nature such as shocking depictions of blood or wounds, or cruel animal treatment. For example, crimescene.com, deathnet.com, michiganmilitia.com.
Weapons	Sites that depict, sell, review or describe guns and weapons, including for sport. For example, www.ak-47.net, warfare.ru.
Web-based Email	Sites that enable users to send and receive email through a web-accessible email account. For example, mail.163.com, mail.google.com, mail.yahoo.com.tw.

27.3.2 Content Filter Add Filter Profile Custom Service

Click Configuration > UTM Profile > Content Filter > Filter Profile > Add or Edit > Custom Service to open the Custom Service screen. You can create a list of good (allowed) web site addresses and a list of bad (blocked) web site addresses. You can also block web sites based on whether the web site's address contains a keyword. Use this screen to add or remove specific sites or keywords from the filter list.

Figure 290 Configuration > UTM Profile > Content Filter > Filter Profile > Custom Service



The following table describes the labels in this screen.

Table 166 Configuration > UTM Profile > Content Filter > Profile > Custom Service

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Enable Custom Service	Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names.

Table 166 Configuration > UTM Profile > Content Filter > Profile > Custom Service (continued)

LABEL	DESCRIPTION
Allow Web traffic for trusted web sites only	When this box is selected, the USG blocks Web access to sites that are not on the Trusted Web Sites list. If they are chosen carefully, this is the most effective way to block objectionable material.
Check Common Trusted/ Forbidden List	Select this check box to check the common trusted and forbidden web sites lists. See Section 27.4 on page 431 and Section 27.5 on page 432 for information on configuring these lists.
Restricted Web Features	Select the check box(es) to restrict a feature. Select the check box(es) to restrict a feature. • When you download a page containing ActiveX or Java, that part of the web page will be blocked with an X. • When you download a page coming from a Web Proxy, the whole web page will be blocked. • When you download a page containing cookies, the cookies will be removed, but the page will not be blocked.
Block ActiveX	ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Allow Java/ActiveX/Cookies/ Web proxy to trusted web sites	When this box is selected, the USG will permit Java, ActiveX and Cookies from sites on the Trusted Web Sites list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted.
Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the trusted web sites.
Trusted Web Site	This column displays the trusted web sites already added. 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", and so on. You can also enter just a top level domain. For example, enter "*.com" to allow all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter. "*" can be used as a wildcard to match any string. The entry must contain at least one "." or it will be invalid.
Forbidden Web Site List	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.

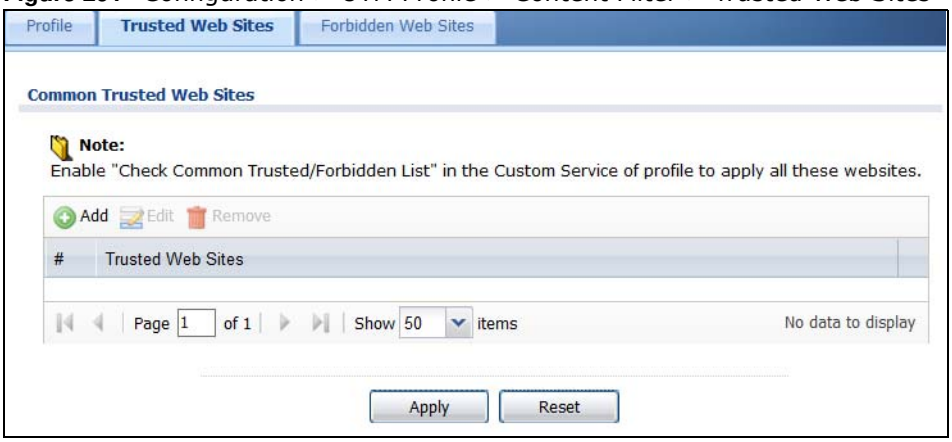
Table 166 Configuration > UTM Profile > Content Filter > Profile > Custom Service (continued)

LABEL	DESCRIPTION
Remove	Select an entry and click this to delete it.
#	This displays the index number of the forbidden web sites.
Forbidden Web Sites	This list displays the forbidden web sites already added. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "*bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", and do on. You can also enter just a top level domain. For example, enter "*.com" to block all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter. "*" can be used as a wildcard to match any string. The entry must contain at least one "." or it will be invalid.
Blocked URL Keywords	This section allows you to block Web sites with URLs that contain certain keywords in the domain name or IP address.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the blocked URL keywords.
Blocked URL Keywords	This list displays the keywords already added. Enter a keyword or a numerical IP address to block. You can also enter a numerical IP address. Use up to 127 case-insensitive characters (0-9a-zA-Z;/?:@&=+$\.-_!~*()%). "*" can be used as a wildcard to match any string. Use "|*" to indicate a single wildcard character. For example enter *Bad_Site* to block access to any web page that includes the exact phrase Bad_Site. This does not block access to web pages that only include part of the phrase (such as Bad for example).
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

27.4 Content Filter Trusted Web Sites Screen

Click Configuration > UTM Profile > Content Filter > Trusted Web Sites to open the Trusted Web Sites screen. You can create a common list of good (allowed) web site addresses. When you configure Filter Profiles, you can select the option to check the Common Trusted Web Sites list. Use this screen to add or remove specific sites from the filter list.

Figure 291 Configuration > UTM Profile > Content Filter > Trusted Web Sites



The following table describes the labels in this screen.

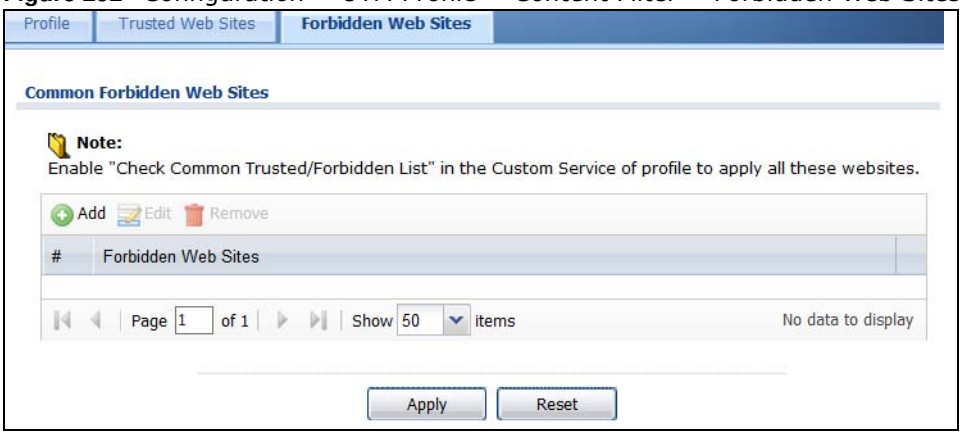
Table 167 Configuration > UTM Profile > Content Filter > Trusted Web Sites

LABEL	DESCRIPTION
Common Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the trusted web sites.
Trusted Web Site	This column displays the trusted web sites already added. 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", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

27.5 Content Filter Forbidden Web Sites Screen

Click Configuration > UTM Profile > Content Filter > Forbidden Web Sites to open the Forbidden Web Sites screen. You can create a common list of bad (blocked) web site addresses. When you configure Filter Profiles, you can select the option to check the Common Forbidden Web Sites list. Use this screen to add or remove specific sites from the filter list.

Figure 292 Configuration > UTM Profile > Content Filter > Forbidden Web Sites



The following table describes the labels in this screen.

Table 168 Configuration > UTM Profile > Content Filter > Forbidden Web Sites

LABEL	DESCRIPTION
Common Forbidden Web Sites	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the forbidden web sites.
Forbidden Web Sites	This list displays the forbidden web sites already added. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", and do on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter.
Apply	Click Apply to save your changes back to the USG.
Cancel	Click Reset to return the screen to its last-saved settings.

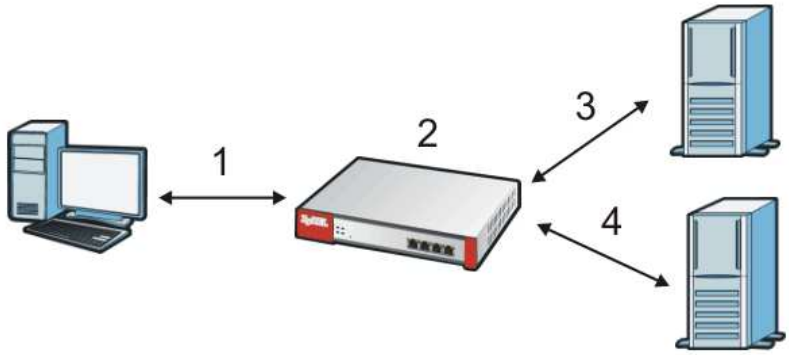
27.6 Content Filter Technical Reference

This section provides content filtering background information.

External Content Filter Server Lookup Procedure

The content filter lookup process is described below.

Figure 293 Content Filter Lookup Procedure



1 A computer behind the USG tries to access a web site.

2 The USG looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the USG's cache. The USG blocks, blocks and logs or just logs the request based on your configuration.

3 Use the Content Filter Cache screen to configure how long a web site address remains in the cache as well as view those web site addresses. All of the web site address records are also cleared from the local cache when the USG restarts.

4 If the USG has no record of the web site, it queries the external content filter database and simultaneously sends the request to the web server.

5 The external content filter server sends the category information back to the USG, which then blocks and/or logs access to the web site based on the settings in the content filter profile. The web site's address and category are then stored in the USG's content filter cache.

28

Anti-Spam

28.1 Overview

The anti-spam feature can mark or discard spam (unsolicited commercial or junk e-mail). Use the white list to identify legitimate e-mail. Use the black list to identify spam e-mail. The USG can also check e-mail against a DNS black list (DNSBL) of IP addresses of servers that are suspected of being used by spammers.

28.1.1 What You Can Do in this Chapter

- Use the Profile screens (Section 28.3 on page 437) to turn anti-spam on or off and manage anti-spam policies.
- Use the Mail Scan screen (Section 28.4 on page 440) to enable and configure the mail scan functions.
- Use the Black/ White List screens (Section 28.5 on page 442) to set up a black list to identify spam and a white list to identify legitimate e-mail.
- Use the DNSBL screens (Section 28.7 on page 447) to have the USG check e-mail against DNS Black Lists.

28.1.2 What You Need to Know

White List

Configure white list entries to identify legitimate e-mail. The white list entries have the USG classify any e-mail that is from a specified sender or uses a specified header field and header value as being legitimate (see E-mail Headers on page 436 for more on mail headers). The anti-spam feature checks an e-mail against the white list entries before doing any other anti-spam checking. If the e-mail matches a white list entry, the USG classifies the e-mail as legitimate and does not perform any more anti-spam checking on that individual e-mail. A properly configured white list helps keep important e-mail from being incorrectly classified as spam. The white list can also increases the USG's anti-spam speed and efficiency by not having the USG perform the full anti-spam checking process on legitimate e-mail.

Black List

Configure black list entries to identify spam. The black list entries have the USG classify any e-mail that is from or forwarded by a specified IP address or uses a specified header field and header value as being spam. If an e-mail does not match any of the white list entries, the USG checks it against the black list entries. The USG classifies an e-mail that matches a black list entry as spam and immediately takes the configured action for dealing with spam. If an e-mail matches a blacklist entry, the USG does not perform any more anti-spam checking on that individual e-mail. A properly

configured black list helps catch spam e-mail and increases the USG's anti-spam speed and efficiency.

SMTP and POP3

Simple Mail Transfer Protocol (SMTP) is the Internet's message transport standard. It controls the sending of e-mail messages between servers. E-mail clients (also called e-mail applications) then use mail server protocols such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve e-mail. E-mail clients also generally use SMTP to send messages to a mail server. The older POP2 requires SMTP for sending messages while the newer POP3 can be used with or without it. This is why many e-mail applications require you to specify both the SMTP server and the POP or IMAP server (even though they may actually be the same server).

The USG's anti-spam feature checks SMTP (TCP port 25) and POP3 (TCP port 110) e-mails by default. You can also specify custom SMTP and POP3 ports for the USG to check.

E-mail Headers

Every email has a header and a body. The header is structured into fields and includes the addresses of the recipient and sender, the subject, and other information about the e-mail and its journey. The body is the actual message text and any attachments. You can have the USG check for specific header fields with specific values.

E-mail programs usually only show you the To:, From:, Subject:, and Date: header fields but there are others such as Received: and Content-Type:. To see all of an e-mail's header, you can select an e-mail in your e-mail program and look at its properties or details. For example, in Microsoft's Outlook Express, select a mail and click File > Properties > Details. This displays the e-mail's header. Click Message Source to see the source for the entire mail including both the header and the body.

E-mail Header Buffer Size

The USG has a 5 K buffer for an individual e-mail header. If an e-mail's header is longer than 5 K, the USG only checks up to the first 5 K.

DNSBL

A DNS Black List (DNSBL) is a server that hosts a list of IP addresses known or suspected of having sent or forwarded spam. A DNSBL is also known as a DNS spam blocking list. The USG can check the routing addresses of e-mail against DNSBLs and classify an e-mail as spam if it was sent or forwarded by a computer with an IP address in the DNSBL.

Finding Out More

See Section 28.8 on page 449 for more background information on anti-spam.

28.2 Before You Begin

- Before using the Anti-Spam features (IP Reputation, Mail Content Analysis and Virus Outbreak Detection) you must activate your Anti-Spam Service license.

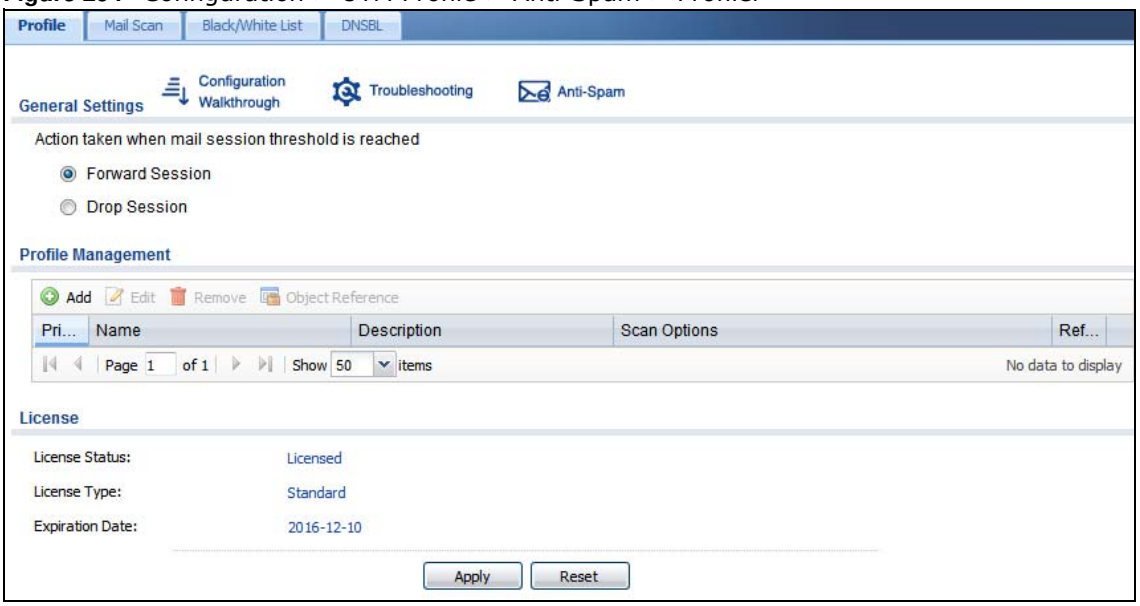
- Configure your zones before you configure anti-spam.

28.3 The Anti-Spam Profile Screen

Click Configuration > UTM Profile > Anti-Spam to open the Anti-Spam Profile screen. Use this screen to turn the anti-spam feature on or off and manage anti-spam policies. You can also select the action the USG takes when the mail sessions threshold is reached.

Click on the icons to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting and other information.

Figure 294 Configuration > UTM Profile > Anti-Spam > Profilel



The following table describes the labels in this screen.

Table 169 Configuration > UTM Profile > Anti-Spam > Profile

LABEL	DESCRIPTION
General Settings	
Action taken when mail sessions threshold is reached	An e-mail session is when an e-mail client and e-mail server (or two e-mail servers) connect through the USG. Select how to handle concurrent e-mail sessions that exceed the maximum number of concurrent e-mail sessions that the anti-spam feature can handle. See the chapter of product specifications for the threshold. Select Forward Session to have the USG allow the excess e-mail sessions without any spam filtering. Select Drop Session to have the USG drop mail connections to stop the excess e-mail sessions. The e-mail client or server will have to re-attempt to send or receive e-mail later when the number of e-mail sessions is under the threshold.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.

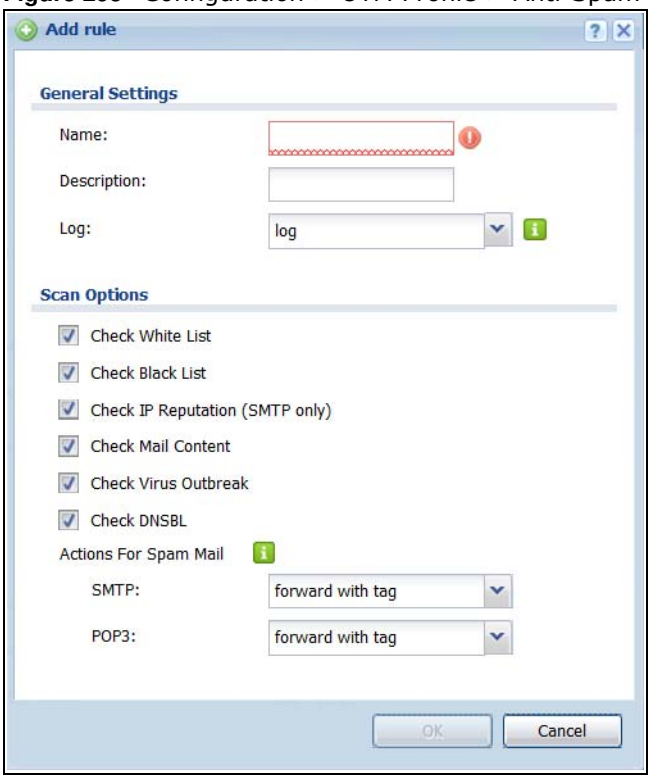
Table 169 Configuration > UTM Profile > Anti-Spam > Profile

LABEL	DESCRIPTION
Object Reference	Select an entry and click Object References to open a screen that shows which settings use the entry. Click Refresh to update information in this screen.
Priority	This is the index number of the anti-spam rule. Antis-spam rules are applied in turn.
Name	The name identifies the anti-spam rule.
Description	This is some optional extra information on the rule.
Scan Options	This shows which types (protocols) of traffic to scan for spam.
Reference	This shows how many objects are referenced in the rule.
License	
License Status	This read-only field displays the status of your anti-spam scanning service registration. Not Licensed displays if you have not successfully registered and activated the service. Expired displays if your subscription to the service has expired. Licensed displays if you have successfully registered the USG and activated the service.
License Type	This read-only field displays what kind of service registration you have for the anti-spam scanning. None displays if you have not successfully registered and activated the service. Standard displays if you have successfully registered the USG and activated the service with your iCard's PIN number. Trial displays if you have successfully registered the USG and activated the trial service subscription.
Expiration Date	This field displays the date your service license expires.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

28.3.1 The Anti-Spam Profile Add or Edit Screen

Click the Add or Edit icon in the Configuration > UTM Profile > Anti-Spam > Profile screen to display the configuration screen as shown next. Use this screen to configure an anti-spam policy that controls what traffic direction of e-mail to check, which e-mail protocols to scan, the scanning options, and the action to take on spam traffic.

Figure 295 Configuration > UTM Profile > Anti-Spam > Profile > Add



The following table describes the labels in this screen.

Table 170 Configuration > UTM Profile > Anti-Spam > Profile > Add

LABEL	DESCRIPTION
General Settings	
Name	Enter a descriptive name for this anti-spam rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the anti-spam rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Log	Select how the USG is to log the event when the DNSBL times out or an e-mail matches the white list, black list, or DNSBL. no: Do not create a log. log: Create a log on the USG. log alert: An alert is an e-mailed log for more serious events that may need more immediate attention. Select this option to have the USG send an alert.
Scan Options	
Check White List	Select this check box to check e-mail against the white list. The USG classifies e-mail that matches a white list entry as legitimate (not spam).
Check Black List	Select this check box to check e-mail against the black list. The USG classifies e-mail that matches a black list entry as spam.
Check IP Reputation (SMTP Only)	Select this to use IP reputation to identify Spam or Unwanted Bulk Email by the sender's IP address.

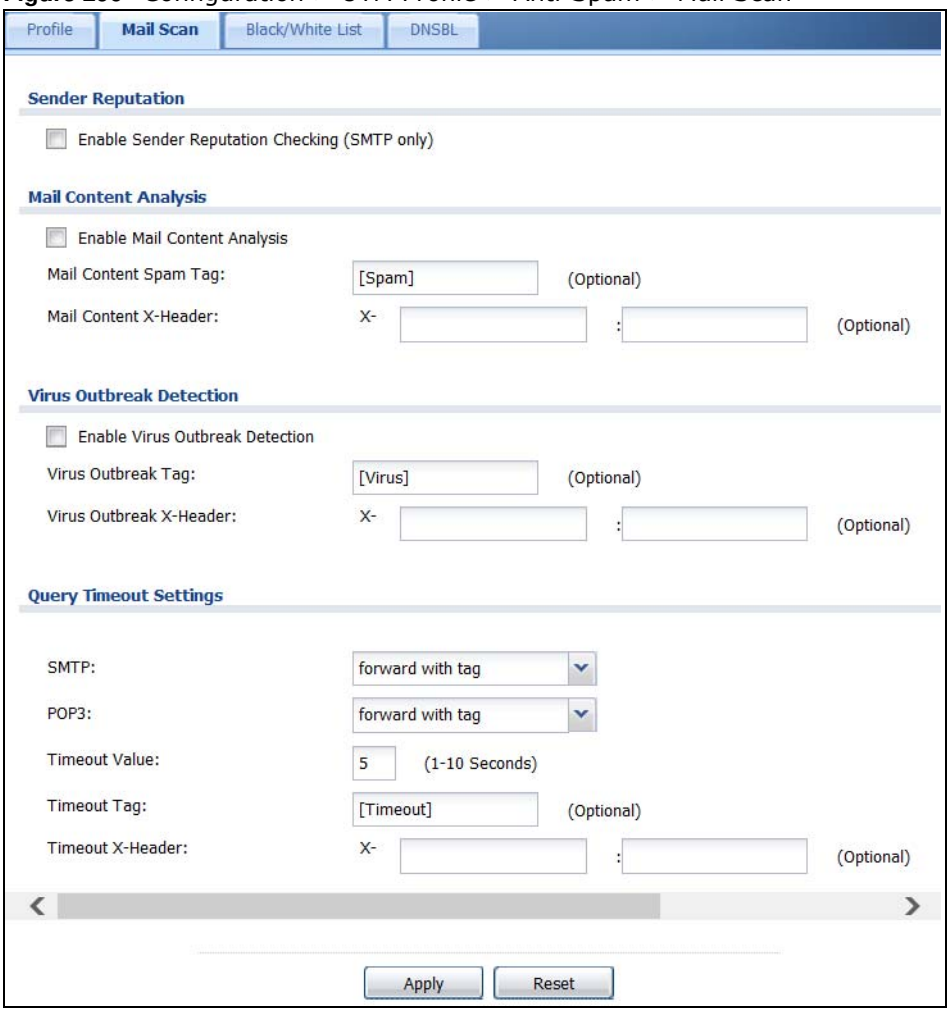
Table 170 Configuration > UTM Profile > Anti-Spam > Profile > Add (continued)

LABEL	DESCRIPTION
Check Mail Content	Select this to identify Spam Email by content, such as malicious content.
Check Virus Outbreak	Select this to scan emails for attached viruses.
Check DNSBL	Select this check box to check e-mail against the USG's configured DNSBL domains. The USG classifies e-mail that matches a DNS black list as spam.
Actions for Spam Mail	Use this section to set how the USG is to handle spam mail.
SMTP	Select how the USG is to handle spam SMTP mail. Select drop to discard spam SMTP mail. Select forward to allow spam SMTP mail to go through. Select forward with tag to add a spam tag to an SMTP spam mail's mail subject and send it on to the destination.
POP3	Select how the USG is to handle spam POP3 mail. Select forward to allow spam POP3 mail to go through. Select forward with tag to add a spam tag to an POP3 spam mail's mail subject and send it on to the destination.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving your changes.

28.4 The Mail Scan Screen

Click Configuration > UTM Profile > Anti-Spam > Mail Scan to open the Mail Scan screen. Use this screen to enable and configure the Mail Scan functions. You must first enable the Mail Scan functions on this screen before selecting them in the Configuration > UTM Profile > Anti-Spam > Profile > Add/ Edit screen.

Figure 296 Configuration > UTM Profile > Anti-Spam > Mail Scan



The following table describes the labels in this screen.

Table 171 Configuration > UTM Profile > Anti-Spam > Mail Scan

LABEL	DESCRIPTION
Sender Reputation	
Enable Sender Reputation Checking (SMTP only)	Select this to have the USG scan for spam e-mail by IP Reputation. Spam or Unwanted Bulk Email is determined by the sender's IP address.
Mail Content Analysis	
Enable Mail Content Analysis	Select this to identify Spam Email by content, such as malicious content.
Mail Content Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of e-mails that are determined to spam based on the mail content analysis. This tag is only added if the anti-spam policy is configured to forward spam mail with a spam tag.
Mail Content X-Header	Specify the name and value for the X-Header to be added when an email is determined to be spam by mail content.
Virus Outbreak Detection	

Table 171 Configuration > UTM Profile > Anti-Spam > Mail Scan

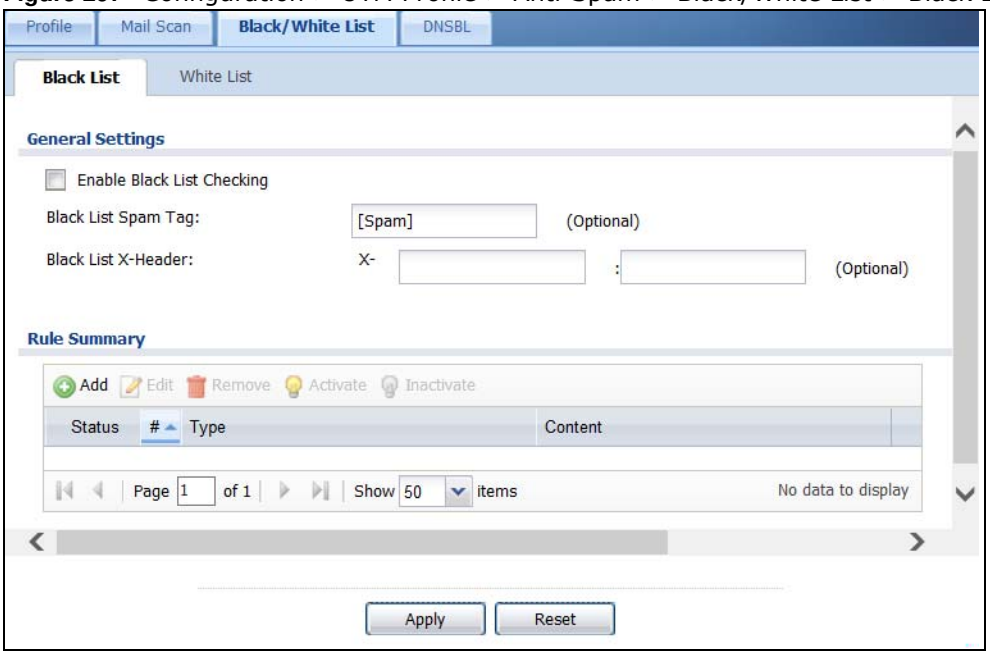
LABEL	DESCRIPTION
Enable Virus Outbreak Detection	This scans emails for attached viruses.
Virus Outbreak Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of e-mails that are determined have an attached viruses. This tag is only added if the anti-spam policy is configured to forward spam mail with a spam tag.
Virus Outbreak X-Header	Specify the name and value for the X-Header to be added when an email is determined to have an attached virus.
Query Timeout Settings	
SMTP	Select how the USG is to handle SMTP mail query timeout. Select drop to discard SMTP mail. Select forward to allow SMTP mail to go through. Select forward with tag to add a tag to an SMTP query timeout mail's mail subject and send it on to the destination.
POP3	Select how the USG is to handle POP3 mail query timeout. Select forward to allow POP3 mail to go through. Select forward with tag to add a tag to an POP3 query timeout mail's mail subject and send it on to the destination.
Timeout Value	Set how long the USG waits for a reply from the mail scan server. If there is no reply before this time period expires, the USG takes the action defined in the relevant Actions when Query Timeout field.
Timeout Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that the USG forwards if queries to the mail scan servers time out.
Timeout X-Header	Specify the name and value for the X-Header to be added when queries to the mail scan servers time out.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

28.5 The Anti-Spam Black List Screen

Click Configuration > UTM Profile > Anti-Spam > Black /White List to display the Anti-Spam Black List screen.

Configure the black list to identify spam e-mail. You can create black list entries based on the sender's or relay server's IP address or e-mail address. You can also create entries that check for particular e-mail header fields with specific values or specific subject text. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 297 Configuration > UTM Profile > Anti-Spam > Black/White List > Black List



The following table describes the labels in this screen.

Table 172 Configuration > UTM Profile > Anti-Spam > Black/White List > Black List

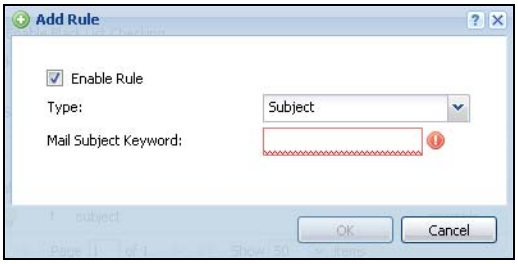
LABEL	DESCRIPTION
General Settings	
Enable Black List Checking	Select this check box to have the USG treat e-mail that matches (an active) black list entry as spam.
Black List Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that match the USG's spam black list.
Black List X-Header	Specify the name and value for the X-Header to be added to e-mails that match the USG's spam black list.
Rule Summary	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
Type	This field displays whether the entry is based on the e-mail's subject, source or relay IP address, source e-mail address, or header.
Content	This field displays the subject content, source or relay IP address, source e-mail address, or header value for which the entry checks.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

28.5.1 The Anti-Spam Black or White List Add/Edit Screen

In the anti-spam Black List or White List screen, click the Add icon or an Edit icon to display the following screen.

Use this screen to configure an anti-spam black list entry to identify spam e-mail. You can create entries based on specific subject text, or the sender's or relay's IP address or e-mail address. You can also create entries that check for particular header fields and values.

Figure 298 Configuration > UTM Profile > Anti-Spam > Black/White List > Black List (or White List) > Add



The following table describes the labels in this screen.

Table 173 Configuration > UTM Profile > Anti-Spam > Black/White List > Black/White List > Add

LABEL	DESCRIPTION
Enable Rule	Select this to have the USG use this entry as part of the black or white list. To actually use the entry, you must also turn on the use of the list in the corresponding list screen, enable the anti-spam feature in the anti-spam general screen, and configure an anti-spam policy to use the list.
Type	Use this field to base the entry on the e-mail's subject, source or relay IP address, source e-mail address, or header. Select Subject to have the USG check e-mail for specific content in the subject line. Select IP Address to have the USG check e-mail for a specific source or relay IP address. Select IPv6 Address to have the USG check e-mail for a specific source or relay IPv6 address. Select E-Mail Address to have the USG check e-mail for a specific source e-mail address or domain name. Select Mail Header to have the USG check e-mail for specific header fields and values. Configure black list header entries to check for e-mail from bulk mail programs or with content commonly used in spam. Configure white list header entries to allow certain header values that identify the e-mail as being from a trusted source.
Mail Subject Keyword	This field displays when you select the Subject type. Enter up to 63 ASCII characters of text to check for in e-mail headers. Spaces are not allowed, although you could substitute a question mark (?). See Section 28.5.2 on page 445 for more details.
Sender or Mail Relay IP Address	This field displays when you select the IP Address type. Enter an IP address in dotted decimal notation.
Sender or Mail Relay IPv6 Address	This field displays when you select the IPv6 Address type. Enter an IPv6 address with prefix.
Netmask	This field displays when you select the IP type. Enter the subnet mask here, if applicable.
Sender E-Mail Address	This field displays when you select the E-Mail type. Enter a keyword (up to 63 ASCII characters). See Section 28.5.2 on page 445 for more details.

Table 173 Configuration > UTM Profile > Anti-Spam > Black/White List > Black/White List > Add

LABEL	DESCRIPTION
Mail Header Field Name	This field displays when you select the Mail Header type. Type the name part of an e-mail header (the part that comes before the colon). Use up to 63 ASCII characters. For example, if you want the entry to check the "Received:" header for a specific mail server's domain, enter "Received" here.
Field Value Keyword	This field displays when you select the Mail Header type. Type the value part of an e-mail header (the part that comes after the colon). Use up to 63 ASCII characters. For example, if you want the entry to check the "Received:" header for a specific mail server's domain, enter the mail server's domain here. See Section 28.5.2 on page 445 for more details.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving your changes.

28.5.2 Regular Expressions in Black or White List Entries

The following applies for a black or white list entry based on an e-mail subject, e-mail address, or e-mail header value.

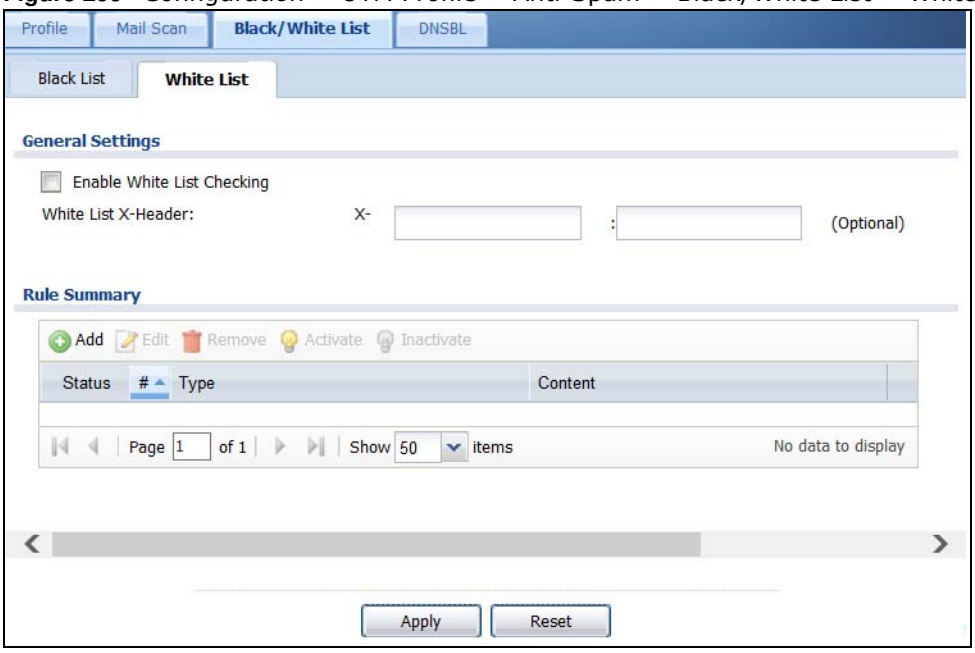
- Use a question mark (?) to let a single character vary. For example, use "a?c" (without the quotation marks) to specify abc, acc and so on.
- You can also use a wildcard (*). For example, if you configure *def.com, any e-mail address that ends in def.com matches. So "mail.def.com" matches.
- The wildcard can be anywhere in the text string and you can use more than one wildcard. You cannot use two wildcards side by side, there must be other characters between them.
- The USG checks the first header with the name you specified in the entry. So if the e-mail has more than one "Received" header, the USG checks the first one.

28.6 The Anti-Spam White List Screen

Click Configuration > UTM Profile > Anti-Spam > Black/White List and then the White List tab to display the Anti-Spam White List screen.

Configure the white list to identify legitimate e-mail. You can create white list entries based on the sender's or relay's IP address or e-mail address. You can also create entries that check for particular header fields and values or specific subject text.

Figure 299 Configuration > UTM Profile > Anti-Spam > Black/White List > White List



The following table describes the labels in this screen.

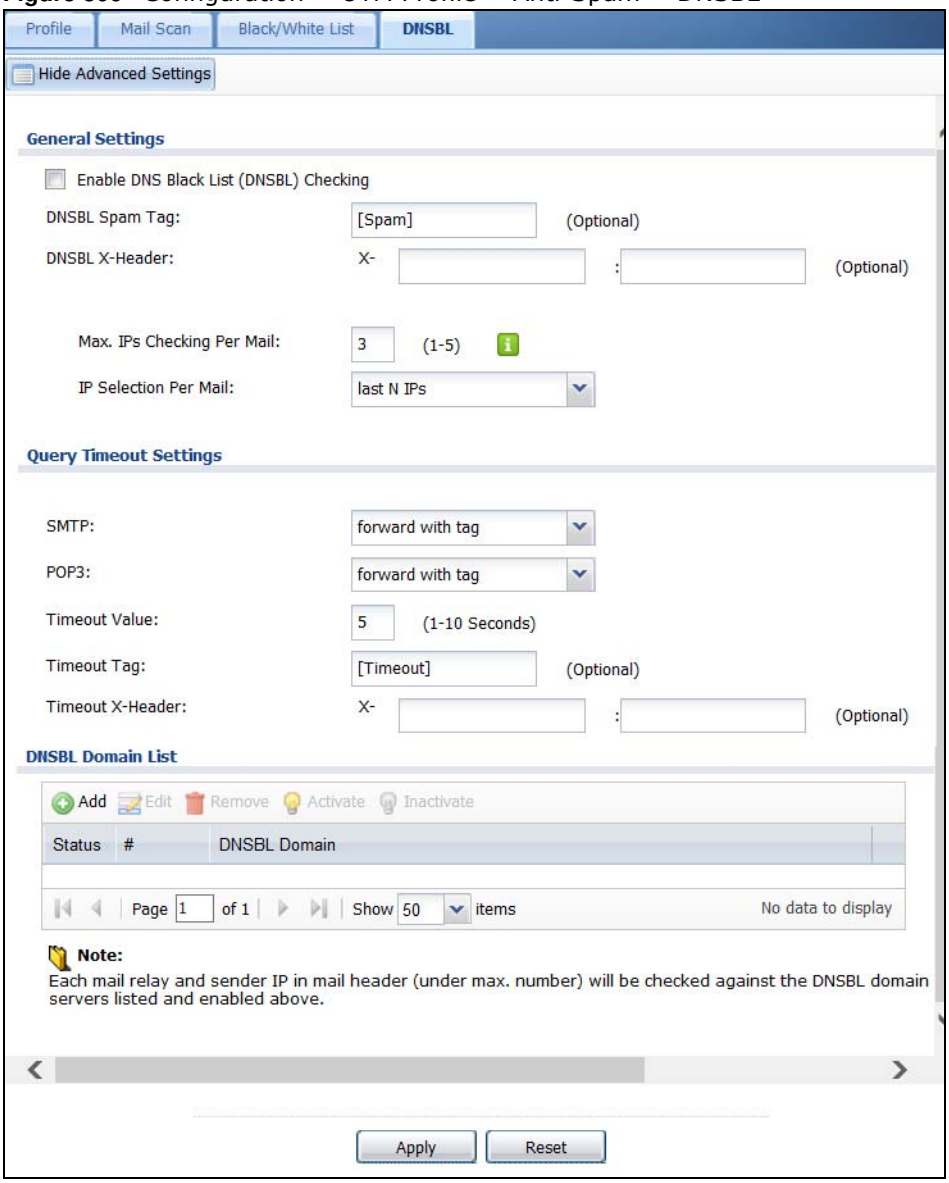
Table 174 Configuration > UTM Profile > Anti-Spam > Black/White List > White List

LABEL	DESCRIPTION
General Settings	
Enable White List Checking	Select this check box to have the USG forward e-mail that matches (an active) white list entry without doing any more anti-spam checking on that individual e-mail.
White List X-Header	Specify the name and value for the X-Header to be added to e-mails that match the USG's spam white list.
Rule Summary	
Add	Click this to create a new entry. See Section 28.5.1 on page 444 for details.
Edit	Select an entry and click this to be able to modify it. See Section 28.5.1 on page 444 for details.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
Type	This field displays whether the entry is based on the e-mail's subject, source or relay IP address, source e-mail address, or a header.
Content	This field displays the subject content, source or relay IP address, source e-mail address, or header value for which the entry checks.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

28.7 The DNSBL Screen

Click Configuration > UTM Profile > Anti-Spam > DNSBL to display the anti-spam DNSBL screen. Use this screen to configure the USG to check the sender and relay IP addresses in e-mail headers against DNS (Domain Name Service)-based spam Black Lists (DNSBLs).

Figure 300 Configuration > UTM Profile > Anti-Spam > DNSBL



The following table describes the labels in this screen.

Table 175 Configuration > UTM Profile > Anti-Spam > DNSBL

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable DNS Black List (DNSBL) Checking	Select this to have the USG check the sender and relay IP addresses in e-mail headers against the DNSBL servers maintained by the DNSBL domains listed in the USG.
DNSBL Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of e-mails that have a sender or relay IP address in the header that matches a black list maintained by one of the DNSBL domains listed in the USG. This tag is only added if the anti-spam policy is configured to forward spam mail with a spam tag.
DSBNL X-Header	Specify the name and value for the X-Header to be added to e-mails that have a sender or relay IP address in the header that matches a black list maintained by one of the DNSBL domains listed in the USG.
Max. IPs Checking Per Mail	Set the maximum number of sender and relay server IP addresses in the mail header to check against the DNSBL domain servers.
IP Selection Per Mail	Select first N IPs to have the USG start checking from the first IP address in the mail header. This is the IP of the sender or the first server that forwarded the mail. Select last N IPs to have the USG start checking from the last IP address in the mail header. This is the IP of the last server that forwarded the mail.
Query Timeout Setting	
SMTP	Select how the USG is to handle SMTP mail (mail going to an e-mail server) if the queries to the DNSBL domains time out. Select drop to discard SMTP mail. Select forward to allow SMTP mail to go through. Select forward with tag to add a DNSBL timeout tag to the mail subject of an SMTP mail and send it.
POP3	Select how the USG is to handle POP3 mail (mail coming to an e-mail client) if the queries to the DNSBL domains time out. Select forward to allow POP3 mail to go through. Select forward with tag to add a DNSBL timeout tag to the mail subject of an POP3 mail and send it.
Timeout Value	Set how long the USG waits for a reply from the DNSBL domains listed below. If there is no reply before this time period expires, the USG takes the action defined in the relevant Actions when Query Timeout field.
Timeout Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that the USG forwards if queries to the DNSBL domains time out.
Timeout X-Header	Specify the name and value for the X-Header to be added to e-mails that the USG forwards if queries to the DNSBL domains time out.
DNSBL Domain List	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.

Table 175 Configuration > UTM Profile > Anti-Spam > DNSBL (continued)

LABEL	DESCRIPTION
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
DNSBL Domain	This is the name of a domain that maintains DNSBL servers. Enter the domain that is maintaining a DNSBL.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

28.8 Anti-Spam Technical Reference

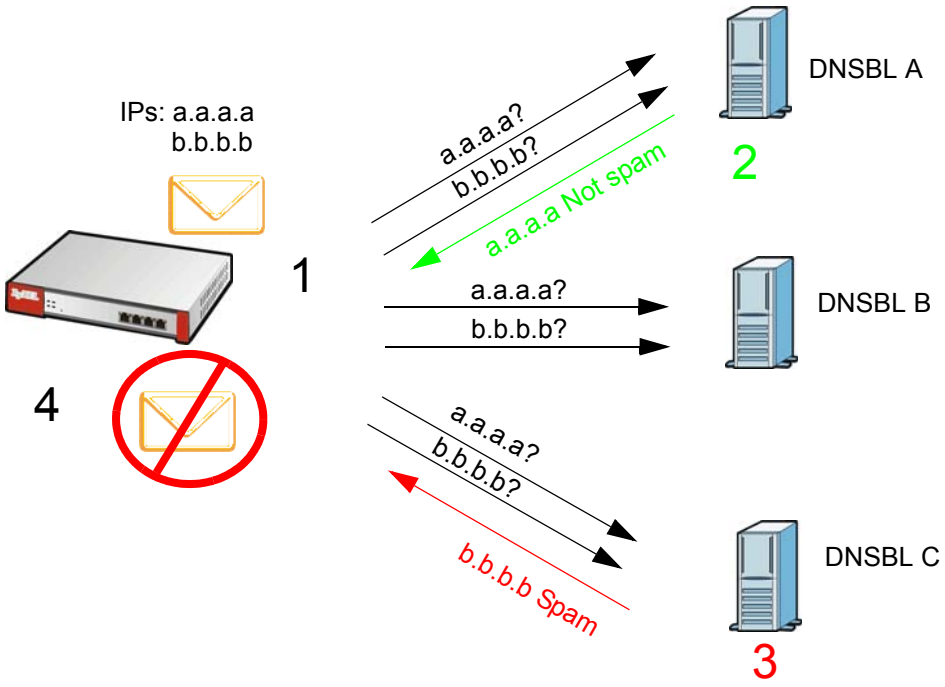
Here is more detailed anti-spam information.

DNSBL

- The USG checks only public sender and relay IP addresses, it does not check private IP addresses.
- The USG sends a separate query (DNS lookup) for each sender or relay IP address in the e-mail's header to each of the USG's DNSBL domains at the same time.
- The DNSBL servers send replies as to whether or not each IP address matches an entry in their list. Each IP address has a separate reply.
- As long as the replies are indicating the IP addresses do not match entries on the DNSBL lists, the USG waits until it receives at least one reply for each IP address.
- If the USG receives a DNSBL reply that one of the IP addresses is in the DNSBL list, the USG immediately classifies the e-mail as spam and takes the anti-spam policy's configured action for spam. The USG does not wait for any more DNSBL replies.
- If the USG receives at least one non-spam reply for each of an e-mail's routing IP addresses, the USG immediately classifies the e-mail as legitimate and forwards it.
- Any further DNSBL replies that come after the USG classifies an e-mail as spam or legitimate have no effect.
- The USG records DNSBL responses for IP addresses in a cache for up to 72 hours. The USG checks an e-mail's sender and relay IP addresses against the cache first and only sends DNSBL queries for IP addresses that are not in the cache.

Here is an example of an e-mail classified as spam based on DNSBL replies.

Figure 301 DNSBL Spam Detection Example



1 The USG receives an e-mail that was sent from IP address a.a.a.a and relayed by an e-mail server at IP address b.b.b.b. The USG sends a separate query to each of its DNSBL domains for IP address a.a.a.a. The USG sends another separate query to each of its DNSBL domains for IP address b.b.b.b.

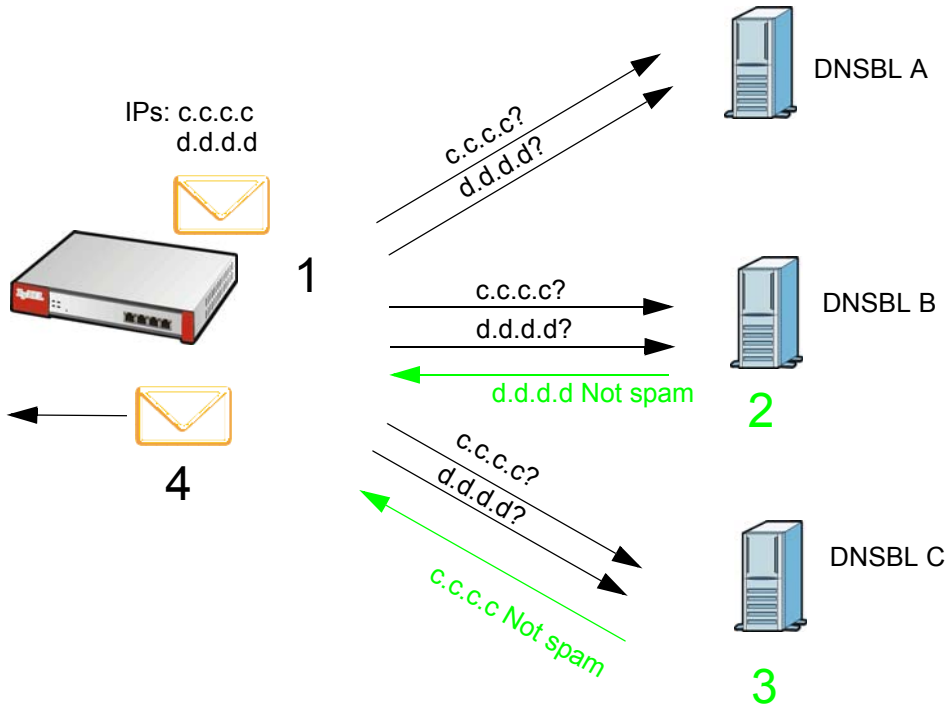
2 DNSBL A replies that IP address a.a.a.a does not match any entries in its list (not spam).

3 DNSBL C replies that IP address b.b.b.b matches an entry in its list.

4 The USG immediately classifies the e-mail as spam and takes the action for spam that you defined in the anti-spam policy. In this example it was an SMTP mail and the defined action was to drop the mail. The USG does not wait for any more DNSBL replies.

Here is an example of an e-mail classified as legitimate based on DNSBL replies.

Figure 302 DNSBL Legitimate E-mail Detection Example



1 The USG receives an e-mail that was sent from IP address c.c.c.c and relayed by an e-mail server at IP address d.d.d.d. The USG sends a separate query to each of its DNSBL domains for IP address c.c.c.c. The USG sends another separate query to each of its DNSBL domains for IP address d.d.d.d.

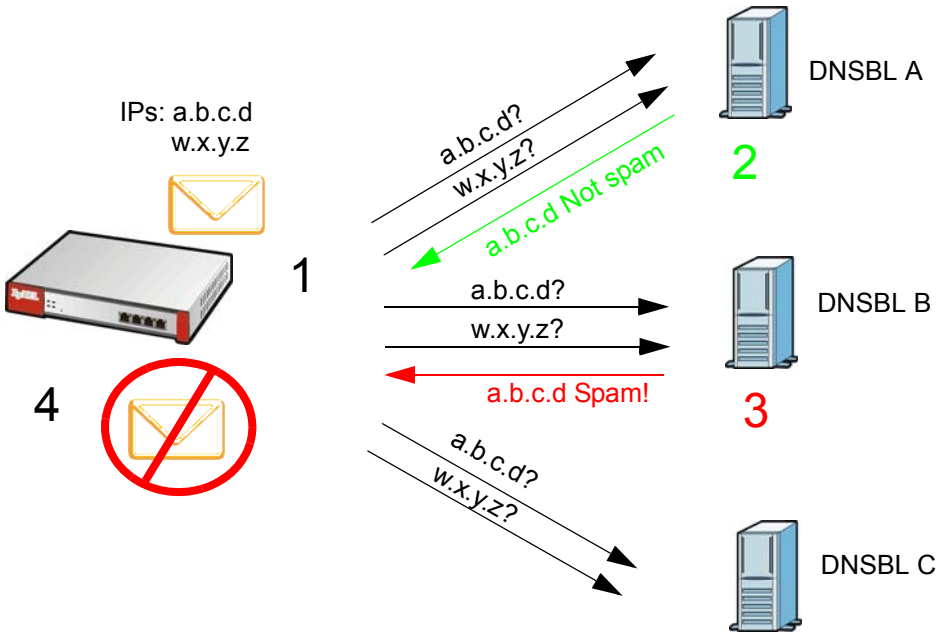
2 DNSBL B replies that IP address d.d.d.d does not match any entries in its list (not spam).

3 DNSBL C replies that IP address c.c.c.c does not match any entries in its list (not spam).

4 Now that the USG has received at least one non-spam reply for each of the e-mail's routing IP addresses, the USG immediately classifies the e-mail as legitimate and forwards it. The USG does not wait for any more DNSBL replies.

If the USG receives conflicting DNSBL replies for an e-mail routing IP address, the USG classifies the e-mail as spam. Here is an example.

Figure 303 Conflicting DNSBL Replies Example



1 The USG receives an e-mail that was sent from IP address a.b.c.d and relayed by an e-mail server at IP address w.x.y.z. The USG sends a separate query to each of its DNSBL domains for IP address a.b.c.d. The USG sends another separate query to each of its DNSBL domains for IP address w.x.y.z.

2 DNSBL A replies that IP address a.b.c.d does not match any entries in its list (not spam).

3 While waiting for a DNSBL reply about IP address w.x.y.z, the USG receives a reply from DNSBL B saying IP address a.b.c.d is in its list.

4 The USG immediately classifies the e-mail as spam and takes the action for spam that you defined in the anti-spam policy. In this example it was an SMTP mail and the defined action was to drop the mail. The USG does not wait for any more DNSBL replies.

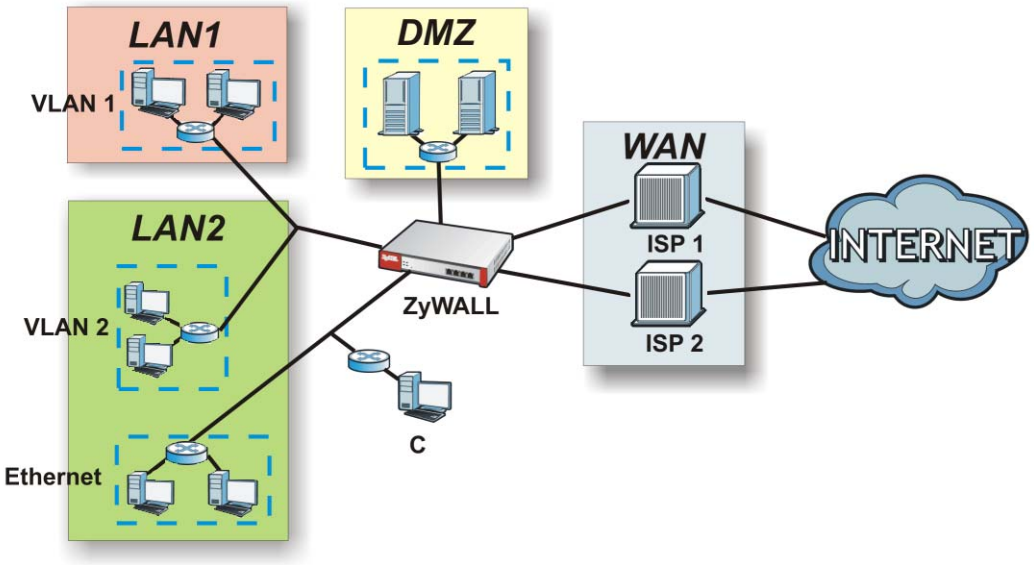
29 Object

29.1 Zones Overview

Set up zones to configure network security and network policies in the USG. A zone is a group of interfaces and/or VPN tunnels. The USG uses zones instead of interfaces in many security and policy settings, such as Secure Policies rules, UTM Profile, and remote management.

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

Figure 304 Example: Zones



Use the Zone screens (see Section 29.7.2 on page 498) to manage the USG's zones.

29.1.1 What You Need to Know

Zones effectively divide traffic into three types--intra-zone traffic, inter-zone traffic, and extra-zone traffic.

Intra-zone Traffic

- Intra-zone traffic is traffic between interfaces or VPN tunnels in the same zone. For example, in Figure 304 on page 453, traffic between VLAN 2 and the Ethernet is intra-zone traffic.

Inter-zone Traffic

Inter-zone traffic is traffic between interfaces or VPN tunnels in different zones. For example, in Figure 304 on page 453, traffic between VLAN 1 and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

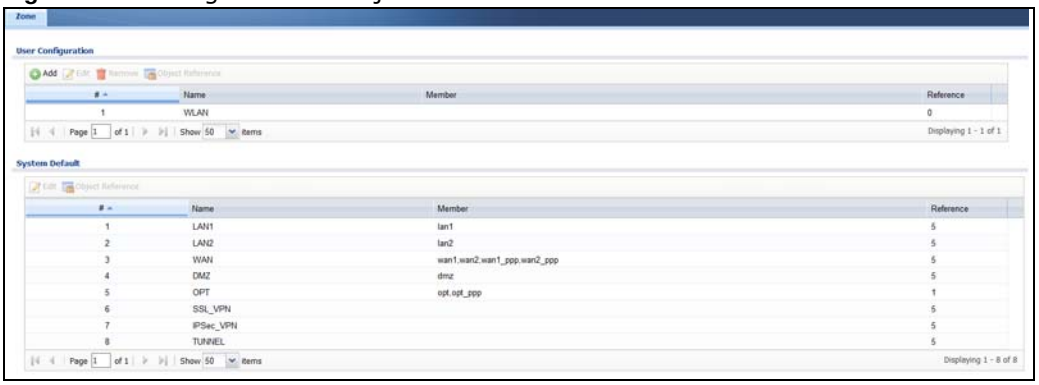
Extra-zone Traffic

- Extra-zone traffic is traffic to or from any interface or VPN tunnel that is not assigned to a zone. For example, in Figure 304 on page 453, traffic to or from computer C is extra-zone traffic.
- Some zone-based security and policy settings may apply to extra-zone traffic, especially if you can set the zone attribute in them to Any or All. See the specific feature for more information.

29.1.2 The Zone Screen

The Zone screen provides a summary of all zones. In addition, this screen allows you to add, edit, and remove zones. To access this screen, click Configuration > Object > Zone.

Figure 305 Configuration > Object > Zone



The following table describes the labels in this screen.

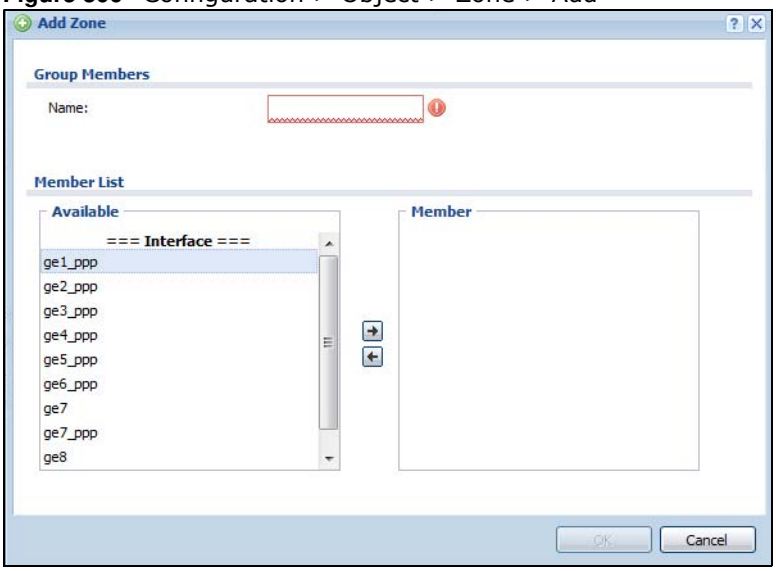
Table 176 Configuration > Object > Zone

LABEL	DESCRIPTION
User Configuration / System Default	The USG comes with pre-configured System Default zones that you cannot delete. You can create your own User Configuration zones
Add	Click this to create a new, user-configured zone.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry. Click Refresh to update information in this screen.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the zone.
Member	This field displays the names of the interfaces that belong to each zone.
Reference	This field displays the number of times an Object Reference is used in a policy.

29.1.2.1 Zone Edit

The Zone Edit screen allows you to add or edit a zone. To access this screen, go to the Zone screen (see Section 29.7.2 on page 498), and click the Add icon or an Edit icon.

Figure 306 Configuration > Object > Zone > Add



The following table describes the labels in this screen.

Table 177 Configuration > Object > Zone > Add/Edit

LABEL	DESCRIPTION
Name	For a system default zone, the name is read only. For a user-configured zone, type the name used to refer to the zone. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Member List	Available lists the interfaces and VPN tunnels that do not belong to any zone. Select the interfaces and VPN tunnels that you want to add to the zone you are editing, and click the right arrow button to add them. Member lists the interfaces and VPN tunnels that belong to the zone. Select any interfaces that you want to remove from the zone, and click the left arrow button to remove them.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

29.2 User/Group Overview

This section describes how to set up user accounts, user groups, and user settings for the USG. You can also set up rules that control when users have to log in to the USG before the USG routes traffic for them.

- The User screen (see Section 29.2.2 on page 458) provides a summary of all user accounts.

- The Group screen (see Section 29.2.3 on page 461) provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. User groups may consist of access users and other user groups. You cannot put admin users in user groups
- The Setting screen (see Section 29.2.4 on page 462) controls default settings, login settings, lockout settings, and other user settings for the USG. You can also use this screen to specify when users must log in to the USG before it routes traffic for them.
- The MAC Address screen (see Section 29.2.5 on page 467) allows you to configure the MAC addresses or OUI (Organizationally Unique Identifier) of wireless clients for MAC authentication using the local user database. The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.

29.2.1 What You Need To Know

User Account

A user account defines the privileges of a user logged into the USG. User accounts are used in security policies, in addition to controlling access to configuration and services in the USG.

User Types

These are the types of user accounts the USG uses.

Table 178 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change USG configuration (web, CLI)	WWW, TELNET, SSH, FTP, Console
limited-admin	Look at USG configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH, Console
Access Users		
user	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
guest	Access network services	WWW
ext-user	External user account	WWW
ext-group-user	External group user account	WWW

Note: The default admin account is always authenticated locally, regardless of the authentication method setting. (See Chapter 29 on page 511 for more information about authentication methods.)

Ext-User Accounts

Set up an ext-user account if the user is authenticated by an external server and you want to set up specific policies for this user in the USG. If you do not want to set up policies for this user, you do not have to set up an ext-user account.

All ext-user users should be authenticated by an external server, such as AD, LDAP or RADIUS. If the USG tries to use the local database to authenticate an ext-user, the authentication attempt always fails. (This is related to AAA servers and authentication methods, which are discussed in those chapters in this guide.)

Note: If the USG tries to authenticate an ext-user using the local database, the attempt always fails.

Once an ext-user user has been authenticated, the USG tries to get the user type (see Table 178 on page 456) from the external server. If the external server does not have the information, the USG sets the user type for this session to User.

For the rest of the user attributes, such as reauthentication time, the USG checks the following places, in order.

1 User account in the remote server.

2 User account (Ext-User) in the USG.

3 Default user account for AD users (ad-users), LDAP users (ldap-users) or RADIUS users (radius-users) in the USG.

See Setting up User Attributes in an External Server on page 469 for a list of attributes and how to set up the attributes in an external server.

Ext-Group-User Accounts

Ext-Group-User accounts work are similar to ext-user accounts but allow you to group users by the value of the group membership attribute configured for the AD or LDAP server. See Section 29.8.5.1 on page 506 for more on the group membership attribute.

User Groups

User groups may consist of user accounts or other user groups. Use user groups when you want to create the same rule for several user accounts, instead of creating separate rules for each one.

Note: You cannot put access users and admin users in the same user group.

Note: You cannot put the default admin account into any user group.

The sequence of members in a user group is not important.

User Awareness

By default, users do not have to log into the USG to use the network services it provides. The USG automatically routes packets for everyone. If you want to restrict network services that certain users can use via the USG, you can require them to log in to the USG first. The USG is then 'aware' of the user who is logged in and you can create 'user-aware policies' that define what services they can use. See Section 29.2.6 on page 468 for a user-aware login example.

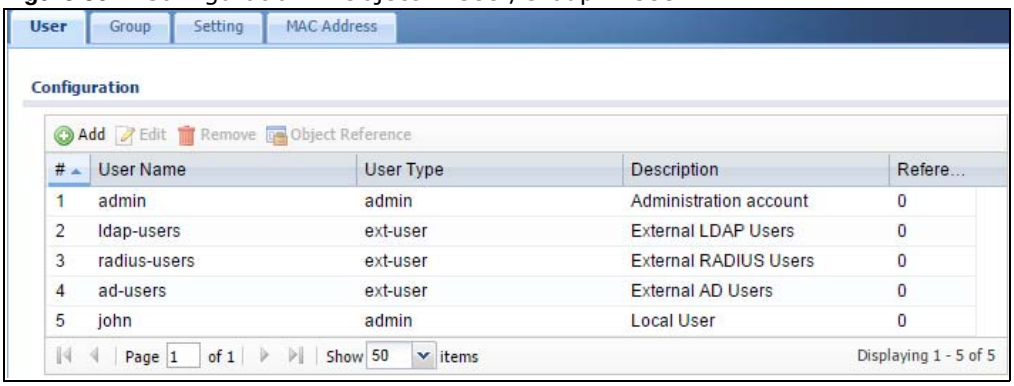
Finding Out More

- See Section 29.2.6 on page 468 for some information on users who use an external authentication server in order to log in.
- The USG supports TTLS using PAP so you can use the USG's local user database to authenticate users with WPA or WPA2 instead of needing an external RADIUS server.

29.2.2 User/Group User Summary Screen

The User screen provides a summary of all user accounts. To access this screen, login to the Web Configurator, and click Configuration > Object > User/ Group.

Figure 307 Configuration > Object > User/Group > User



The following table describes the labels in this screen.

Table 179 Configuration > Object > User/Group > User

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific user.
User Name	This field displays the user name of each user.
User Type	This field displays the types of user accounts the USG uses: • admin - this user can look at and change the configuration of the USG • limited-admin - this user can look at the configuration of the USG but not to change it • user - this user has access to the USG's services and can also browse user-mode commands (CLI). • guest - this user has access to the USG's services but cannot look at the configuration • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 456 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 457 for more information about this type.
Description	This field displays the description for each user.
Reference	This displays the number of times an object reference is used in a profile.

29.2.2.1 User Add/Edit Screen

The User Add/ Edit screen allows you to create a new user account or edit an existing one.

29.2.2.2 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]
- - [dashes]

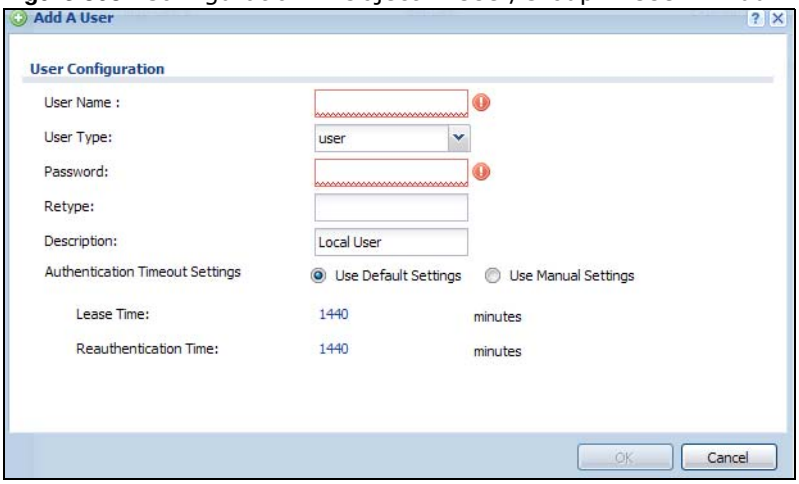
The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not 'bob'.
- User names have to be different than user group names.
- Here are the reserved user names:

• adm	• admin	• any	• bin	• daemon
• debug	• devicehaecived	• ftp	• games	• halt
• ldap-users	• lp	• mail	• news	• nobody
• operator	• radius-users	• root	• shutdown	• sshd
• sync	• uucp	• zyxel		

To access this screen, go to the User screen (see Section 29.2.2 on page 458), and click either the Add icon or an Edit icon.

Figure 308 Configuration > Object > User/Group > User > Add



The following table describes the labels in this screen.

Table 180 Configuration > Object > User/Group > User > Add

LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved. See Section 29.2.2.2 on page 458.
User Type	This field displays the types of user accounts the USG uses: • admin - this user can look at and change the configuration of the USG • limited-admin - this user can look at the configuration of the USG but not to change it • user - this user has access to the USG's services and can also browse user-mode commands (CLI). • guest - this user has access to the USG's services but cannot look at the configuration. • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 456 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 457 for more information about this type.
Password	This field is not available if you select the ext-user or ext-group-user type. Enter the password of this user account. It can consist of 4 - 31 alphanumeric characters.
Retype	This field is not available if you select the ext-user or ext-group-user type.
Group Identifier	This field is available for a ext-group-user type user account. Specify the value of the AD or LDAP server's Group Membership Attribute that identifies the group to which this user belongs.
Associated AAA Server Object	This field is available for a ext-group-user type user account. Select the AAA server to use to authenticate this account's users.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.
Authentication Timeout Settings	If you want the system to use default settings, select Use Default Settings. If you want to set authentication timeout to a value other than the default settings, select Use Manual Settings then fill your preferred values in the fields that follow.
Lease Time	If you select Use Default Settings in the Authentication Timeout Settings field, the default lease time is shown. If you select Use Manual Settings, you need to enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 29.2.4 on page 462), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	If you select Use Default Settings in the Authentication Timeout Settings field, the default lease time is shown. If you select Use Manual Settings, you need to type the number of minutes this user can be logged into the USG in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike Lease Time, the user has no opportunity to renew the session without logging out.
Configuration Validation	Use a user account from the group specified above to test if the configuration is correct. Enter the account's user name in the User Name field and click Test.

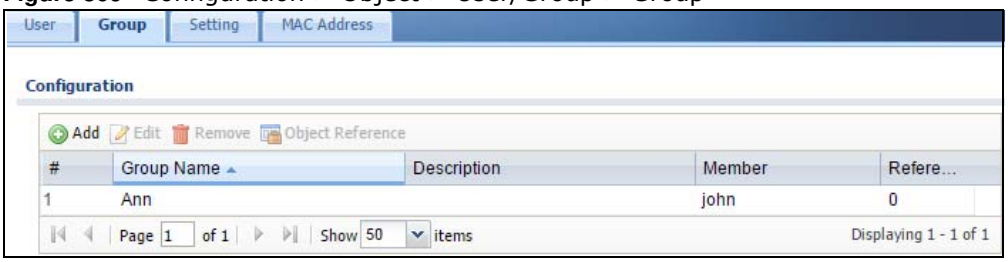
Table 180 Configuration > Object > User/Group > User > Add (continued)

LABEL	DESCRIPTION
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.2.3 User/Group Group Summary Screen

User groups consist of access users and other user groups. You cannot put admin users in user groups. The Group screen provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. To access this screen, login to the Web Configurator, and click Configuration > Object > User/ Group > Group.

Figure 309 Configuration > Object > User/Group > Group



The following table describes the labels in this screen. See Section 29.2.3.1 on page 461 for more information as well.

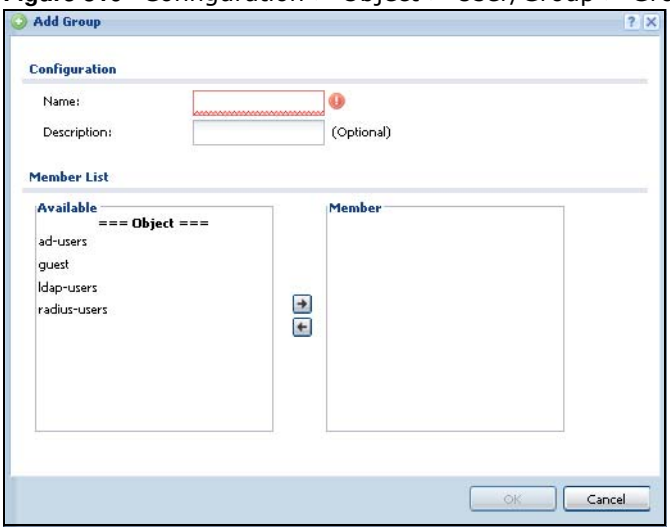
Table 181 Configuration > Object > User/Group > Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Removing a group does not remove the user accounts in the group.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific user group.
Group Name	This field displays the name of each user group.
Description	This field displays the description for each user group.
Member	This field lists the members in the user group. Each member is separated by a comma.
Reference	This displays the number of times an object reference is used in a profile.

29.2.3.1 Group Add/Edit Screen

The Group Add/ Edit screen allows you to create a new user group or edit an existing one. To access this screen, go to the Group screen (see Section 29.2.3 on page 461), and click either the Add icon or an Edit icon.

Figure 310 Configuration > Object > User/Group > Group > Add



The following table describes the labels in this screen.

Table 182 Configuration > Object > User/Group > Group > Add

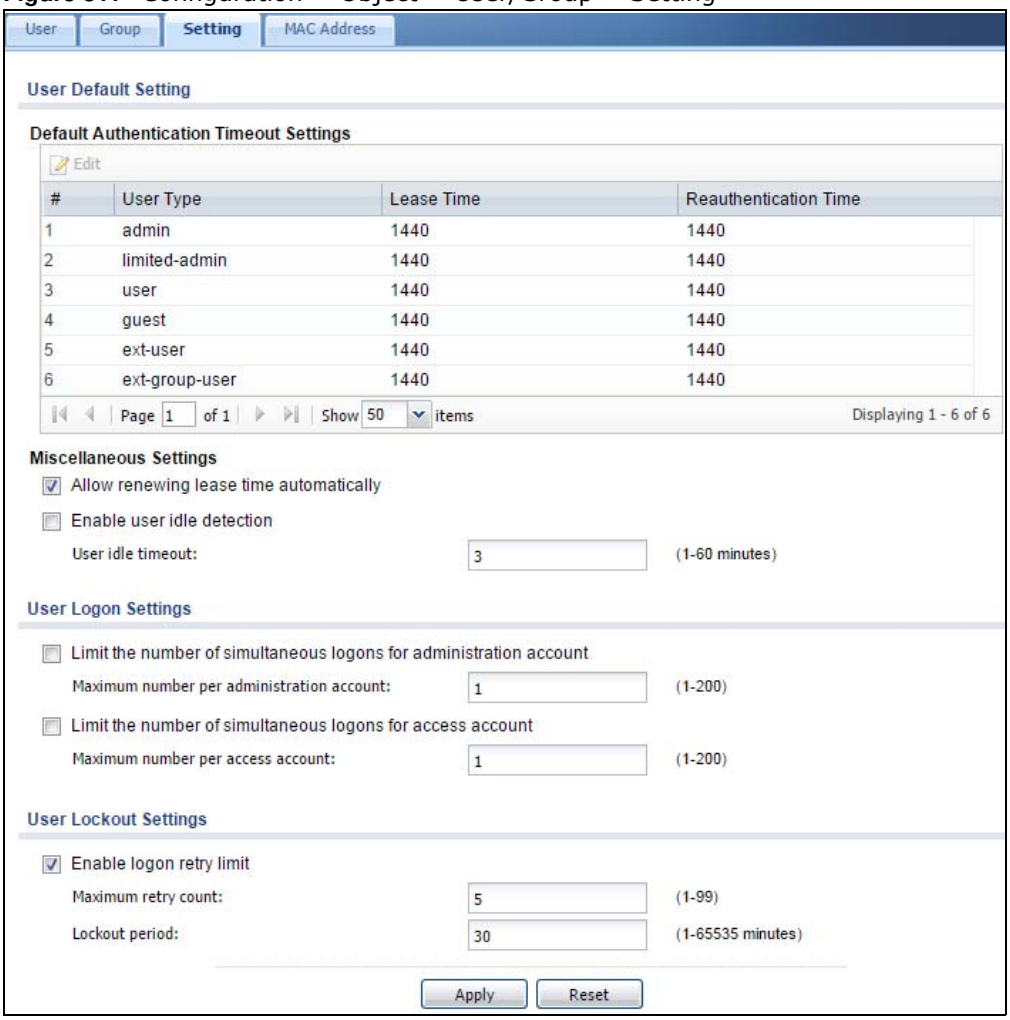
LABEL	DESCRIPTION
Name	Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names.
Description	Enter the description of the user group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	The Member list displays the names of the users and user groups that have been added to the user group. The order of members is not important. Select users and groups from the Available list that you want to be members of this group and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.2.4 User/Group Setting Screen

The Setting screen controls default settings, login settings, lockout settings, and other user settings for the USG. You can also use this screen to specify when users must log in to the USG before it routes traffic for them.

To access this screen, login to the Web Configurator, and click Configuration > Object > User/Group > Setting.

Figure 311 Configuration > Object > User/Group > Setting



The following table describes the labels in this screen.

Table 183 Configuration > Object > User/Group > Setting

LABEL	DESCRIPTION
User Authentication Timeout Settings	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
#	This field is a sequential value, and it is not associated with a specific entry.

Table 183 Configuration > Object > User/Group > Setting (continued)

LABEL	DESCRIPTION
User Type	These are the kinds of user account the USG supports. • admin - this user can look at and change the configuration of the USG • limited-admin - this user can look at the configuration of the USG but not to change it • user - this user has access to the USG's services but cannot look at the configuration • guest - this user has access to the USG's services but cannot look at the configuration • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 456 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 457 for more information about this type.
Lease Time	This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 29.2.4 on page 462), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the USG in one session before having to log in again. Unlike Lease Time, the user has no opportunity to renew the session without logging out.
Miscellaneous Settings	
Allow renewing lease time automatically	Select this check box if access users can renew lease time automatically, as well as manually, simply by selecting the Updating lease time automatically check box on their screen.
Enable user idle detection	This is applicable for access users. Select this check box if you want the USG to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The USG automatically logs out the access user once the User idle timeout has been reached.
User idle timeout	This is applicable for access users. This field is effective when Enable user idle detection is checked. Type the number of minutes each access user can be logged in and idle before the USG automatically logs out the access user.
User Logon Settings	
Limit the number of simultaneous logons for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when Limit ... for administration account is checked. Type the maximum number of simultaneous logins by each admin user.
Limit the number of simultaneous logons for access account	Select this check box if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can login as many times as they want as long as they use different IP addresses.
Maximum number per access account	This field is effective when Limit ... for access account is checked. Type the maximum number of simultaneous logins by each access user.

Table 183 Configuration > Object > User/Group > Setting (continued)

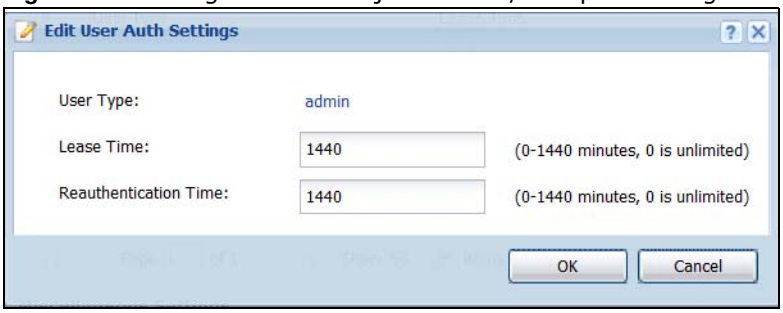
LABEL	DESCRIPTION
User Lockout Settings	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when Enable logon retry limit is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified lockout period. The number must be between 1 and 99.
Lockout period	This field is effective when Enable logon retry limit is checked. Type the number of minutes the user must wait to try to login again, if logon retry limit is enabled and the maximum retry count is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click Apply to save the changes.
Reset	Click Reset to return the screen to its last-saved settings.

29.2.4.1 Default User Authentication Timeout Settings Edit Screens

The Default Authentication Timeout Settings Edit screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.

To access this screen, go to the Configuration > Object > User/Group > Setting screen (see Section 29.2.4 on page 462), and click one of the Default Authentication Timeout Settings section's Edit icons.

Figure 312 Configuration > Object > User/Group > Setting > Edit



The following table describes the labels in this screen.

Table 184 Configuration > Object > User/Group > Setting > Edit

LABEL	DESCRIPTION
User Type	This read-only field identifies the type of user account for which you are configuring the default settings. • admin - this user can look at and change the configuration of the USG • limited-admin - this user can look at the configuration of the USG but not to change it. • user - this user has access to the USG's services but cannot look at the configuration. • guest - this user has access to the USG's services but cannot look at the configuration. • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 456 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 457 for more information about this type.
Lease Time	Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 29.2.4 on page 462), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	Type the number of minutes this type of user account can be logged into the USG in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike Lease Time, the user has no opportunity to renew the session without logging out.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.2.4.2 User Aware Login Example

Access users cannot use the Web Configurator to browse the configuration of the USG. Instead, after access users log into the USG, the following screen appears.

Figure 313 Web Configurator for Non-Admin Users



The following table describes the labels in this screen.

Table 185 Web Configurator for Non-Admin Users

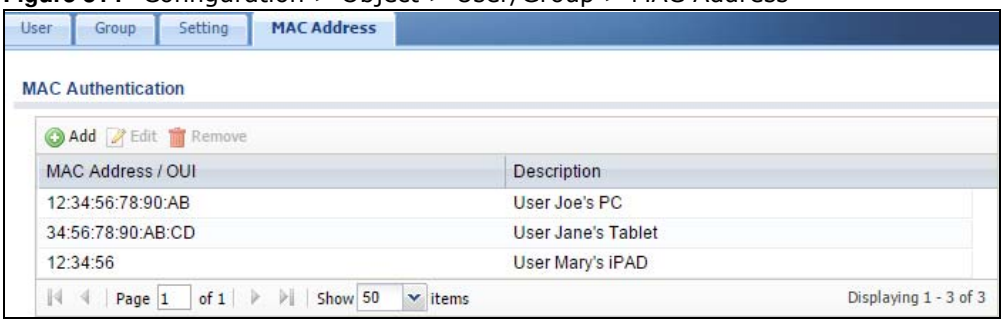
LABEL	DESCRIPTION
User-defined lease time (max ... minutes)	Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified.
Renew	Access users can click this button to reset the lease time, the amount of time remaining before the USG automatically logs them out. The USG sets this amount of time according to the • User-defined lease time field in this screen • Lease time field in the User Add/ Edit screen (see Section 29.2.5.1 on page 468) • Lease time field in the Setting screen (see Section 29.2.4 on page 462)
Updating lease time automatically	This box appears if you checked the Allow renewing lease time automatically box in the Setting screen. (See Section 29.2.4 on page 462.) Access users can select this check box to reset the lease time automatically 30 seconds before it expires. Otherwise, access users have to click the Renew button to reset the lease time.
Remaining time before lease timeout	This field displays the amount of lease time that remains, though the user might be able to reset it.
Remaining time before auth. timeout	This field displays the amount of time that remains before the USG automatically logs the access user out, regardless of the lease time.

29.2.5 User/Group MAC Address Summary Screen

This screen shows the MAC addresses of wireless clients, which can be authenticated by their MAC addresses using the local user database. Click Configuration > Object > User/ Group > MAC Address to open this screen.

Note: You need to configure an SSID security profile's MAC authentication settings to have the AP use the USG's local database to authenticate wireless clients by their MAC addresses.

Figure 314 Configuration > Object > User/Group > MAC Address



The following table describes the labels in this screen.

Table 186 Configuration > Object > User/Group > MAC Address

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.

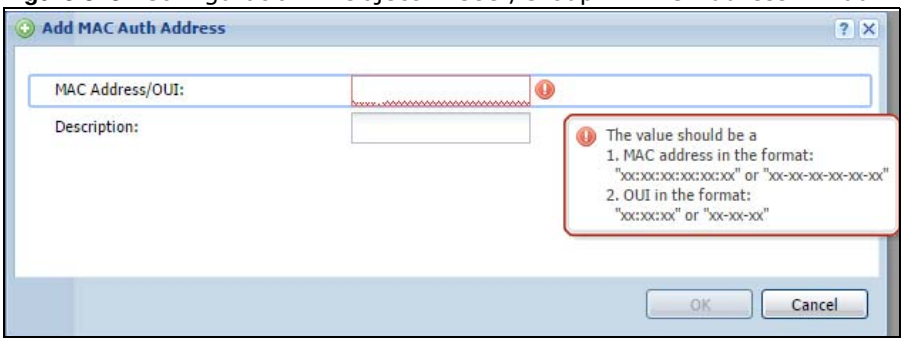
Table 186 Configuration > Object > User/Group > MAC Address (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
MAC Address/ OUI	This field displays the MAC address or OUI (Organizationally Unique Identifier of computer hardware manufacturers) of wireless clients using MAC authentication with the USG local user database.
Description	This field displays a description of the device identified by the MAC address or OUI.

29.2.5.1 MAC Address Add/Edit Screen

This screen allows you to create a new allowed device or edit an existing one. To access this screen, go to the MAC Address screen (see Section 29.2.5 on page 467), and click either the Add icon or an Edit icon.

Figure 315 Configuration > Object > User/Group > MAC Address > Add



The following table describes the labels in this screen.

Table 187 Configuration > Object > User/Group > MAC Address > Add

LABEL	DESCRIPTION
MAC Address/ OUI	Type the MAC address (six hexadecimal number pairs separated by colons or hyphens) or OUI (three hexadecimal number pairs separated by colons or hyphens) to identify specific wireless clients for MAC authentication using the USG local user database. The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.
Description	Enter an optional description of the wireless device(s) identified by the MAC or OUI. You can use up to 60 characters, punctuation marks, and spaces.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.2.6 User /Group Technical Reference

This section provides some information on users who use an external authentication server in order to log in.

Setting up User Attributes in an External Server

To set up user attributes, such as reauthentication time, in LDAP or RADIUS servers, use the following keywords in the user configuration file.

Table 188 LDAP/RADIUS: Keywords for User Attributes

KEYWORD	CORRESPONDING ATTRIBUTE IN WEB CONFIGURATOR
type	User Type. Possible Values: admin, limited-admin, user, guest.
leaseTime	Lease Time. Possible Values: 1-1440 (minutes).
reauthTime	Reauthentication Time. Possible Values: 1-1440 (minutes).

The following examples show you how you might set up user attributes in LDAP and RADIUS servers.

Figure 316 LDAP Example: Keywords for User Attributes

```
type: admin
leaseTime: 99
reauthTime: 199
```

Figure 317 RADIUS Example: Keywords for User Attributes

```
type=user;leaseTime=222;reauthTime=222
```

Creating a Large Number of Ext-User Accounts

If you plan to create a large number of Ext-User accounts, you might use CLI commands, instead of the Web Configurator, to create the accounts. Extract the user names from the LDAP or RADIUS server, and create a shell script that creates the user accounts.

29.3 AP Profile Overview

This section shows you how to configure preset profiles for the Access Points (APs) connected to your USG's wireless network.

- The Radio screen (Section 29.3.1 on page 470) creates radio configurations that can be used by the APs.
- The SSID screen (Section 29.3.2 on page 476) configures three different types of profiles for your networked APs.

29.3.0.1 What You Need To Know

The following terms and concepts may help as you read this section.

Wireless Profiles

At the heart of all wireless AP configurations on the USG are profiles. A profile represents a group of saved settings that you can use across any number of connected APs. You can set up the following wireless profile types:

- Radio - This profile type defines the properties of an AP's radio transmitter. You can have a maximum of 32 radio profiles on the USG.
- SSID - This profile type defines the properties of a single wireless network signal broadcast by an AP. Each radio on a single AP can broadcast up to 8 SSIDs. You can have a maximum of 32 SSID profiles on the USG.
- Security - This profile type defines the security settings used by a single SSID. It controls the encryption method required for a wireless client to associate itself with the SSID. You can have a maximum of 32 security profiles on the USG.
- MAC Filtering - This profile provides an additional layer of security for an SSID, allowing you to block access or allow access to that SSID based on wireless client MAC addresses. If a client's MAC address is on the list, then it is either allowed or denied, depending on how you set up the MAC Filter profile. You can have a maximum of 32 MAC filtering profiles on the USG.

SSID

The SSID (Service Set IDentifier) is the name that identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. In other words, it is the name of the wireless network that clients use to connect to it.

WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the AP and the wireless stations associated with it in order to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. Key differences between WPA(2) and WEP are improved data encryption and user authentication.

IEEE 802.1x

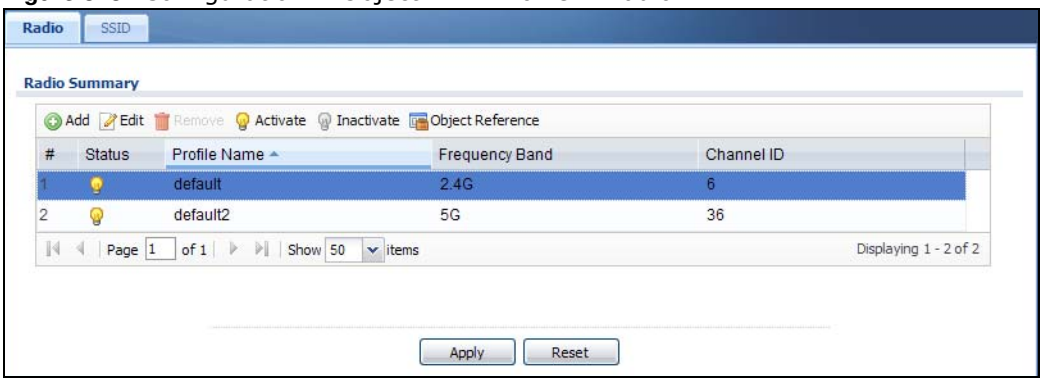
The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication is done using an external RADIUS server.

29.3.1 Radio Screen

This screen allows you to create radio profiles for the APs on your network. A radio profile is a list of settings that the built-in AP can use to configure its radio transmitters. To access this screen click Configuration > Object > AP Profile.

Note: You can have a maximum of 32 radio profiles on the USG.

Figure 318 Configuration > Object > AP Profile > Radio



The following table describes the labels in this screen.

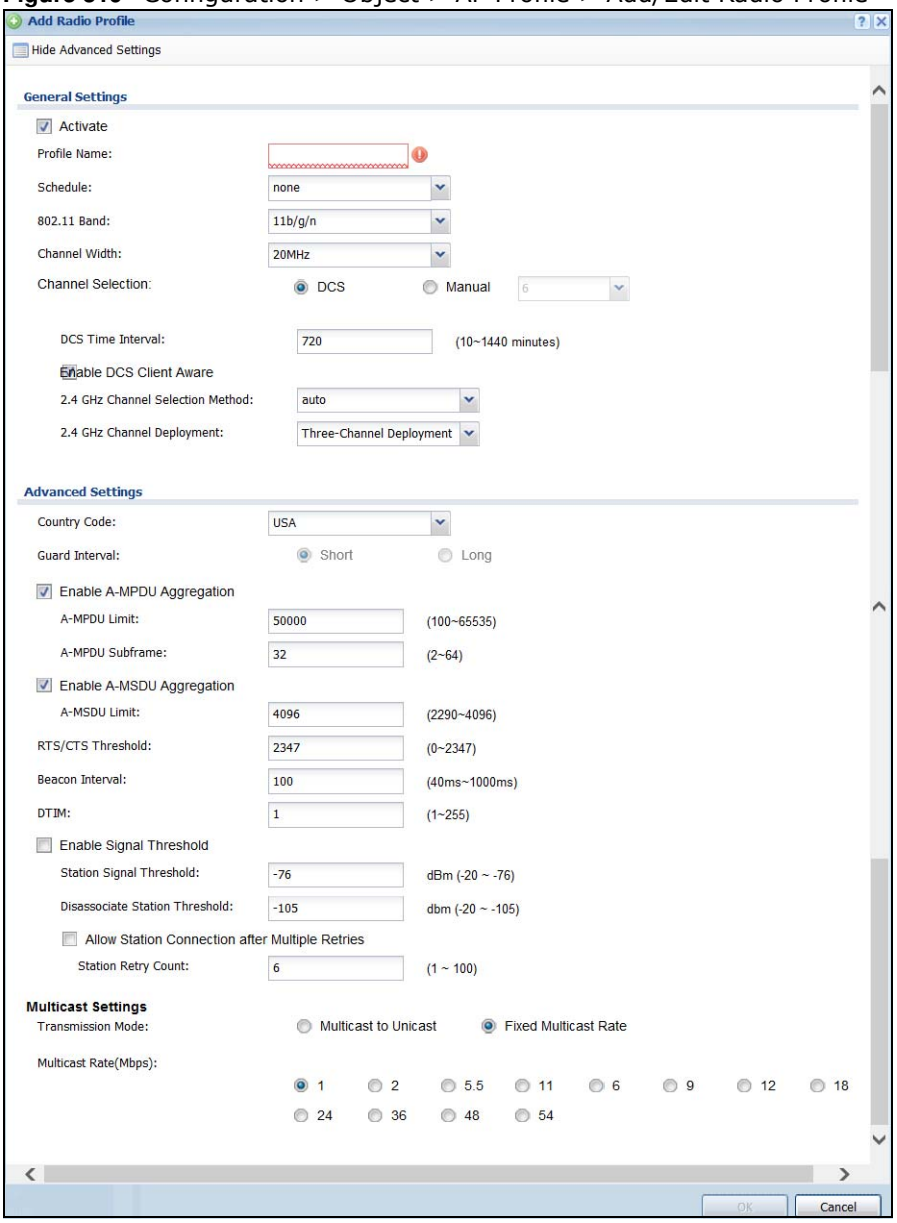
Table 189 Configuration > Object > AP Profile > Radio

LABEL	DESCRIPTION
Add	Click this to add a new radio profile.
Edit	Click this to edit the selected radio profile.
Remove	Click this to remove the selected radio profile.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Object Reference	Click this to view which other objects are linked to the selected radio profile.
#	This field is a sequential value, and it is not associated with a specific profile.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field indicates the name assigned to the radio profile.
Frequency Band	This field indicates the frequency band which this radio profile is configured to use.
Channel ID	This field indicates the broadcast channel which this radio profile is configured to use.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

29.3.1.1 Add/Edit Radio Profile

This screen allows you to create a new radio profile or edit an existing one. To access this screen, click the Add button or select a radio profile from the list and click the Edit button.

Figure 319 Configuration > Object > AP Profile > Add/Edit Radio Profile



The following table describes the labels in this screen.

Table 190 Configuration > Object > AP Profile > Add/Edit Radio Profile

LABEL	DESCRIPTION
Hide / Show Advanced Settings	Click this to hide or show the Advanced Settings in this window.
Create New Object	Select an item from this menu to create a new object of that type. Any objects created in this way are automatically linked to this radio profile.
General Settings	

Table 190 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
Activate	Select this option to make this profile active.
Profile Name	Enter up to 31 alphanumeric characters to be used as this profile's name. Spaces and underscores are allowed.
802.11 Band	Select the wireless band which this radio profile should use. 2.4 GHz is the frequency used by IEEE 802.11b/g/n wireless clients. 5 GHz is the frequency used by IEEE 802.11ac/a/n wireless clients.
Channel Width	Select the wireless channel bandwidth you want the AP to use. A standard 20 MHz channel offers transfer speeds of up to 217Mbps (2.4GHz) or 217Mbps (5GHZ) whereas a 40MHz channel uses two standard channels and offers speeds of up to 450Mbps (2.4GHz) or 450Mbps (5GHZ). An IEEE 802.11ac-specific 80MHz channel offers speeds of up to 1.3Gbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. A 80 MHz channel consists of two adjacent 40 MHz channels. The wireless clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Because not all devices support 40 MHz and/or 80 MHz channels, select 20/40MHz or 20/40/80MHz to allow the AP to adjust the channel bandwidth automatically. Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.
Channel Selection	Select the wireless channel which this radio profile should use. Select DCS to have the AP automatically select the radio channel upon which it broadcasts by scanning the area around it and determining what channels are currently being used by other devices. Select Manual and specify the channels the AP uses. It is recommended that you choose the channel least in use by other APs in the region where this profile will be implemented. This will reduce the amount of interference between wireless clients and the AP to which this profile is assigned. Some 5 GHz channels include the label indoor use only. These are for use with an indoor AP only. Do not use them with an outdoor AP. Note: If you change the country code later, **Channel Selection** is set to **Manual** automatically.
DCS Time Interval	This field is available when you set Channel Selection to DCS. Enter a number of minutes. This regulates how often the USG surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the USG will then dynamically select the next available clean channel or a channel with lower interference.
Enable DCS Client Aware	This field is available when you set Channel Selection to DCS. Select this to have the AP wait until all connected clients have disconnected before switching channels. If you disable this then the AP switches channels immediately regardless of any client connections. In this instance, clients that are connected to the AP when it switches channels are dropped.

Table 190 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
2.4 GHz Channel Selection Method	This field is available when you set Channel Selection to DCS. Select auto to have the AP search for available channels automatically in the 2.4 GHz band. The available channels vary depending on what you select in the 2.4 GHz Channel Deployment field. Select manual and specify the channels the AP uses in the 2.4 GHz band.
Channel ID	This field is available only when you set Channel Selection to DCS and set 2.4 GHz Channel Selection Method to manual. Select the check boxes of the channels that you want the AP to use.
2.4 GHz Channel Deployment	This field is available only when you set Channel Selection to DCS and set 2.4 GHz Channel Selection Method to auto. Select Three-Channel Deployment to limit channel switching to channels 1,6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three "safe" channels. Select Four-Channel Deployment to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1-11 then the USG uses channels 1, 4, 7, 11 in this configuration; otherwise, the USG uses channels 1, 5, 9, 13 in this configuration. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum.
Enable 5 GHz DFS Aware	This field is available only when you select 11a, 11a/n or 11ac in the 802.11 Band field. Select this if your APs are operating in an area known to have RADAR devices. This allows the device to downgrade its frequency to below 5 GHz in the event a RADAR signal is detected, thus preventing it from interfering with that signal. Enabling this forces the AP to select a non-DFS channel.
5 GHz Channel Selection Method	This shows auto and allows the AP to search for available channels automatically in the 5 GHz band.
Advanced Settings	
Country Code	Select the country where the USG is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems.
Guard Interval	This field is available only when the channel width is 20/40MHz or 20/40/80MHz. Set the guard interval for this radio profile to either short or long. The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the interval increases data transfer rates but also increases interference. Increasing the interval reduces data transfer rates but also reduces interference.
Enable A-MPDU Aggregation	Select this to enable A-MPDU aggregation. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.
A-MPDU Limit	Enter the maximum frame size to be aggregated.
A-MPDU Subframe	Enter the maximum number of frames to be aggregated each time.

Table 190 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
Enable A-MSDU Aggregation	Select this to enable A-MSDU aggregation. Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates.
A-MSDU Limit	Enter the maximum frame size to be aggregated.
RTS/CTS Threshold	Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
Enable Signal Threshold	Select the check box to use the signal threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP. Clear the check box to not require wireless clients to have a minimum signal strength to connect to the AP.
Station Signal Threshold	Set a minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold. -20 dBm is the strongest signal you can require and -76 is the weakest.
Disassociate Station Threshold	Set a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the USG disconnects the wireless client from the AP. -20 dBm is the strongest signal you can require and -90 is the weakest.
Allow Station Connection after Multiple Retries	Select this option to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength.
Station Retry Count	Set the maximum number of times a wireless client can attempt to re-connect to the AP.
Multicast Settings	Use this section to set a transmission mode and maximum rate for multicast traffic.
Transmission Mode	Set how the AP handles multicast traffic. Select Multicast to Unicast to broadcast wireless multicast traffic to all of the wireless clients as unicast traffic. Unicast traffic dynamically changes the data rate based on the application's bandwidth requirements. The retransmit mechanism of unicast traffic provides more reliable transmission of the multicast traffic, although it also produces duplicate packets. Select Fixed Multicast Rate to send wireless multicast traffic at a single data rate. You must know the multicast application's bandwidth requirements and set it in the following field.
Multicast Rate (Mbps)	If you set the multicast transmission mode to fixed multicast rate, set the data rate for multicast traffic here. For example, to deploy 4 Mbps video, select a fixed multicast rate higher than 4 Mbps.

Table 190 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.3.2 SSID Screen

The SSID screens allow you to configure three different types of profiles for your networked APs: an SSID list, which can assign specific SSID configurations to your APs; a security list, which can assign specific encryption methods to the APs when allowing wireless clients to connect to them; and a MAC filter list, which can limit connections to an AP based on wireless clients MAC addresses.

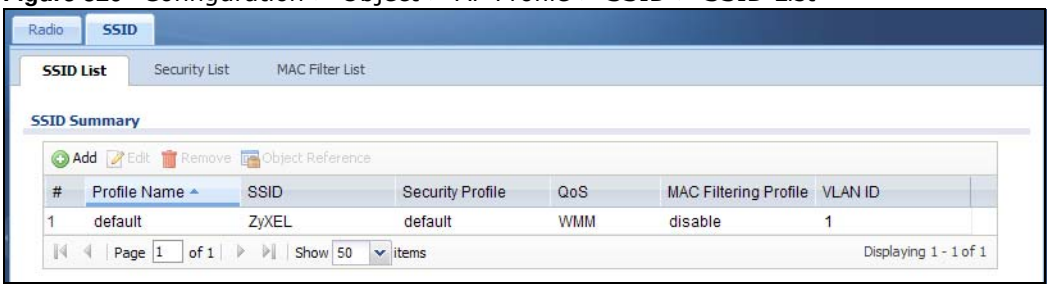
29.3.2.1 SSID List

This screen allows you to create and manage SSID configurations that can be used by the APs. An SSID, or Service Set IDentifier, is basically the name of the wireless network to which a wireless client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies (such as the WiFi adapter in a laptop), and is displayed as the wireless network name when a person makes a connection to it.

To access this screen click Configuration > Object > AP Profile > SSID.

Note: You can have a maximum of 32 SSID profiles on the USG.

Figure 320 Configuration > Object > AP Profile > SSID > SSID List



The following table describes the labels in this screen.

Table 191 Configuration > Object > AP Profile > SSID > SSID List

LABEL	DESCRIPTION
Add	Click this to add a new SSID profile.
Edit	Click this to edit the selected SSID profile.
Remove	Click this to remove the selected SSID profile.
Object Reference	Click this to view which other objects are linked to the selected SSID profile (for example, radio profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the SSID profile.
SSID	This field indicates the SSID name as it appears to wireless clients.
Security Profile	This field indicates which (if any) security profile is associated with the SSID profile.
QoS	This field indicates the QoS type associated with the SSID profile.

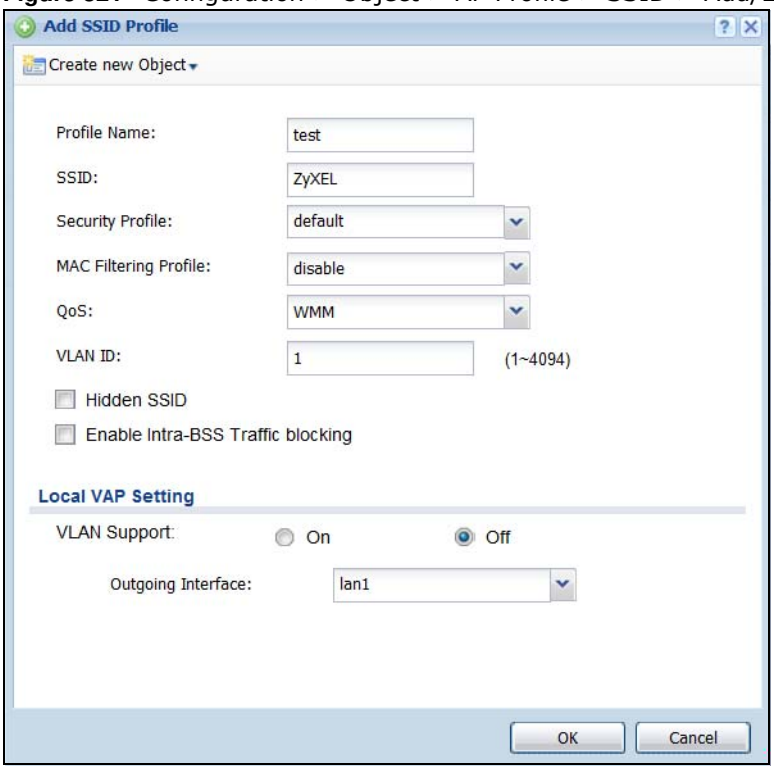
Table 191 Configuration > Object > AP Profile > SSID > SSID List (continued)

LABEL	DESCRIPTION
MAC Filtering Profile	This field indicates which (if any) MAC Filter Profile is associated with the SSID profile.
VLAN ID	This field indicates the VLAN ID associated with the SSID profile.

29.3.2.2 Add/Edit SSID Profile

This screen allows you to create a new SSID profile or edit an existing one. To access this screen, click the Add button or select an SSID profile from the list and click the Edit button.

Figure 321 Configuration > Object > AP Profile > SSID > Add/Edit SSID Profile



The following table describes the labels in this screen.

Table 192 Configuration > Object > AP Profile > SSID > Add/Edit SSID Profile

LABEL	DESCRIPTION
Create new Object	Select an object type from the list to create a new one associated with this SSID profile.
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
SSID	Enter the SSID name for this profile. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed.
Security Profile	Select a security profile from this list to associate with this SSID. If none exist, you can use the Create new Object menu to create one. Note: It is highly recommended that you create security profiles for all of your SSIDs to enhance your network security.

Table 192 Configuration > Object > AP Profile > SSID > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
MAC Filtering Profile	Select a MAC filtering profile from the list to associate with this SSID. If none exist, you can use the Create new Object menu to create one. MAC filtering allows you to limit the wireless clients connecting to your network through a particular SSID by wireless client MAC addresses. Any clients that have MAC addresses not in the MAC filtering profile of allowed addresses are denied connections. The disable setting means no MAC filtering is used.
QoS	Select a Quality of Service (QoS) access category to associate with this SSID. Access categories minimize the delay of data packets across a wireless network. Certain categories, such as video or voice, are given a higher priority due to the time sensitive nature of their data packets. QoS access categories are as follows: disable: Turns off QoS for this SSID. All data packets are treated equally and not tagged with access categories. WMM: Enables automatic tagging of data packets. The USG assigns access categories to the SSID by examining data as it passes through it and making a best guess effort. If something looks like video traffic, for instance, it is tagged as such. WMM_VOICE: All wireless traffic to the SSID is tagged as voice data. This is recommended if an SSID is used for activities like placing and receiving VoIP phone calls. WMM_VIDEO: All wireless traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing. WMM_BEST_EFFORT: All wireless traffic to the SSID is tagged as "best effort," meaning the data travels the best route it can without displacing higher priority traffic. This is good for activities that do not require the best bandwidth throughput, such as surfing the Internet. WMM_BACKGROUND: All wireless traffic to the SSID is tagged as low priority or "background traffic", meaning all other access categories take precedence over this one. If traffic from an SSID does not have strict throughput requirements, then this access category is recommended. For example, an SSID that only has network printers connected to it.
VLAN ID	Enter the VLAN ID that will be used to tag all traffic originating from this SSID if the VLAN is different from the native VLAN.
Hidden SSID	Select this if you want to "hide" your SSID from wireless clients. This tells any wireless clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wireless clients respect this flag and display it anyway. When an SSID is "hidden" and a wireless client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your wireless connection setup screen(s) (these vary by client, client connectivity software, and operating system).
Enable Intra-BSS Traffic Blocking	Select this option to prevent crossover traffic from within the same SSID.
Local VAP Setting	This part of the screen only applies to USG models that have built-in wireless functionality (AP) - see Table 1 on page 19.
VLAN Support	Select On to have the USG assign the VLAN ID listed in the top part of the screen to the built-in AP. Select Off to have the USG ignore the VLAN ID listed in the top part of the screen. Select an Outgoing Interface to have the USG assign an IP address in the same subnet as the selected interface to the built-in AP.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

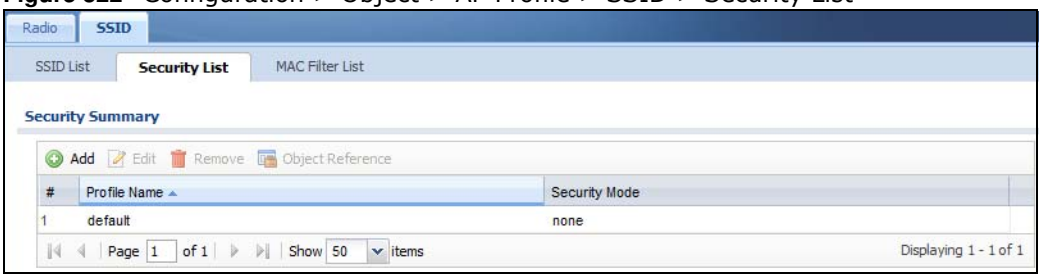
29.3.2.3 Security List

This screen allows you to manage wireless security configurations that can be used by your SSIDs. Wireless security is implemented strictly between the AP broadcasting the SSID and the stations that are connected to it.

To access this screen click Configuration > Object > AP Profile > SSID > Security List.

Note: You can have a maximum of 32 security profiles on the USG.

Figure 322 Configuration > Object > AP Profile > SSID > Security List



The following table describes the labels in this screen.

Table 193 Configuration > Object > AP Profile > SSID > Security List

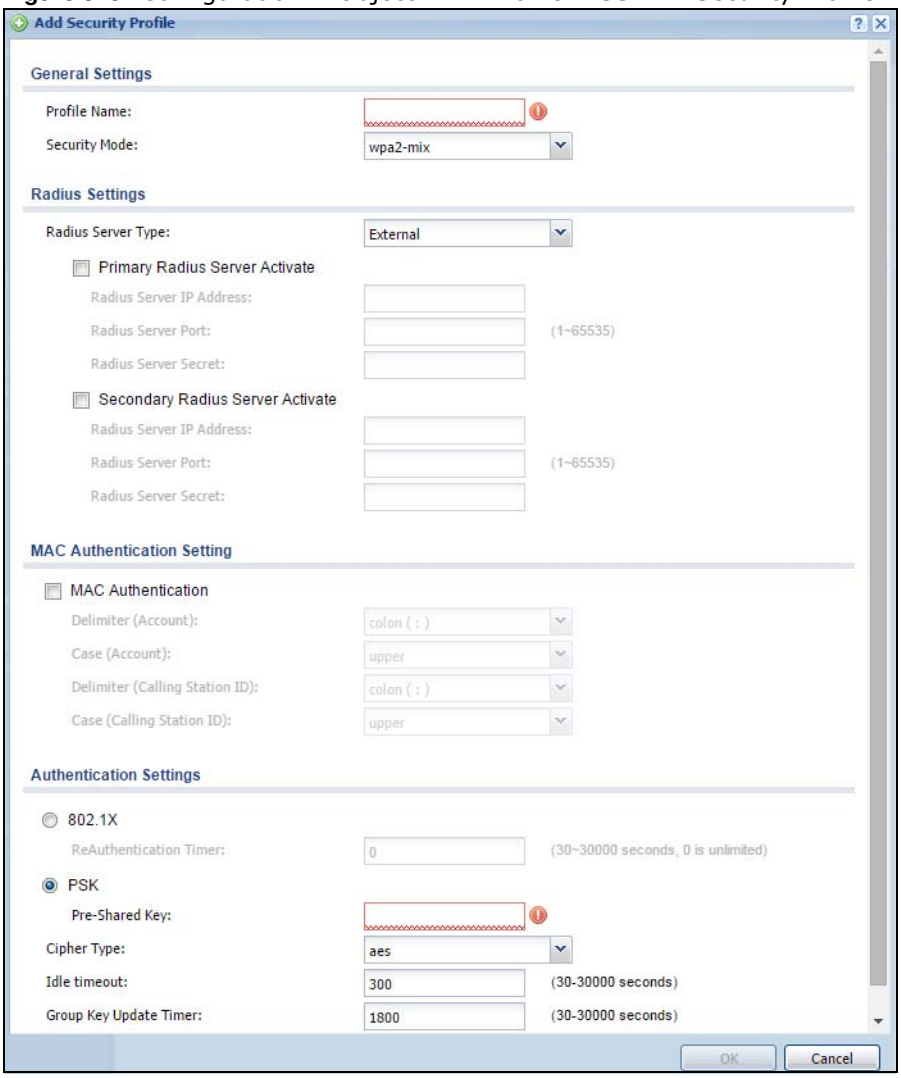
LABEL	DESCRIPTION
Add	Click this to add a new security profile.
Edit	Click this to edit the selected security profile.
Remove	Click this to remove the selected security profile.
Object Reference	Click this to view which other objects are linked to the selected security profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the security profile.
Security Mode	This field indicates this profile's security mode (if any).

29.3.2.3.1 Add/Edit Security Profile

This screen allows you to create a new security profile or edit an existing one. To access this screen, click the Add button or select a security profile from the list and click the Edit button.

Note: This screen's options change based on the Security Mode selected. Only the default screen is displayed here.

Figure 323 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile



The following table describes the labels in this screen.

Table 194 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: none, wep, wpa2, or wpa2-mix.
Radius Server Type	Select Internal to use the USG's internal authentication database, or External to use an external RADIUS server for authentication.

Table 194 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

LABEL	DESCRIPTION
Primary / Secondary Radius Server Activate	Select this to have the USG use the specified RADIUS server.
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
MAC Authentication	Select this to use an external server or the USG's local database to authenticate wireless clients by their MAC addresses. Users cannot get an IP address if the MAC authentication fails. An external server can use the wireless client's account (username/password) or Calling Station ID for MAC authentication. Configure the ones the external server uses.
Delimiter (Account)	Select the separator the external server uses for the two-character pairs within account MAC addresses.
Case (Account)	Select the case (upper or lower) the external server requires for letters in the account MAC addresses.
Delimiter (Calling Station ID)	RADIUS servers can require the MAC address in the Calling Station ID RADIUS attribute. Select the separator the external server uses for the pairs in calling station MAC addresses.
Case (Calling Station ID)	Select the case (upper or lower) the external server requires for letters in the calling station MAC addresses.
802.1X	Select this to enable 802.1x secure authentication.
Auth. Method	This field is available only when you set the RADIUS server type to Internal. Select an authentication method if you have created any in the Configuration > Object > Auth. Method screen.
ReAuthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited requests.
The following fields are available if you set Security Mode to wep.	
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Authentication Type	Select a WEP authentication method. Choices are Open or Share key.
Key Length	Select the bit-length of the encryption key to be used in WEP connections. If you select WEP-64: • Enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each Key used. or • Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each Key used. If you select WEP-128: • Enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each Key used. or • Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each Key used.
Key 1~4	Based on your Key Length selection, enter the appropriate length hexadecimal or ASCII key.

Table 194 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

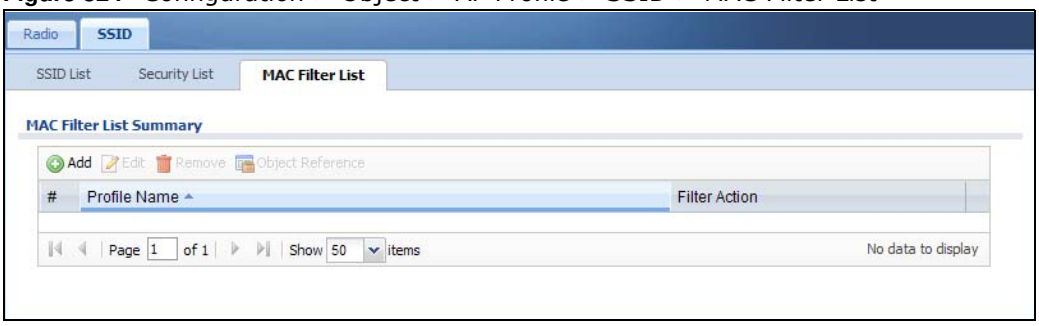
LABEL	DESCRIPTION
The following fields are available if you set Security Mode to wpa2 or wpa2-mix.	
PSK	Select this option to use a Pre-Shared Key with WPA encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Cipher Type	Select an encryption cipher type from the list. • auto - This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. • tkip - This is the Temporal Key Integrity Protocol encryption method added later to the WEP encryption protocol to further secure. Not all wireless clients may support this. • aes - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this.
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA encryption key.
Pre-Authentication	This field is available only when you set Security Mode to wpa2 or wpa2-mix and enable 802.1x authentication. Enable or Disable pre-authentication to allow the AP to send authentication information to other APs on the network, allowing connected wireless clients to switch APs without having to re-authenticate their network connection.
Management Frame Protection	This field is available only when you select wpa2 or wpa2-mix in the Security Mode field and set Cipher Type to aes. Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks. Select the check box to enable management frame protection (MFP) to add security to 802.11 management frames. Select Optional if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. Select Required and wireless clients must support MFP in order to join the AP's wireless network.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.3.2.4 MAC Filter List

This screen allows you to create and manage security configurations that can be used by your SSIDs. To access this screen click Configuration > Object > AP Profile > SSID > MAC Filter List.

Note: You can have a maximum of 32 MAC filtering profiles on the USG.

Figure 324 Configuration > Object > AP Profile > SSID > MAC Filter List



The following table describes the labels in this screen.

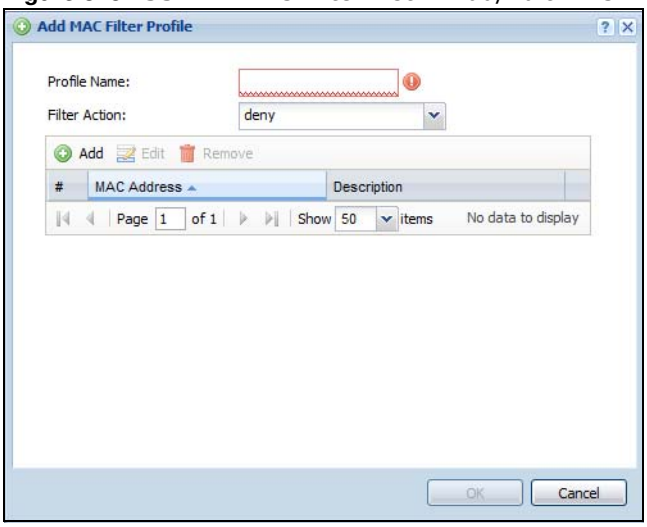
Table 195 Configuration > Object > AP Profile > SSID > MAC Filter List

LABEL	DESCRIPTION
Add	Click this to add a new MAC filtering profile.
Edit	Click this to edit the selected MAC filtering profile.
Remove	Click this to remove the selected MAC filtering profile.
Object Reference	Click this to view which other objects are linked to the selected MAC filtering profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the MAC filtering profile.
Filter Action	This field indicates this profile's filter action (if any).

29.3.2.4.1 Add/Edit MAC Filter Profile

This screen allows you to create a new MAC filtering profile or edit an existing one. To access this screen, click the Add button or select a MAC filter profile from the list and click the Edit button.

Figure 325 SSID > MAC Filter List > Add/Edit MAC Filter Profile



The following table describes the labels in this screen.

Table 196 SSID > MAC Filter List > Add/Edit MAC Filter Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Filter Action	Select allow to permit the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select deny to block the wireless clients with the specified MAC addresses.
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific profile.
MAC Address	This field specifies a MAC address associated with this profile.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.4 MON Profile

29.4.1 Overview

This screen allows you to set up monitor mode configurations that allow your connected APs to scan for other wireless devices in the vicinity.

29.4.1.1 What You Can Do in this Chapter

The MON Profile screen (Section 29.4.2 on page 485) creates preset monitor mode configurations that can be used by the APs.

29.4.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Active Scan

An active scan is performed when an 802.11-compatible wireless monitoring device is explicitly triggered to scan a specified channel or number of channels for other wireless devices broadcasting on the 802.11 frequencies by sending probe request frames.

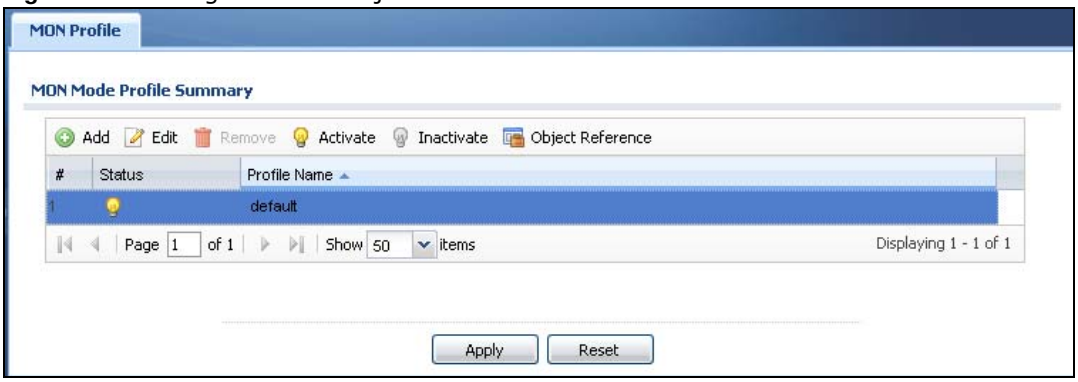
Passive Scan

A passive scan is performed when an 802.11-compatible monitoring device is set to periodically listen to a specified channel or number of channels for other wireless devices broadcasting on the 802.11 frequencies.

29.4.2 MON Profile

This screen allows you to create monitor mode configurations that can be used by the APs. To access this screen, login to the Web Configurator, and click Configuration > Object > MON Profile.

Figure 326 Configuration > Object > MON Profile



The following table describes the labels in this screen.

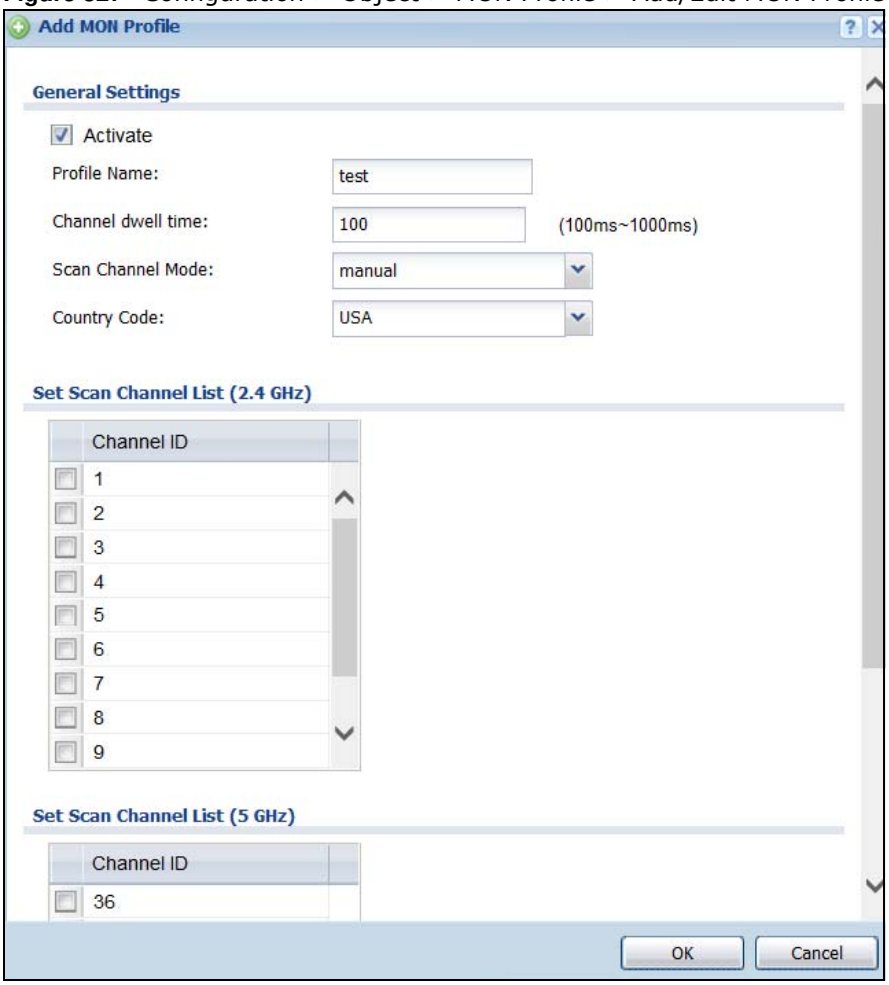
Table 197 Configuration > Object > MON Profile

LABEL	DESCRIPTION
Add	Click this to add a new monitor mode profile.
Edit	Click this to edit the selected monitor mode profile.
Remove	Click this to remove the selected monitor mode profile.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Object Reference	Click this to view which other objects are linked to the selected monitor mode profile (for example, an AP management profile).
#	This field is a sequential value, and it is not associated with a specific user.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field indicates the name assigned to the monitor profile.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

29.4.2.1 Add/Edit MON Profile

This screen allows you to create a new monitor mode profile or edit an existing one. To access this screen, click the Add button or select and existing monitor mode profile and click the Edit button.

Figure 327 Configuration > Object > MON Profile > Add/Edit MON Profile



The following table describes the labels in this screen.

Table 198 Configuration > Object > MON Profile > Add/Edit MON Profile

LABEL	DESCRIPTION
Activate	Select this to activate this monitor mode profile.
Profile Name	This field indicates the name assigned to the monitor mode profile.
Channel dwell time	Enter the interval (in milliseconds) before the AP switches to another channel for monitoring.
Scan Channel Mode	Select auto to have the AP switch to the next sequential channel once the Channel dwell time expires. Select manual to set specific channels through which to cycle sequentially when the Channel dwell time expires. Selecting this options makes the Scan Channel List options available.
Country Code	Select the country where the USG is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems.

Table 198 Configuration > Object > MON Profile > Add/Edit MON Profile (continued)

LABEL	DESCRIPTION
Set Scan Channel List (2.4 GHz)	Move a channel from the Available channels column to the Channels selected column to have the APs using this profile scan that channel when Scan Channel Mode is set to manual. These channels are limited to the 2 GHz range (802.11 b/g/n).
Set Scan Channel List (5 GHz)	Move a channel from the Available channels column to the Channels selected column to have the APs using this profile scan that channel when Scan Channel Mode is set to manual. These channels are limited to the 5 GHz range (802.11 a/n).
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.5 Address Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

- The Address screen (Section 29.5.2 on page 488) provides a summary of all addresses in the USG. Use the Address Add/ Edit screen to create a new address or edit an existing one.
- Use the Address Group summary screen (Section 29.5.2.2 on page 490) and the Address Group Add/ Edit screen, to maintain address groups in the USG.

29.5.1 What You Need To Know

Address objects and address groups are used in dynamic routes, security policies, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

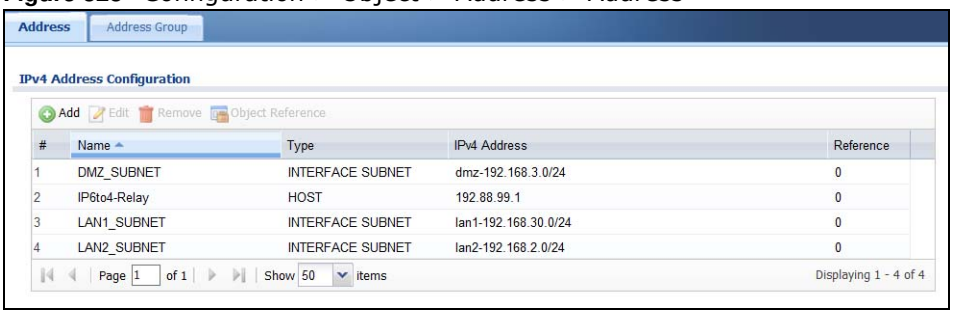
29.5.2 Address Summary Screen

The address screens are used to create, maintain, and remove addresses. There are the types of address objects.

- HOST - a host address is defined by an IP Address.
- RANGE - a range address is defined by a Starting IP Address and an Ending IP Address.
- SUBNET - a network address is defined by a Network IP address and Netmask subnet mask.

The Address screen provides a summary of all addresses in the USG. To access this screen, click Configuration > Object > Address > Address. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 328 Configuration > Object > Address > Address



The following table describes the labels in this screen. See Section 29.5.2.1 on page 489 for more information as well.

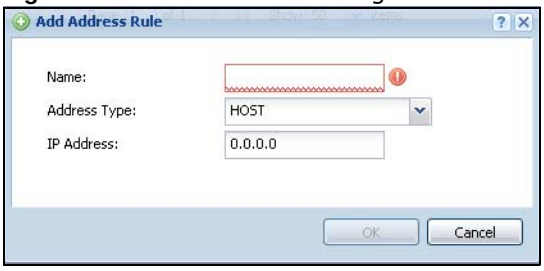
Table 199 Configuration > Object > Address > Address

LABEL	DESCRIPTION
IPv4 Address Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific address.
Name	This field displays the configured name of each address object.
Type	This field displays the type of each address object. "INTERFACE" means the object uses the settings of one of the USG's interfaces.
IPv4 Address	This field displays the IPv4 addresses represented by each address object. If the object's settings are based on one of the USG's interfaces, the name of the interface displays first followed by the object's current address settings.
Reference	This displays the number of times an object reference is used in a profile.

29.5.2.1 IPv4 Address Add/Edit Screen

The Configuration > IPv4 Address Add/Edit screen allows you to create a new address or edit an existing one. To access this screen, go to the Address screen (see Section 29.5.2 on page 488), and click either the Add icon or an Edit icon in the IPv4 Address Configuration section.

Figure 329 IPv4 Address Configuration > Add/Edit



The following table describes the labels in this screen.

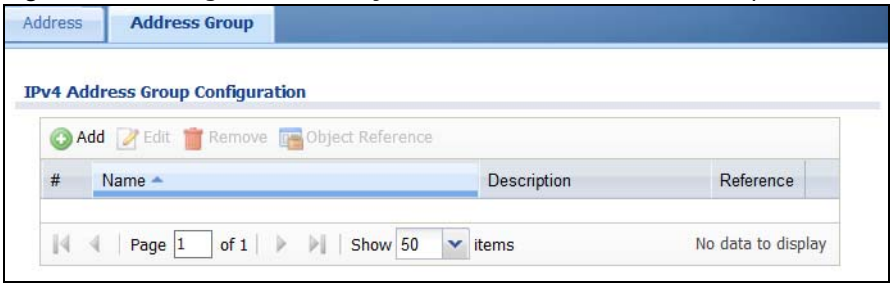
Table 200 IPv4 Address Configuration > Add/Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Address Type	Select the type of address you want to create. Choices are: HOST, RANGE, SUBNET, INTERFACE IP, INTERFACE SUBNET, and INTERFACE GATEWAY. Note: The USG automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change 1's IP address, the USG automatically updates the corresponding interface-based, LAN subnet address object.
IP Address	This field is only available if the Address Type is HOST. This field cannot be blank. Enter the IP address that this address object represents.
Starting IP Address	This field is only available if the Address Type is RANGE. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
Ending IP Address	This field is only available if the Address Type is RANGE. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network	This field is only available if the Address Type is SUBNET, in which case this field cannot be blank. Enter the IP address of the network that this address object represents.
Netmask	This field is only available if the Address Type is SUBNET, in which case this field cannot be blank. Enter the subnet mask of the network that this address object represents. Use dotted decimal format.
Interface	If you selected INTERFACE IP, INTERFACE SUBNET, or INTERFACE GATEWAY as the Address Type, use this field to select the interface of the network that this address object represents.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.5.2.2 Address Group Summary Screen

The Address Group screen provides a summary of all address groups. To access this screen, click Configuration > Object > Address > Address Group. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 330 Configuration > Object > Address > Address Group



The following table describes the labels in this screen. See Section 29.5.2.3 on page 491 for more information as well.

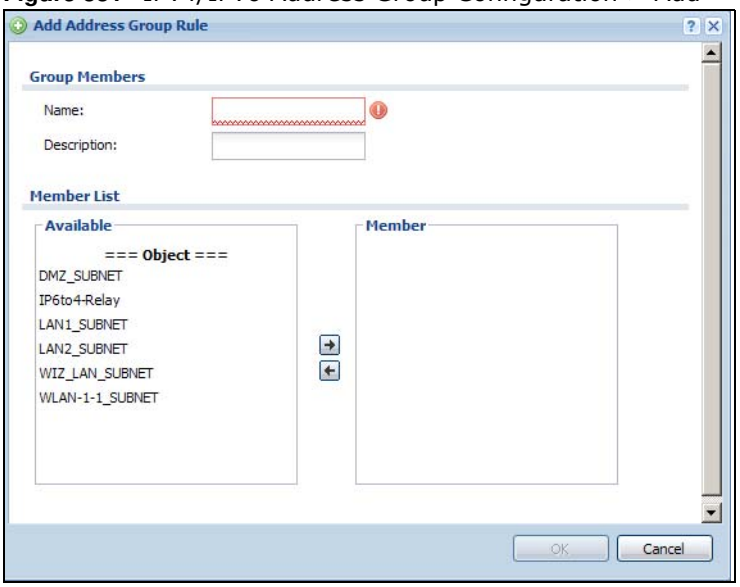
Table 201 Configuration > Object > Address > Address Group

LABEL	DESCRIPTION
IPv4 Address Group Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.
Reference	This displays the number of times an object reference is used in a profile.
IPv6 Address Group Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.

29.5.2.3 Address Group Add/Edit Screen

The Address Group Add/ Edit screen allows you to create a new address group or edit an existing one. To access this screen, go to the Address Group screen (see Section 29.5.2.2 on page 490), and click either the Add icon or an Edit icon in the IPv4 Address Group Configuration or IPv6 Address Group Configuration section.

Figure 331 IPv4/IPv6 Address Group Configuration > Add



The following table describes the labels in this screen.

Table 202 IPv4/IPv6 Address Group Configuration > Add

LABEL	DESCRIPTION
Name	Enter a name for the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	This field displays the description of each address group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	The Member list displays the names of the address and address group objects that have been added to the address group. The order of members is not important. Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.6 Service Overview

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

- Use the Service screens (Section 29.6.2 on page 493) to view and configure the USG's list of services and their definitions.
- Use the Service Group screens (Section 29.6.2 on page 493) to view and configure the USG's list of service groups.

29.6.1 What You Need to Know

IP Protocols

IP protocols are based on the eight-bit protocol field in the IP header. This field represents the next-level protocol that is sent in this packet. This section discusses three of the most common IP protocols.

Computers use Transmission Control Protocol (TCP, IP protocol 6) and User Datagram Protocol (UDP, IP protocol 17) to exchange data with each other. TCP guarantees reliable delivery but is slower and more complex. Some uses are FTP, HTTP, SMTP, and TELNET. UDP is simpler and faster but is less reliable. Some uses are DHCP, DNS, RIP, and SNMP.

TCP creates connections between computers to exchange data. Once the connection is established, the computers exchange data. If data arrives out of sequence or is missing, TCP puts it in sequence or waits for the data to be re-transmitted. Then, the connection is terminated.

In contrast, computers use UDP to send short messages to each other. There is no guarantee that the messages arrive in sequence or that the messages arrive at all.

Both TCP and UDP use ports to identify the source and destination. Each port is a 16-bit number. Some port numbers have been standardized and are used by low-level system processes; many others have no particular meaning.

Unlike TCP and UDP, Internet Control Message Protocol (ICMP, IP protocol 1) is mainly used to send error messages or to investigate problems. For example, ICMP is used to send the response if a computer cannot be reached. Another use is ping. ICMP does not guarantee delivery, but networks often treat ICMP messages differently, sometimes looking at the message itself to decide where to send it.

Service Objects and Service Groups

Use service objects to define IP protocols.

- TCP applications
- UDP applications
- ICMP messages
- user-defined services (for other types of IP protocols)

These objects are used in policy routes, and security policies.

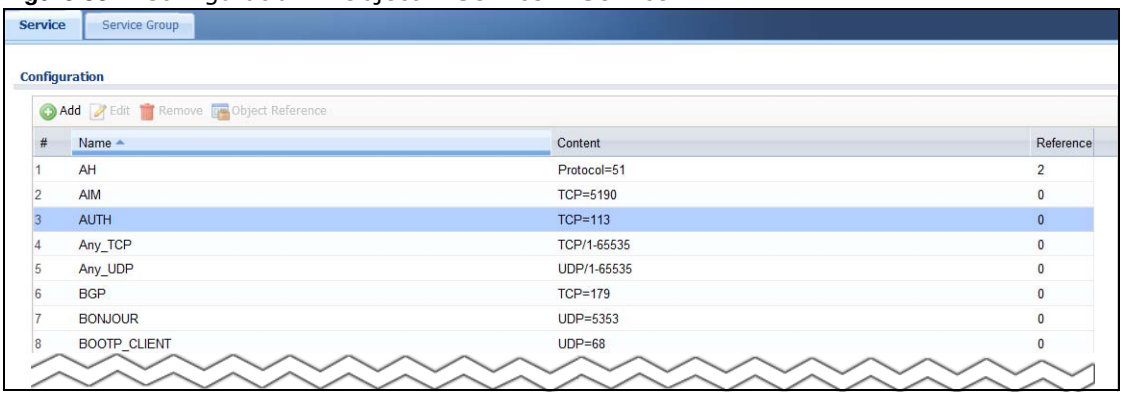
Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

29.6.2 The Service Summary Screen

The Service summary screen provides a summary of all services and their definitions. In addition, this screen allows you to add, edit, and remove services.

To access this screen, log in to the Web Configurator, and click Configuration > Object > Service > Service. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 332 Configuration > Object > Service > Service



The following table describes the labels in this screen.

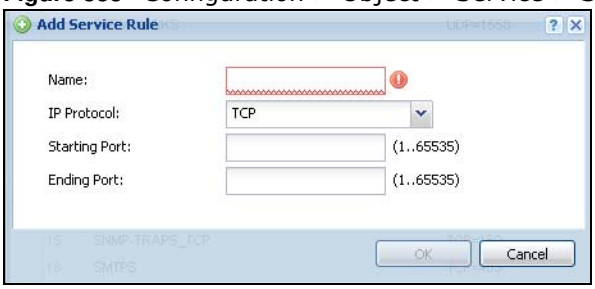
Table 203 Configuration > Object > Service > Service

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific service.
Name	This field displays the name of each service.
Content	This field displays a description of each service.
Reference	This displays the number of times an object reference is used in a profile.

29.6.2.1 The Service Add/Edit Screen

The Service Add/ Edit screen allows you to create a new service or edit an existing one. To access this screen, go to the Service screen (see Section 29.6.2 on page 493), and click either the Add icon or an Edit icon.

Figure 333 Configuration > Object > Service > Service > Edit



The following table describes the labels in this screen.

Table 204 Configuration > Object > Service > Service > Edit

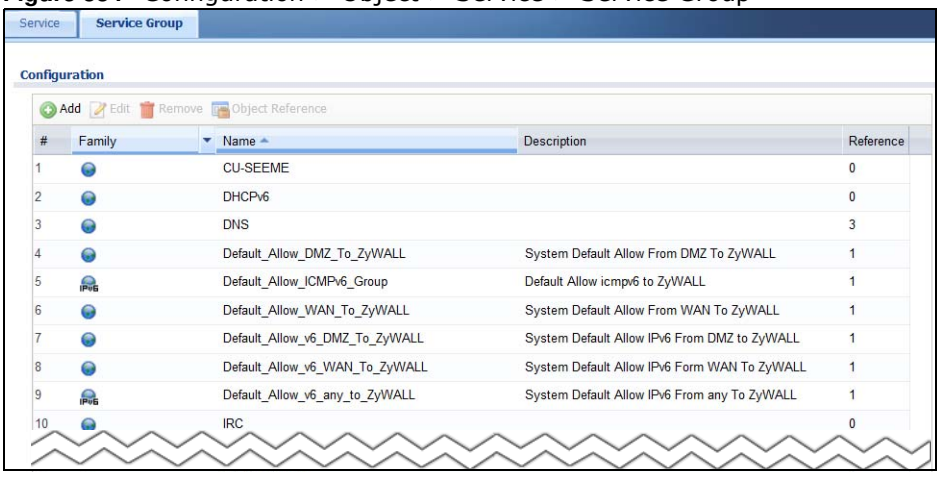
LABEL	DESCRIPTION
Name	Type the name used to refer to the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IP Protocol	Select the protocol the service uses. Choices are: TCP, UDP, ICMP, ICMPv6, and User Defined.
Starting Port Ending Port	This field appears if the IP Protocol is TCP or UDP. Specify the port number(s) used by this service. If you fill in one of these fields, the service uses that port. If you fill in both fields, the service uses the range of ports.
ICMP Type	This field appears if the IP Protocol is ICMP or ICMPv6. Select the ICMP message used by this service. This field displays the message text, not the message number.
IP Protocol Number	This field appears if the IP Protocol is User Defined. Enter the number of the next-level protocol (IP protocol). Allowed values are 1 - 255.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.6.3 The Service Group Summary Screen

The Service Group summary screen provides a summary of all service groups. In addition, this screen allows you to add, edit, and remove service groups.

To access this screen, log in to the Web Configurator, and click Configuration > Object > Service > Service Group.

Figure 334 Configuration > Object > Service > Service Group



The following table describes the labels in this screen. See Section 29.6.3.1 on page 496 for more information as well.

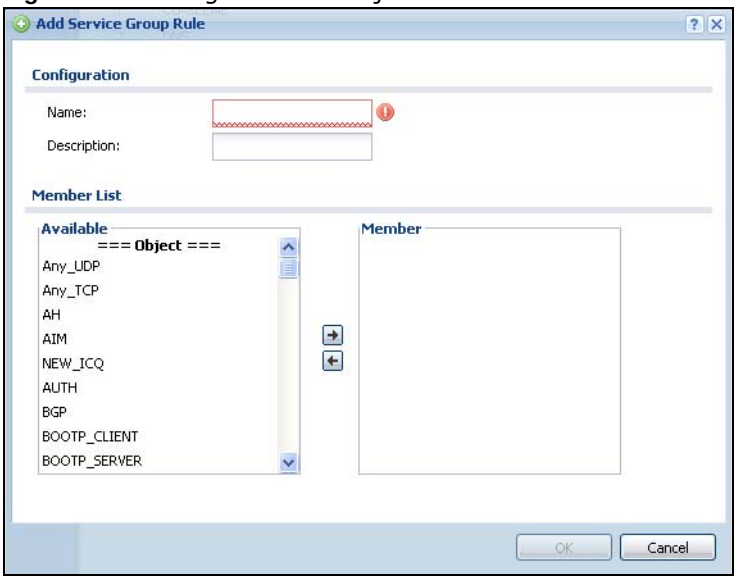
Table 205 Configuration > Object > Service > Service Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific service group.
Family	This field displays the Server Group supported type, which is according to your configurations in the Service Group Add/ Edit screen. There are 3 types of families: • : Supports IPv4 only • : Supports IPv6 only • : Supports both IPv4 and IPv6
Name	This field displays the name of each service group. By default, the USG uses services starting with "Default_Allow_" in the security policies to allow certain services to connect to the USG.
Description	This field displays the description of each service group, if any.
Reference	This displays the number of times an object reference is used in a profile.

29.6.3.1 The Service Group Add/Edit Screen

The Service Group Add/ Edit screen allows you to create a new service group or edit an existing one. To access this screen, go to the Service Group screen (see Section 29.6.3 on page 495), and click either the Add icon or an Edit icon.

Figure 335 Configuration > Object > Service > Service Group > Edit



The following table describes the labels in this screen.

Table 206 Configuration > Object > Service > Service Group > Edit

LABEL	DESCRIPTION
Name	Enter the name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.
Member List	The Member list displays the names of the service and service group objects that have been added to the service group. The order of members is not important. Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.7 Schedule Overview

Use schedules to set up one-time and recurring schedules for policy routes, security policies, and content filtering. The USG supports one-time and recurring schedules. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the USG.

Note: Schedules are based on the USG's current date and time.

- Use the Schedule summary screen (Section 29.7.2 on page 498) to see a list of all schedules in the USG.
- Use the One-Time Schedule Add/ Edit screen (Section 29.7.2.1 on page 499) to create or edit a one-time schedule.
- Use the Recurring Schedule Add/ Edit screen (Section 29.7.2.2 on page 500) to create or edit a recurring schedule.
- Use the Schedule Group screen (Section 29.7.3 on page 501) to merge individual schedule objects as one object.

29.7.1 What You Need to Know

One-time Schedules

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring Schedules

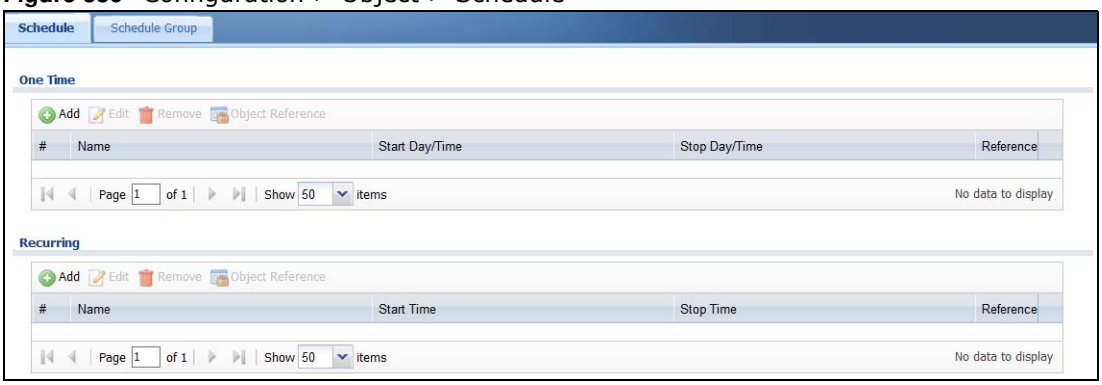
Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring

schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

29.7.2 The Schedule Summary Screen

The Schedule summary screen provides a summary of all schedules in the USG. To access this screen, click Configuration > Object > Schedule.

Figure 336 Configuration > Object > Schedule



The following table describes the labels in this screen. See Section 29.7.2.1 on page 499 and Section 29.7.2.2 on page 500 for more information as well.

Table 207 Configuration > Object > Schedule

LABEL	DESCRIPTION
One Time	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Day / Time	This field displays the date and time at which the schedule begins.
Stop Day / Time	This field displays the date and time at which the schedule ends.
Reference	This displays the number of times an object reference is used in a profile.
Recurring	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.

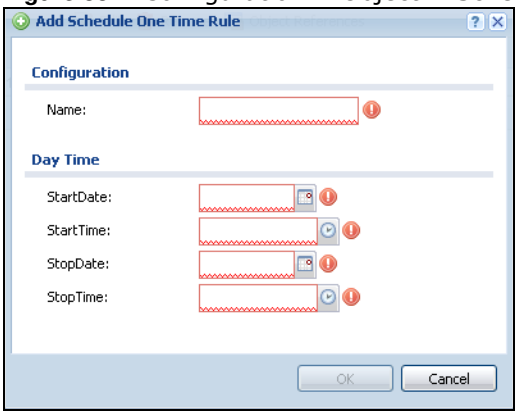
Table 207 Configuration > Object > Schedule (continued)

LABEL	DESCRIPTION
Start Time	This field displays the time at which the schedule begins.
Stop Time	This field displays the time at which the schedule ends.
Reference	This displays the number of times an object reference is used in a profile.

29.7.2.1 The One-Time Schedule Add/Edit Screen

The One-Time Schedule Add/Edit screen allows you to define a one-time schedule or edit an existing one. To access this screen, go to the Schedule screen (see Section 29.7.2 on page 498), and click either the Add icon or an Edit icon in the One Time section.

Figure 337 Configuration > Object > Schedule > Edit (One Time)



The following table describes the labels in this screen.

Table 208 Configuration > Object > Schedule > Edit (One Time)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the one-time schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartDate	Specify the year, month, and day when the schedule begins. • Year - 1900 - 2999 • Month - 1 - 12 • Day - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StartTime	Specify the hour and minute when the schedule begins. • Hour - 0 - 23 • Minute - 0 - 59
StopDate	Specify the year, month, and day when the schedule ends. • Year - 1900 - 2999 • Month - 1 - 12 • Day - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StopTime	Specify the hour and minute when the schedule ends. • Hour - 0 - 23 • Minute - 0 - 59

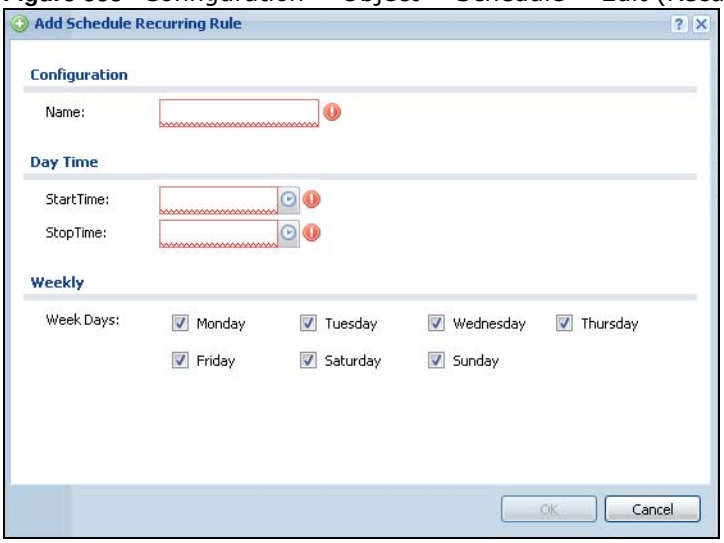
Table 208 Configuration > Object > Schedule > Edit (One Time) (continued)

LABEL	DESCRIPTION
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.7.2.2 The Recurring Schedule Add/Edit Screen

The Recurring Schedule Add/ Edit screen allows you to define a recurring schedule or edit an existing one. To access this screen, go to the Schedule screen (see Section 29.7.2 on page 498), and click either the Add icon or an Edit icon in the Recurring section.

Figure 338 Configuration > Object > Schedule > Edit (Recurring)



The Year, Month, and Day columns are not used in recurring schedules and are disabled in this screen. The following table describes the remaining labels in this screen.

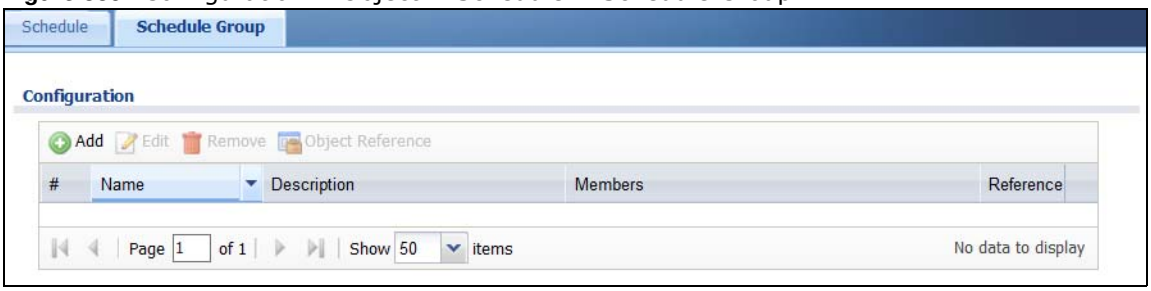
Table 209 Configuration > Object > Schedule > Edit (Recurring)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartTime	Specify the hour and minute when the schedule begins each day. • Hour - 0 - 23 • Minute - 0 - 59
StopTime	Specify the hour and minute when the schedule ends each day. • Hour - 0 - 23 • Minute - 0 - 59
Weekly	
Week Days	Select each day of the week the recurring schedule is effective.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.7.3 The Schedule Group Screen

The Schedule Group summary screen provides a summary of all groups of schedules in the USG. To access this screen, click Configuration > Object > Schedule > Group.

Figure 339 Configuration > Object > Schedule > Schedule Group



The following table describes the fields in the above screen.

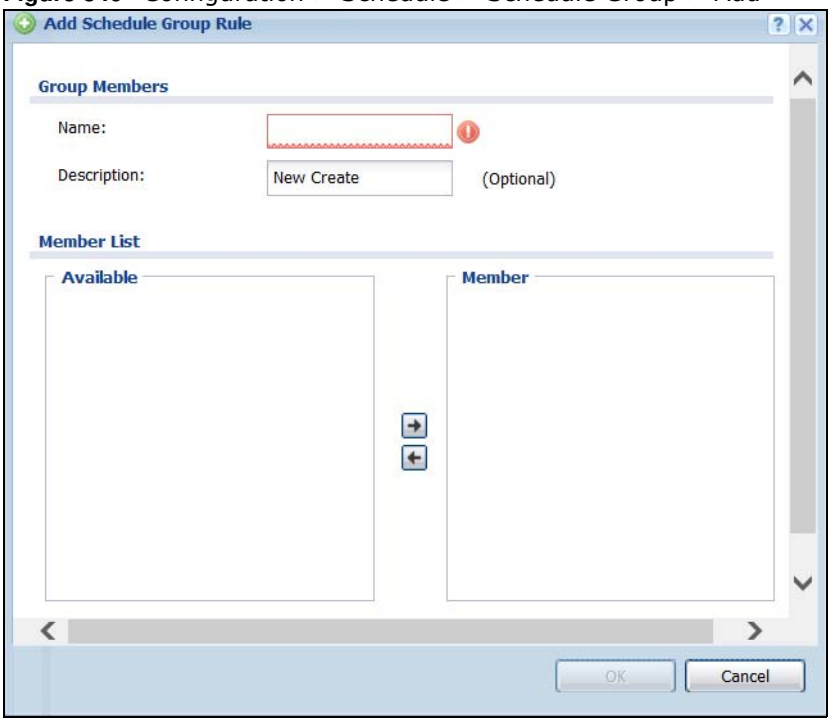
Table 210 Configuration > Object > Schedule > Schedule Group

LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule group, which is used to refer to the schedule.
Description	This field displays the decription of the schedule group.
Members	This field lists the members in the schedule group. Each member is separated by a comma.
Reference	This displays the number of times an object reference is used in a profile.

29.7.3.1 The Schedule Group Add/Edit Screen

The Schedule Group Add/ Edit screen allows you to define a schedule group or edit an existing one. To access this screen, go to the Schedule screen (see), and click either the Add icon or an Edit icon in the Schedule Group section.

Figure 340 Configuration > Schedule > Schedule Group > Add



The following table describes the fields in the above screen.

Table 211 Configuration > Schedule > Schedule Group > Add

LABEL	DESCRIPTION
Group Members	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.
Member List	The Member list displays the names of the service and service group objects that have been added to the service group. The order of members is not important. Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.8 AAA Server Overview

You can use a AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a Active Directory, LDAP, or RADIUS server. Use the AAA Server screens to create and manage objects that contain settings for using AAA servers. You use

AAA server objects in configuring ext-group-user user objects and authentication method objects (see Chapter 29 on page 511).

29.8.1 Directory Service (AD/LDAP)

LDAP/AD allows a client (the USG) to connect to a server to retrieve information from a directory. A network example is shown next.

Figure 341 Example: Directory Service Client and Server



The following describes the user authentication procedure via an LDAP/AD server.

1. A user logs in with a user name and password pair.
2. The USG tries to bind (or log in) to the LDAP/AD server.
3. When the binding process is successful, the USG checks the user information in the directory against the user name and password pair.
4. If it matches, the user is allowed access. Otherwise, access is blocked.

29.8.2 RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate a large number of users from a central location.

Figure 342 RADIUS Server Network Example



29.8.3 ASAS

ASAS (Authenex Strong Authentication System) is a RADIUS server that works with the One-Time Password (OTP) feature. Purchase a USG OTP package in order to use this feature. The package

contains server software and physical OTP tokens (PIN generators). Do the following to use OTP. See the documentation included on the ASAS' CD for details.

1 Install the ASAS server software on a computer.

2 Create user accounts on the USG and in the ASAS server.

3 Import each token's database file (located on the included CD) into the server.

4 Assign users to OTP tokens (on the ASAS server).

5 Configure the ASAS as a RADIUS server in the USG's Configuration > Object > AAA Server screens.

6 Give the OTP tokens to (local or remote) users.

- Use the Configuration > Object > AAA Server > Active Directory (or LDAP) screens (Section 29.8.5 on page 505) to configure Active Directory or LDAP server objects.
- Use the Configuration > Object > AAA Server > RADIUS screen (Section 29.8.2 on page 503) to configure the default external RADIUS server to use for user authentication.

29.8.4 What You Need To Know

AAA Servers Supported by the USG

The following lists the types of authentication server the USG supports.

- Local user database

  The USG uses the built-in local user database to authenticate administrative users logging into the USG's Web Configurator or network access users logging into the network through the USG. You can also use the local user database to authenticate VPN users.
- Directory Service (LDAP/AD)

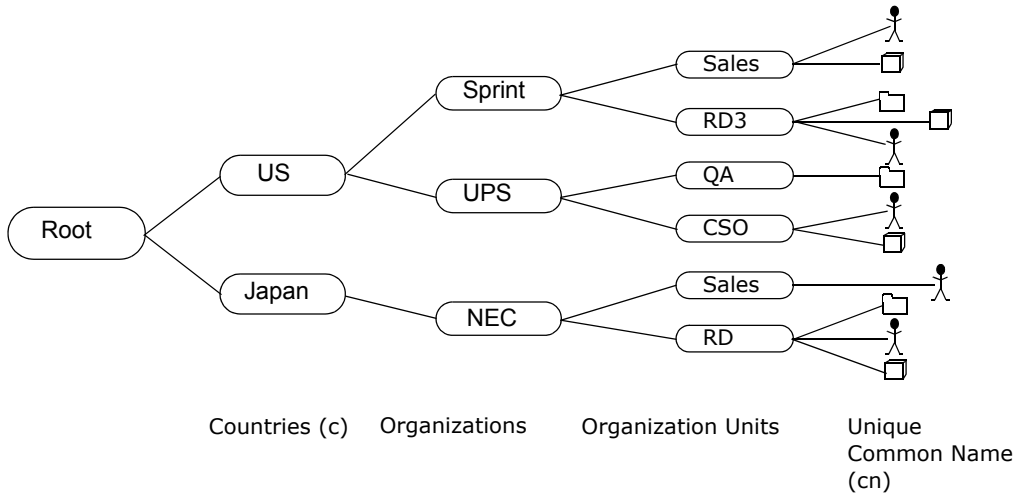
  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.
- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

Directory Structure

The directory entries are arranged in a hierarchical order much like a tree structure. Normally, the directory structure reflects the geographical or organizational boundaries. The following figure shows a basic directory structure branching from countries to organizations to organizational units to individuals.

Figure 343 Basic Directory Structure



Distinguished Name (DN)

A DN uniquely identifies an entry in a directory. A DN consists of attribute-value pairs separated by commas. The leftmost attribute is the Relative Distinguished Name (RDN). This provides a unique name for entries that have the same "parent DN" ("`cn=domain1.com`, `ou=Sales`, `o=MyCompany`" in the following examples).

```
cn=domain1.com, ou = Sales, o=MyCompany, c=US
cn=domain1.com, ou = Sales, o=MyCompany, c=JP
```

Base DN

A base DN specifies a directory. A base DN usually contains information such as the name of an organization, a domain name and/or country. For example, `o=MyCompany`, `c=UK` where `o` means organization and `c` means country.

Bind DN

A bind DN is used to authenticate with an LDAP/AD server. For example a bind DN of `cn=zywallAdmin` allows the USG to log into the LDAP/AD server using the user name of `zywallAdmin`. The bind DN is used in conjunction with a bind password. When a bind DN is not specified, the USG will try to log in as an anonymous user. If the bind password is incorrect, the login will fail.

29.8.5 Active Directory or LDAP Server Summary

Use the Active Directory or LDAP screen to manage the list of AD or LDAP servers the USG can use in authenticating users.

Click Configuration > Object > AAA Server > Active Directory (or LDAP) to display the Active Directory (or LDAP) screen.

Figure 344 Configuration > Object > AAA Server > Active Directory (or LDAP)



The following table describes the labels in this screen.

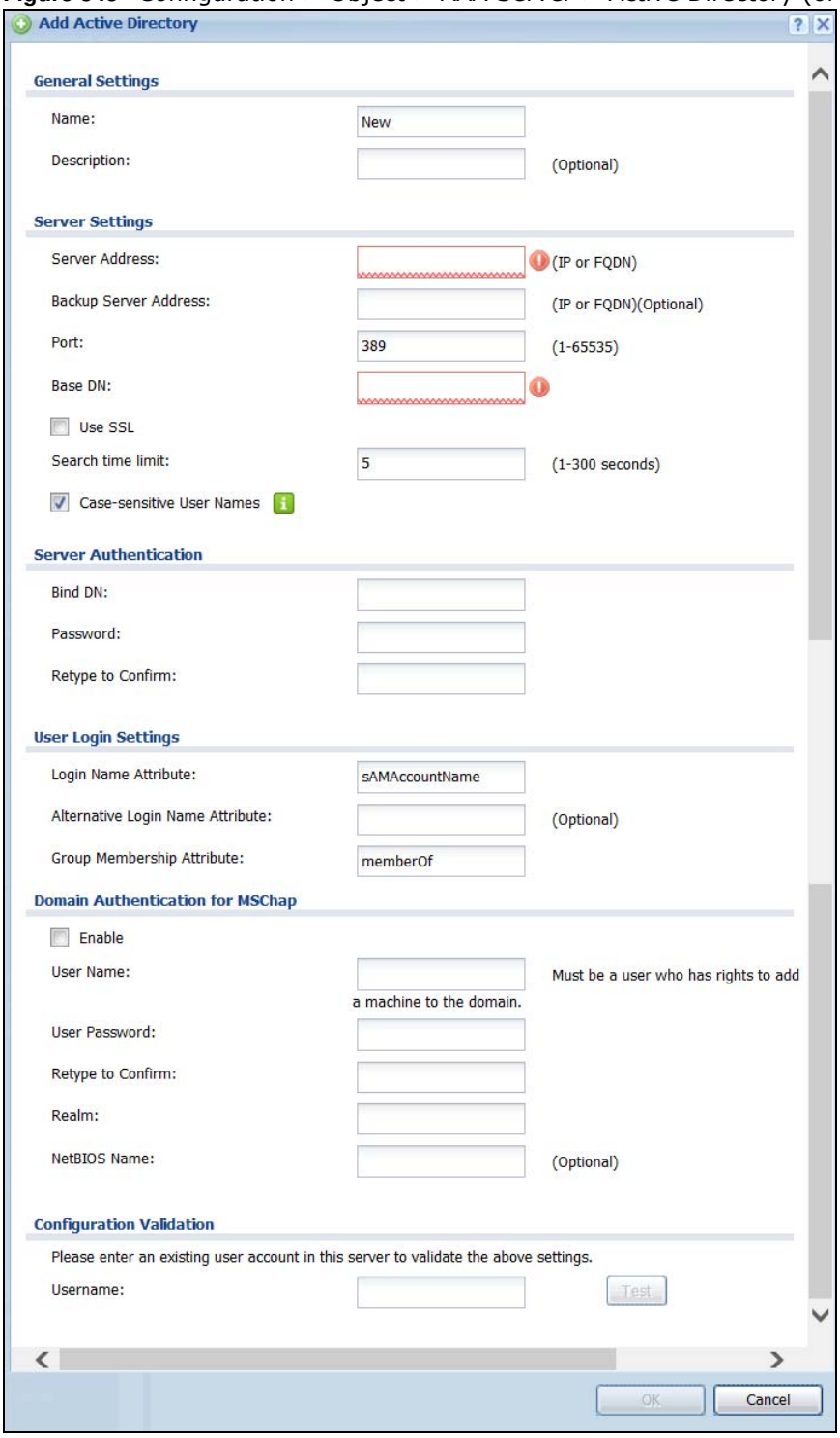
Table 212 Configuration > Object > AAA Server > Active Directory (or LDAP)

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific AD or LDAP server.
Name	This field displays the name of the Active Directory.
Server Address	This is the address of the AD or LDAP server.
Base DN	This specifies a directory. For example, o=ZyXEL, c=US.

29.8.5.1 Adding an Active Directory or LDAP Server

Click Object > AAA Server > Active Directory (or LDAP) to display the Active Directory (or LDAP) screen. Click the Add icon or an Edit icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 345 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add



The following table describes the labels in this screen.

Table 213 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server Address	Enter the address of the AD or LDAP server.
Backup Server Address	If the AD or LDAP server has a backup server, enter its address here.
Port	Specify the port number on the AD or LDAP server to which the USG sends authentication requests. Enter a number between 1 and 65535. This port number should be the same on all AD or LDAP server(s) in this group.
Base DN	Specify the directory (up to 127 alphanumerical characters). For example, o=ZyXEL, c=US. This is only for LDAP.
Use SSL	Select Use SSL to establish a secure connection to the AD or LDAP server(s).
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the USG disconnects from the AD or LDAP server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the AD or LDAP server(s) or the AD or LDAP server(s) is down.
Case-sensitive User Names	Select this if the server checks the case of the usernames.
Bind DN	Specify the bind DN for logging into the AD or LDAP server. Enter up to 127 alphanumerical characters. For example, cn=zywallAdmin specifies zywallAdmin as the user name.
Password	If required, enter the password (up to 15 alphanumerical characters) for the USG to bind (or log in) to the AD or LDAP server.
Retype to Confirm	Retype your new password for confirmation.
Login Name Attribute	Enter the type of identifier the users are to use to log in. For example "name" or "e-mail address".
Alternative Login Name Attribute	If there is a second type of identifier that the users can use to log in, enter it here. For example "name" or "e-mail address".
Group Membership Attribute	An AD or LDAP server defines attributes for its accounts. Enter the name of the attribute that the USG is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".
Domain Authentication for MSChap	Select the Enable checkbox to enable domain authentication for MSChap. This is only for Active Directory.
User Name	Enter the user name for the user who has rights to add a machine to the domain. This is only for Active Directory.
User Password	Enter the password for the associated user name. This is only for Active Directory.

Table 213 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add (continued)

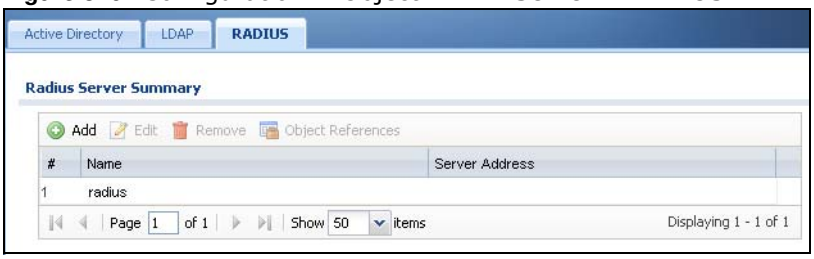
LABEL	DESCRIPTION
Retype to Confirm	Retype your new password for confirmation. This is only for Active Directory.
Realm	Enter the realm FQDN. This is only for Active Directory.
NetBIOS Name	Type the NetBIOS name. This field is optional. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN which allows local computers to find computers on the remote network and vice versa.
Configuration Validation	Use a user account from the server specified above to test if the configuration is correct. Enter the account's user name in the Username field and click Test.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

29.8.6 RADIUS Server Summary

Use the RADIUS screen to manage the list of RADIUS servers the USG can use in authenticating users.

Click Configuration > Object > AAA Server > RADIUS to display the RADIUS screen.

Figure 346 Configuration > Object > AAA Server > RADIUS



The following table describes the labels in this screen.

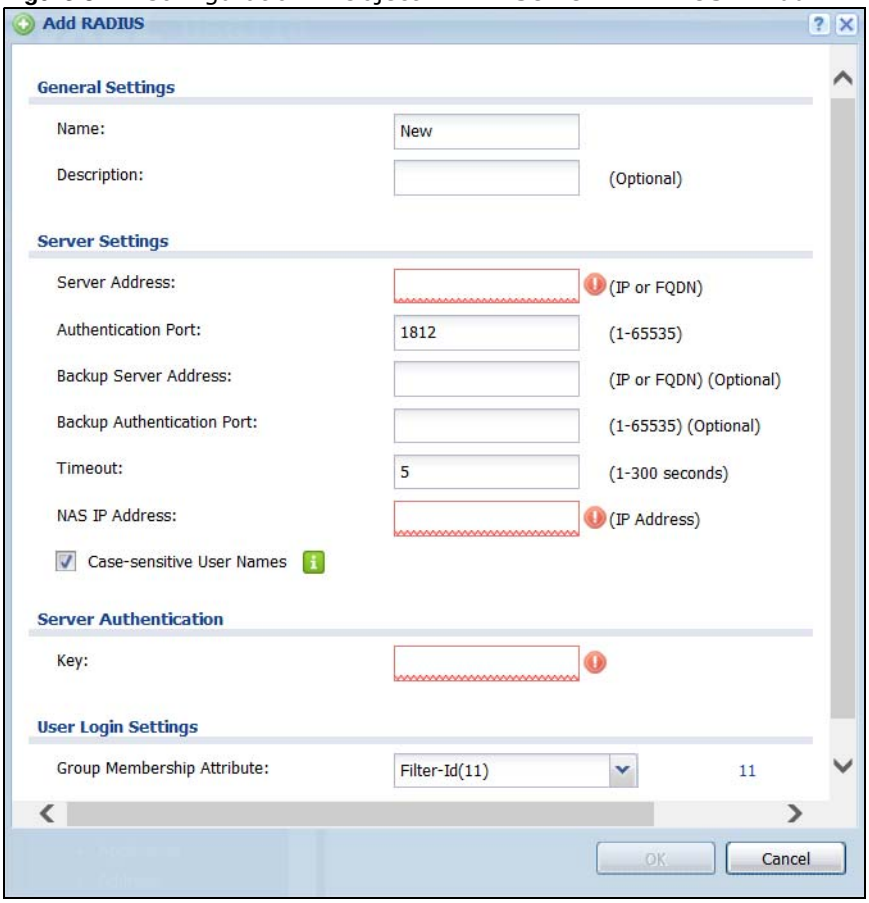
Table 214 Configuration > Object > AAA Server > RADIUS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field displays the index number.
Name	This is the name of the RADIUS server entry.
Server Address	This is the address of the AD or LDAP server.

29.8.6.1 Adding a RADIUS Server

Click Configuration > Object > AAA Server > RADIUS to display the RADIUS screen. Click the Add icon or an Edit icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 347 Configuration > Object > AAA Server > RADIUS > Add



The following table describes the labels in this screen.

Table 215 Configuration > Object > AAA Server > RADIUS > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server Address	Enter the address of the RADIUS server.
Authentication Port	Specify the port number on the RADIUS server to which the USG sends authentication requests. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup server, enter its address here.
Backup Authentication Port	Specify the port number on the RADIUS server to which the USG sends authentication requests. Enter a number between 1 and 65535.

Table 215 Configuration > Object > AAA Server > RADIUS > Add (continued)

LABEL	DESCRIPTION
Timeout	Specify the timeout period (between 1 and 300 seconds) before the USG disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
NAS IP Address	Type the IP address of the NAS (Network Access Server).
Case-sensitive User Names	Select this if you want configure your username as case-sensitive.
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the USG. The key is not sent over the network. This key must be the same on the external authentication server and the USG.
Group Membership Attribute	A RADIUS server defines attributes for its accounts. Select the name and number of the attribute that the USG is to check to determine to which group a user belongs. If it does not display, select user-defined and specify the attribute's number. This attribute's value is called a group identifier; it determines to which group a user belongs. You can add `ext-group-user` user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a `ext-group-user` user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

29.9 Auth. Method Overview

Authentication method objects set how the USG authenticates wireless, HTTP/HTTPS clients, and peer IPSec routers (extended authentication) clients. Configure authentication method objects to have the USG use the local user database, and/or the authentication servers and authentication server groups specified by AAA server objects. By default, user accounts created and stored on the USG are authenticated locally.

- Use the Configuration > Object > Auth. Method screens (Section 29.9.3 on page 512) to create and manage authentication method objects.

29.9.1 Before You Begin

Configure AAA server objects before you configure authentication method objects.

29.9.2 Example: Selecting a VPN Authentication Method

After you set up an authentication method object in the Auth. Method screens, you can use it in the VPN Gateway screen to authenticate VPN users for establishing a VPN connection. Refer to the chapter on VPN for more information.

Follow the steps below to specify the authentication method for a VPN connection.

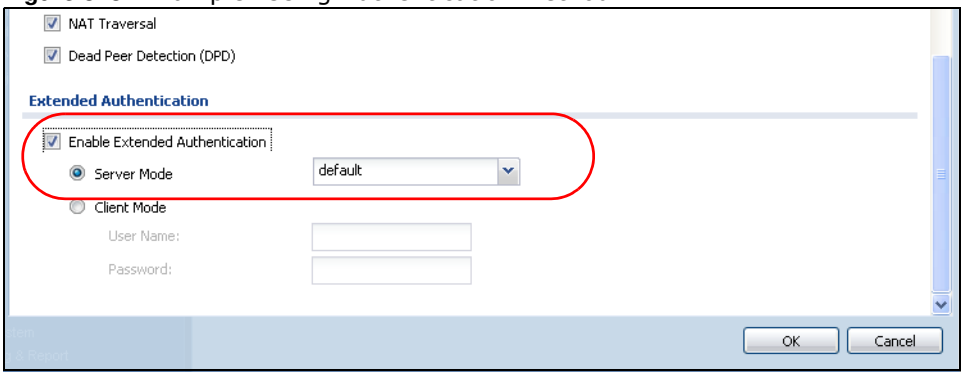
1 Access the Configuration > VPN > IPSec VPN > VPN Gateway > Edit screen.

2 Click Show Advance Setting and select Enable Extended Authentication.

3 Select Server Mode and select an authentication method object from the drop-down list box.

4 Click OK to save the settings.

Figure 348 Example: Using Authentication Method in VPN

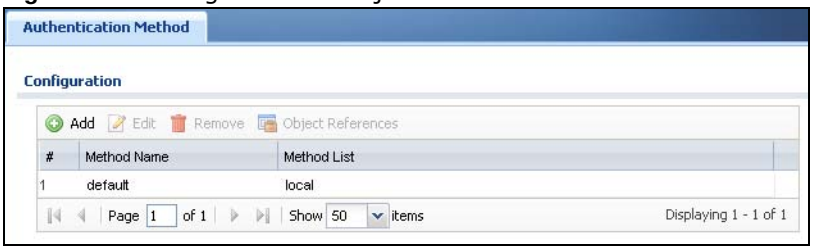


29.9.3 Authentication Method Objects

Click Configuration > Object > Auth. Method to display the screen as shown.

Note: You can create up to 16 authentication method objects.

Figure 349 Configuration > Object > Auth. Method



The following table describes the labels in this screen.

Table 216 Configuration > Object > Auth. Method

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field displays the index number.
Method Name	This field displays a descriptive name for identification purposes.
Method List	This field displays the authentication method(s) for this entry.

29.9.3.1 Creating an Authentication Method Object

Follow the steps below to create an authentication method object.

1 Click Configuration > Object > Auth. Method.

2 Click Add.

3 Specify a descriptive name for identification purposes in the Name field. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".

4 Click Add to insert an authentication method in the table.

5 Select a server object from the Method List drop-down list box.

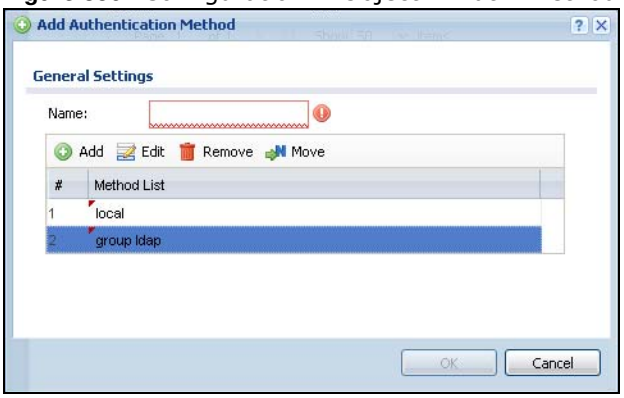
6 You can add up to four server objects to the table. The ordering of the Method List column is important. The USG authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

If two accounts with the same username exist on two authentication servers you specify, the USG does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.

Note: You can NOT select two server objects of the same type.

7 Click OK to save the settings or click Cancel to discard all changes and return to the previous screen.

Figure 350 Configuration > Object > Auth. Method > Add



The following table describes the labels in this screen.

Table 217 Configuration > Object > Auth. Method > Add

LABEL	DESCRIPTION
Name	Specify a descriptive name for identification purposes. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.

Table 217 Configuration > Object > Auth. Method > Add (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Move	To change a method's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed. The ordering of your methods is important as USG authenticates the users using the authentication methods in the order they appear in this screen.
#	This field displays the index number.
Method List	Select a server object from the drop-down list box. You can create a server object in the AAA Server screen. The USG authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen. If two accounts with the same username exist on two authentication servers you specify, the USG does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

29.10 Certificate Overview

The USG can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

- Use the My Certificates screens (see Section 29.10.3 on page 517 to Section 29.10.3.3 on page 523) to generate and export self-signed certificates or certification requests and import the CA-signed certificates.
- Use the Trusted Certificates screens (see Section 29.10.4 on page 524 to Section 29.10.4.2 on page 528) to save CA certificates and trusted remote host certificates to the USG. The USG trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

29.10.1 What You Need to Know

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

1. Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
2. Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
3. Tim uses his private key to sign the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).
5. Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The USG uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The USG does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The USG can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The USG only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Self-signed Certificates

You can have the USG act as a certification authority and sign its own certificates.

Factory Default Certificate

The USG generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The USG currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the USG.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

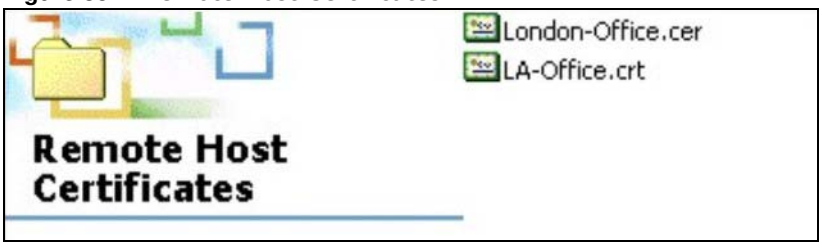
29.10.2 Verifying a Certificate

Before you import a trusted certificate into the USG, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

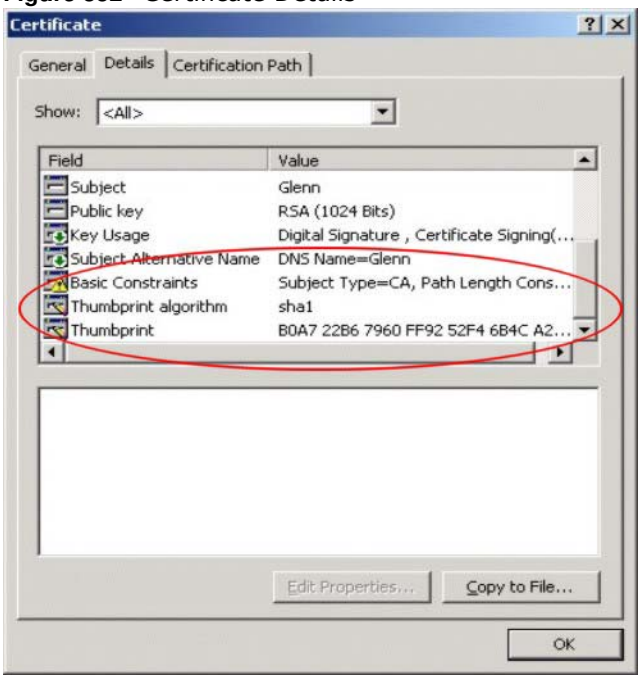
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 351 Remote Host Certificates



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

Figure 352 Certificate Details

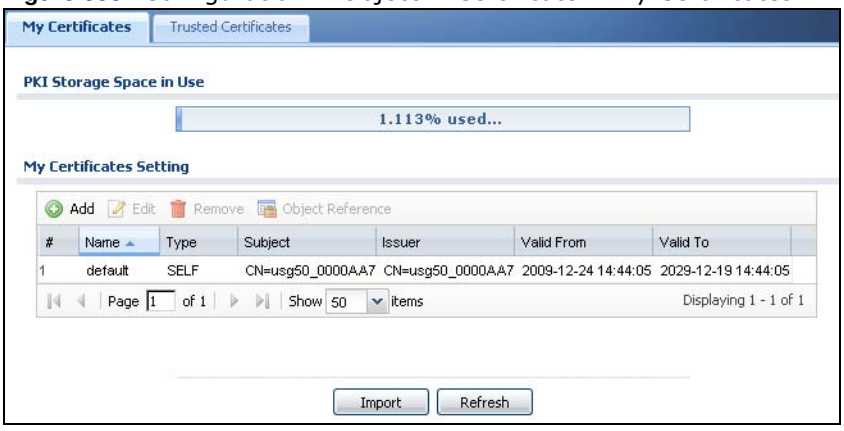


4 Use a secure method to verify that the certificate owner has the same information in the Thumbprint Algorithm and Thumbprint fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

29.10.3 The My Certificates Screen

Click Configuration > Object > Certificate > My Certificates to open the My Certificates screen. This is the USG's summary list of certificates and certification requests.

Figure 353 Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

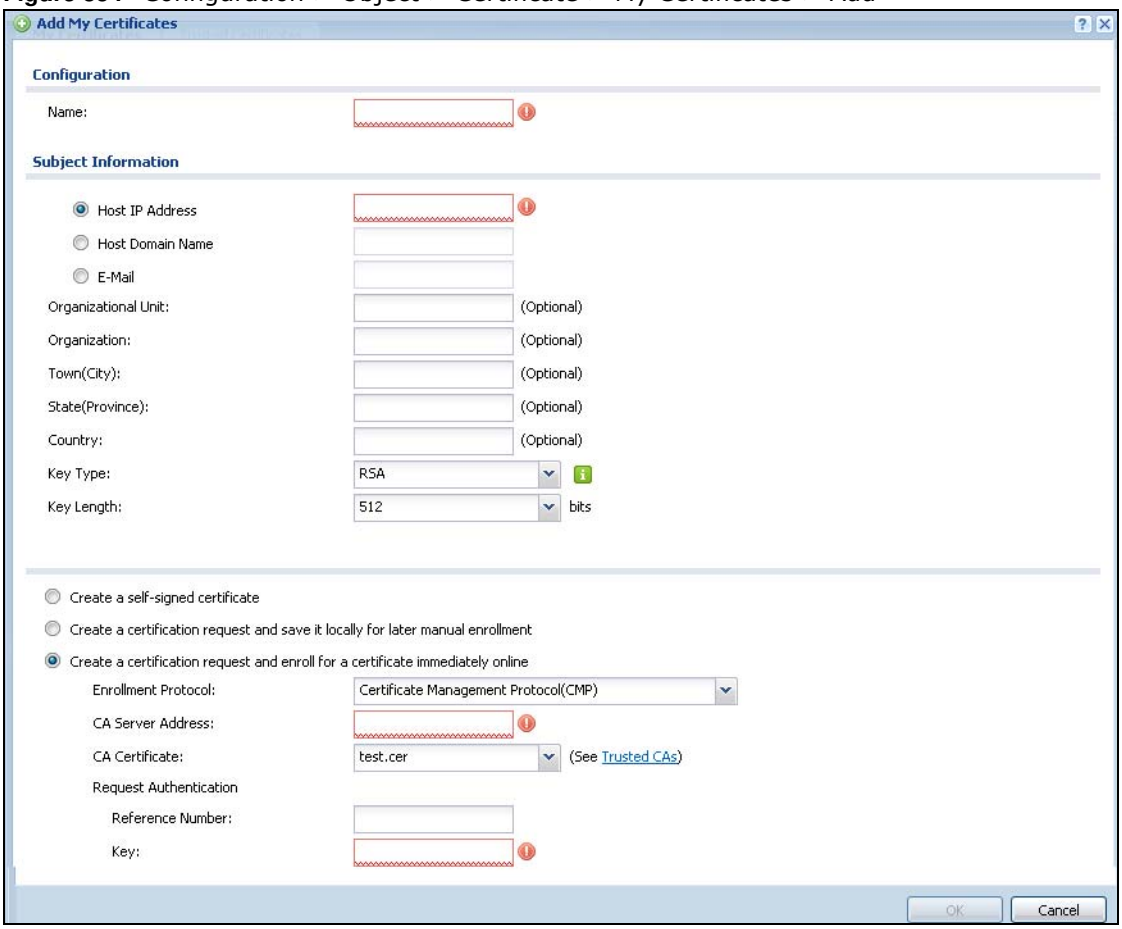
Table 218 Configuration > Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the USG's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Add	Click this to go to the screen where you can have the USG generate a certificate or a certification request.
Edit	Double-click an entry or select it and click Edit to open a screen with an in-depth list of information about the certificate.
Remove	The USG keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object References	You cannot delete certificates that any of the USG's features are configured to use. Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request. SELF represents a self-signed certificate. CERT represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click Import to open a screen where you can save a certificate to the USG.
Refresh	Click Refresh to display the current validity status of the certificates.

29.10.3.1 The My Certificates Add Screen

Click Configuration > Object > Certificate > My Certificates and then the Add icon to open the My Certificates Add screen. Use this screen to have the USG create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 354 Configuration > Object > Certificate > My Certificates > Add



The following table describes the labels in this screen.

Table 219 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a Host IP Address, Host IPv6 Address, Host Domain Name, or E-Mail. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string. A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.

Table 219 Configuration > Object > Certificate > My Certificates > Add (continued)

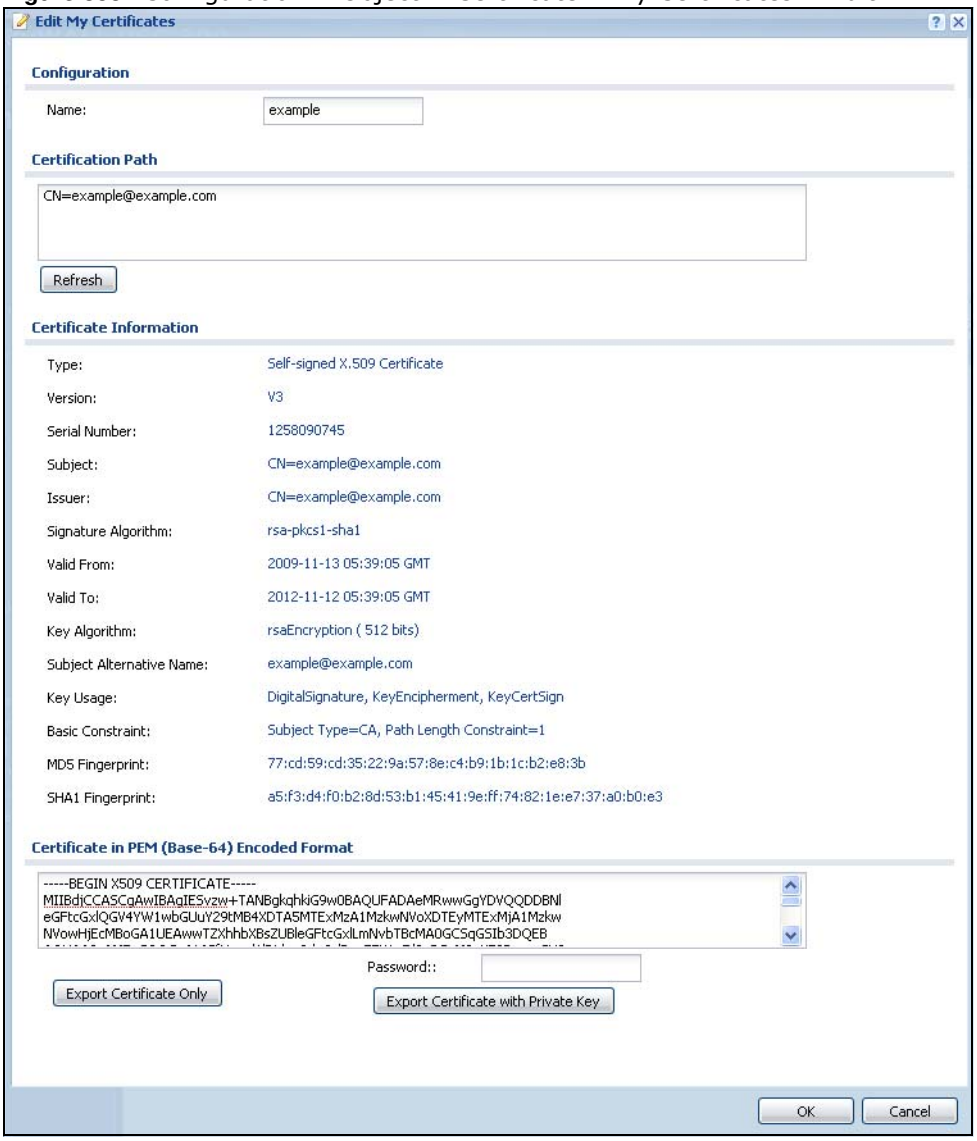
LABEL	DESCRIPTION
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
State, (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	Select RSA to use the Rivest, Shamir and Adleman public-key algorithm. Select DSA to use the Digital Signature Algorithm public-key algorithm.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Extended Key Usage	
Server Authentication	Select this to have USG generate and store a request for server authentication certificate.
Client Authentication	Select this to have USG generate and store a request for client authentication certificate.
IKE Intermediate	Select this to have USG generate and store a request for IKE Intermediate authentication certificate.
Create a self-signed certificate	Select this to have the USG generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the USG generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the My Certificate Details screen (see Section 29.10.3.2 on page 521) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select this to have the USG generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the Trusted Certificates screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the Reference Number and Key if the certification authority requires them.
OK	Click OK to begin certificate or certification request generation.
Cancel	Click Cancel to quit and return to the My Certificates screen.

If you configured the My Certificate Create screen to have the USG enroll a certificate and the certificate enrollment is not successful, you see a screen with a Return button that takes you back to the My Certificate Create screen. Click Return and check your information in the My Certificate Create screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the USG to enroll a certificate online.

29.10.3.2 The My Certificates Edit Screen

Click Configuration > Object > Certificate > My Certificates and then the Edit icon to open the My Certificate Edit screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 355 Configuration > Object > Certificate > My Certificates > Edit



The following table describes the labels in this screen.

Table 220 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	This field displays for a certificate, not a certification request. Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The USG does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the USG.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the Subject Name field. "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The USG uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the USG uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.

Table 220 Configuration > Object > Certificate > My Certificates > Edit (continued)

LABEL	DESCRIPTION
MD5 Fingerprint	This is the certificate's message digest that the USG calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the USG calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save.
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save.
OK	Click OK to save your changes back to the USG. You can only change the name.
Cancel	Click Cancel to quit and return to the My Certificates screen.

29.10.3.3 The My Certificates Import Screen

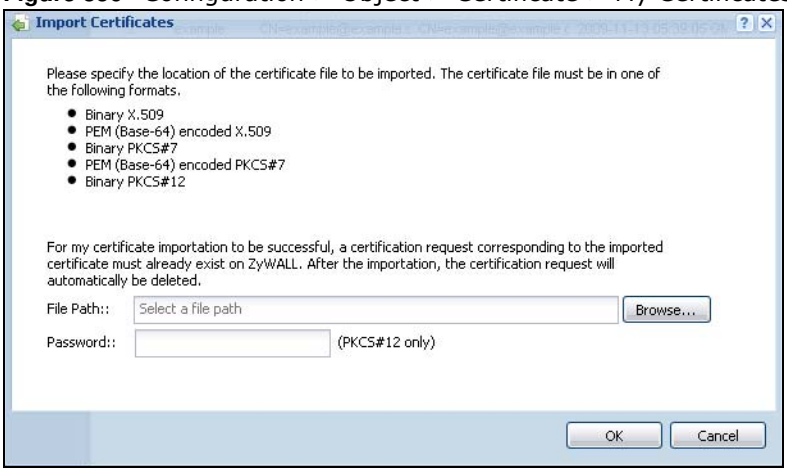
Click Configuration > Object > Certificate > My Certificates > Import to open the My Certificate Import screen. Follow the instructions in this screen to save an existing certificate to the USG.

Note: You can import a certificate that matches a corresponding certification request that was generated by the USG. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

The certificate you import replaces the corresponding request in the My Certificates screen.

You must remove any spaces from the certificate's filename before you can import it.

Figure 356 Configuration > Object > Certificate > My Certificates > Import



The following table describes the labels in this screen.

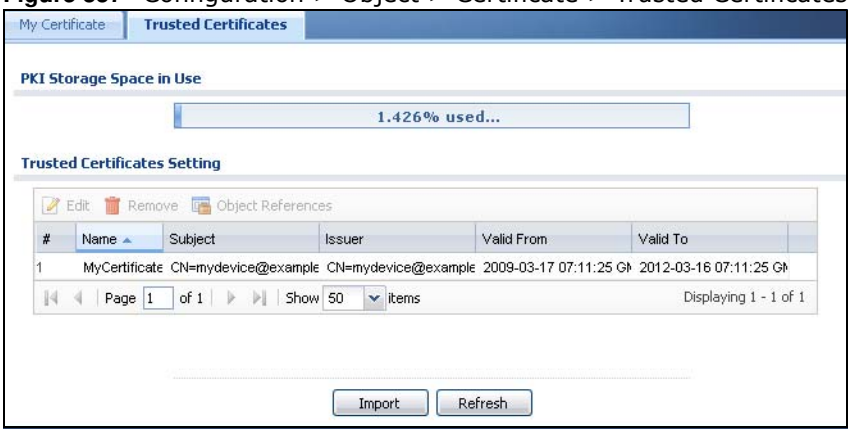
Table 221 Configuration > Object > Certificate > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the USG.
Browse	Click Browse to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click OK to save the certificate on the USG.
Cancel	Click Cancel to quit and return to the My Certificates screen.

29.10.4 The Trusted Certificates Screen

Click Configuration > Object > Certificate > Trusted Certificates to open the Trusted Certificates screen. This screen displays a summary list of certificates that you have set the USG to accept as trusted. The USG also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

Figure 357 Configuration > Object > Certificate > Trusted Certificates



The following table describes the labels in this screen.

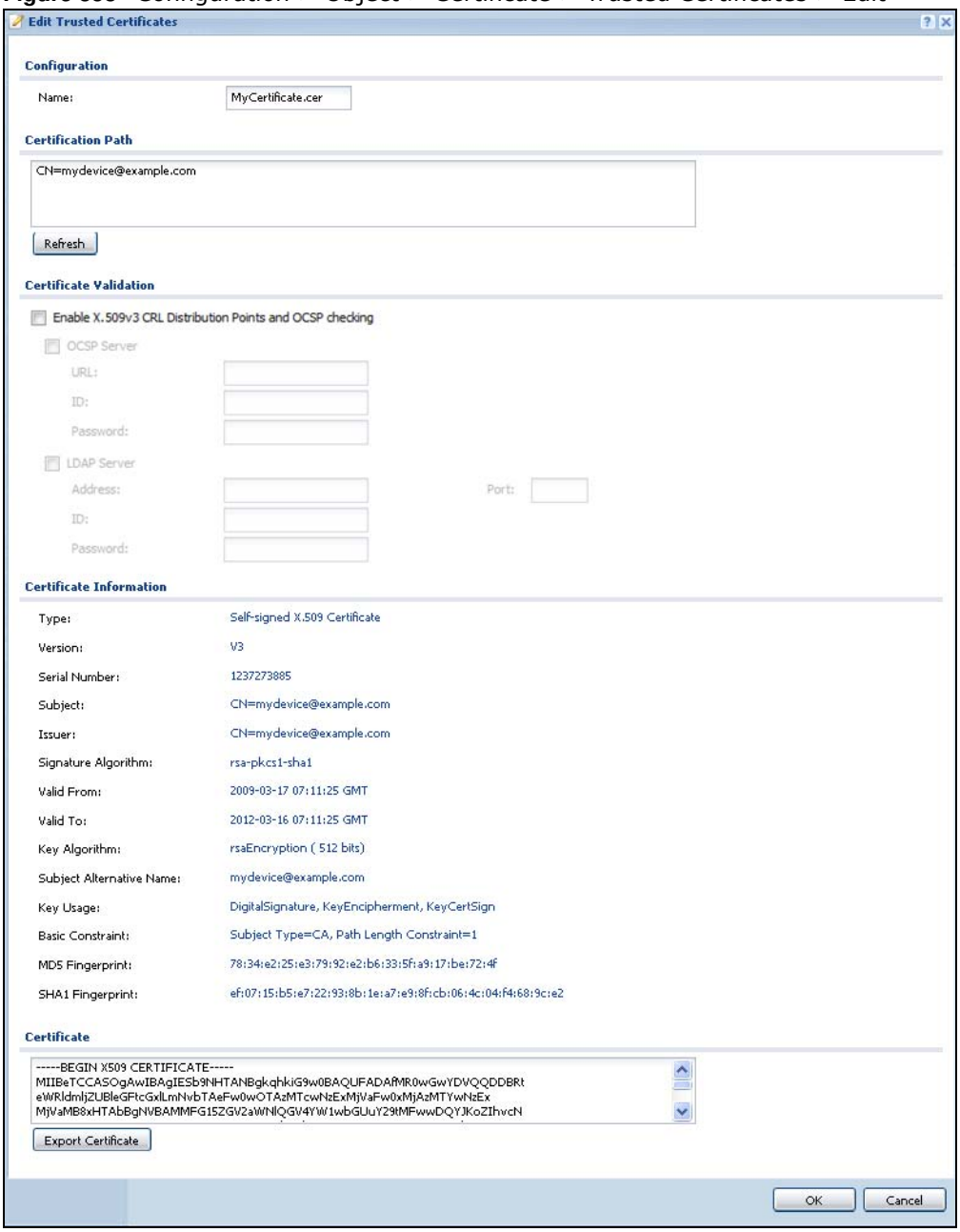
Table 222 Configuration > Object > Certificate > Trusted Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the USG's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click Edit to open a screen with an in-depth list of information about the certificate.
Remove	The USG keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object References	You cannot delete certificates that any of the USG's features are configured to use. Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click Import to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the USG.
Refresh	Click this button to display the current validity status of the certificates.

29.10.4.1 The Trusted Certificates Edit Screen

Click Configuration > Object > Certificate > Trusted Certificates and then a certificate's Edit icon to open the Trusted Certificates Edit screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the USG to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 358 Configuration > Object > Certificate > Trusted Certificates > Edit



The following table describes the labels in this screen.

Table 223 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	Click the Refresh button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The USG does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this check box to turn on/off certificate revocation. When it is turned on, the USG validates a certificate by getting Certificate Revocation List (CRL) through HTTP or LDAP (can be configured after selecting the LDAP Server check box) and online responder (can be configured after selecting the OCSP Server check box).
OCSP Server	Select this check box if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and path name of the OCSP server.
ID	The USG may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The USG may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

Table 223 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

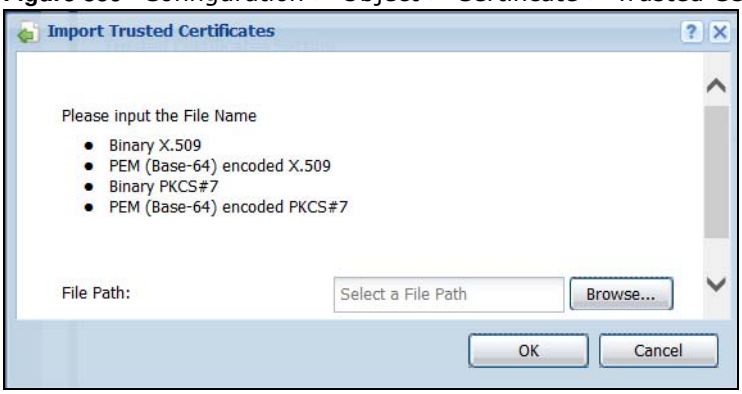
LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the USG uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the USG calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the USG calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save.
OK	Click OK to save your changes back to the USG. You can only change the name.
Cancel	Click Cancel to quit and return to the Trusted Certificates screen.

29.10.4.2 The Trusted Certificates Import Screen

Click Configuration > Object > Certificate > Trusted Certificates > Import to open the Trusted Certificates Import screen. Follow the instructions in this screen to save a trusted certificate to the USG.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 359 Configuration > Object > Certificate > Trusted Certificates > Import



The following table describes the labels in this screen.

Table 224 Configuration > Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the USG.
Browse	Click Browse to find the certificate file you want to upload.
OK	Click OK to save the certificate on the USG.
Cancel	Click Cancel to quit and return to the previous screen.

29.10.5 Certificates Technical Reference

OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the USG checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the USG only gets information on the certificates that it needs to verify, not a huge list. When the USG requests certificate status information, the OCSP server returns a "expired", "current" or "unknown" response.

29.11 ISP Account Overview

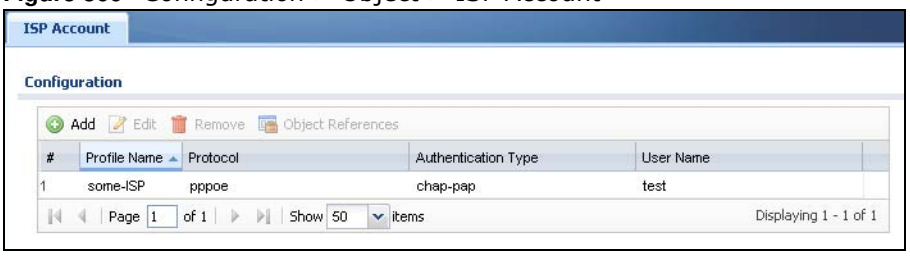
Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE/PPTP interfaces. An ISP account is a profile of settings for Internet access using PPPoE or PPTP.

Use the Object > ISP Account screens (Section 29.11.1 on page 529) to create and manage ISP accounts in the USG.

29.11.1 ISP Account Summary

This screen provides a summary of ISP accounts in the USG. To access this screen, click Configuration > Object > ISP Account.

Figure 360 Configuration > Object > ISP Account



The following table describes the labels in this screen. See the ISP Account Edit section below for more information as well.

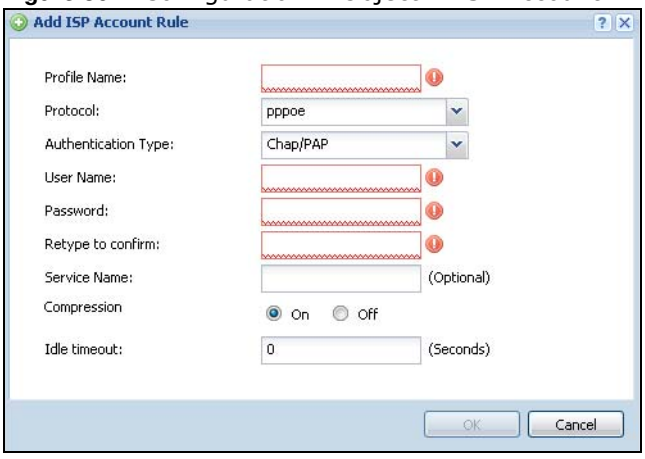
Table 225 Configuration > Object > ISP Account

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific entry.
Profile Name	This field displays the profile name of the ISP account. This name is used to identify the ISP account.
Protocol	This field displays the protocol used by the ISP account.
Authentication Type	This field displays the authentication type used by the ISP account.
User Name	This field displays the user name of the ISP account.

29.11.1.1 ISP Account Edit

The ISP Account Edit screen lets you add information about new accounts and edit information about existing accounts. To open this window, open the ISP Account screen. (See Section 29.11.1 on page 529.) Then, click on an Add icon or Edit icon to open the ISP Account Edit screen below.

Figure 361 Configuration > Object > ISP Account > Edit



The following table describes the labels in this screen.

Table 226 Configuration > Object > ISP Account > Edit

LABEL	DESCRIPTION
Profile Name	This field is read-only if you are editing an existing account. Type in the profile name of the ISP account. The profile name is used to refer to the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Protocol	This field is read-only if you are editing an existing account. Select the protocol used by the ISP account. Options are: pppoe - This ISP account uses the PPPoE protocol. pptp - This ISP account uses the PPTP protocol.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: CHAP/PAP - Your USG accepts either CHAP or PAP when requested by this remote node. Chap - Your USG accepts CHAP only. PAP - Your USG accepts PAP only. MSCHAP - Your USG accepts MSCHAP only. MSCHAP-V2 - Your USG accepts MSCHAP-V2 only.
Encryption Method	This field is available if this ISP account uses the PPTP protocol. Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: nomppe - This ISP account does not use MPPE. mppe-40 - This ISP account uses 40-bit MPPE. mppe-128 - This ISP account uses 128-bit MMPE.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above. The password can only consist of alphanumeric characters (A-Z, a-z, 0-9). This field can be blank.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Server IP	If this ISP account uses the PPPoE protocol, this field is not displayed. If this ISP account uses the PPTP protocol, type the IP address of the PPTP server.
Connection ID	This field is available if this ISP account uses the PPTP protocol. Type your identification name for the PPTP server. This field can be blank.
Service Name	If this ISP account uses the PPPoE protocol, type the PPPoE service name to access. PPPoE uses the specified service name to identify and reach the PPPoE server. This field can be blank. If this ISP account uses the PPTP protocol, this field is not displayed.
Compression	Select On button to turn on stac compression, and select Off to turn off stac compression. Stac compression is a data compression technique capable of compressing data by a factor of about four.
Idle Timeout	This value specifies the number of seconds that must elapse without outbound traffic before the USG automatically disconnects from the PPPoE/PPTP server. This value must be an integer between 0 and 360. If this value is zero, this timeout is disabled.
OK	Click OK to save your changes back to the USG. If there are no errors, the program returns to the ISP Account screen. If there are errors, a message box explains the error, and the program stays in the ISP Account Edit screen.
Cancel	Click Cancel to return to the ISP Account screen without creating the profile (if it is new) or saving any changes to the profile (if it already exists).

29.12 SSL Application Overview

You use SSL application objects in SSL VPN. Configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access. You can apply one or more SSL application objects in the VPN > SSL VPN screen for a user account/user group.

- Use the SSL Application screen (Section 29.12.2 on page 534) to view the USG's configured SSL application objects.
- Use the SSL Application Edit screen to create or edit web-based application objects to allow remote users to access an application via standard web browsers (Section 29.12.2.1 on page 534).
- You can also use the SSL Application Edit screen to specify the name of a folder on a Linux or Windows file server which remote users can access using a standard web browser (Section 29.12.2.1 on page 534).

29.12.1 What You Need to Know

Application Types

You can configure the following SSL application on the USG.

- Web-based

  A web-based application allows remote users to access an intranet site using standard web browsers.

Remote User Screen Links

Available SSL application names are displayed as links in remote user screens. Depending on the application type, remote users can simply click the links or follow the steps in the pop-up dialog box to access.

Remote Desktop Connections

Use SSL VPN to allow remote users to manage LAN computers. Depending on the functions supported by the remote desktop software, they can install or remove software, run programs, change settings, and open, copy, create, and delete files. This is useful for troubleshooting, support, administration, and remote access to files and programs.

The LAN computer to be managed must have VNC (Virtual Network Computing) or RDP (Remote Desktop Protocol) server software installed. The remote user's computer does not use VNC or RDP client software. The USG works with the following remote desktop connection software:

RDP

- Windows Remote Desktop (supported in Internet Explorer)

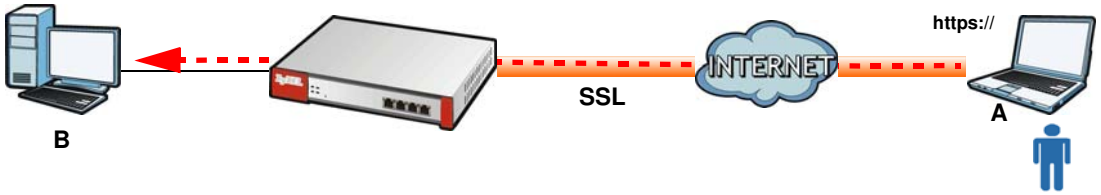
VNC

- RealVNC
- TightVNC

- UltraVNC

For example, user A uses an SSL VPN connection to log into the USG. Then he manages LAN computer B which has RealVNC server software installed.

Figure 362 SSL-protected Remote Management



Weblinks

You can configure weblink SSL applications to allow remote users to access web sites.

29.12.1.1 Example: Specifying a Web Site for Access

This example shows you how to create a web-based application for an internal web site. The address of the web site is http://info with web page encryption.

1 Click Configuration > Object > SSL Application in the navigation panel.

2 Click the Add button and select Web Application in the Type field.

In the Server Type field, select Web Server.

Enter a descriptive name in the Display Name field. For example, "CompanyIntranet".

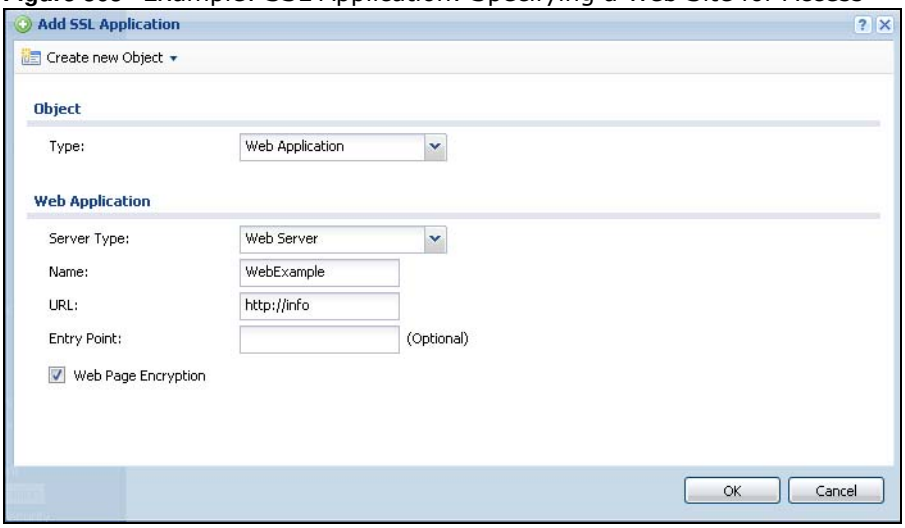
In the URLAddress field, enter "http://my-info".

Select Web Page Encryption to prevent users from saving the web content.

Click OK to save the settings.

The configuration screen should look similar to the following figure.

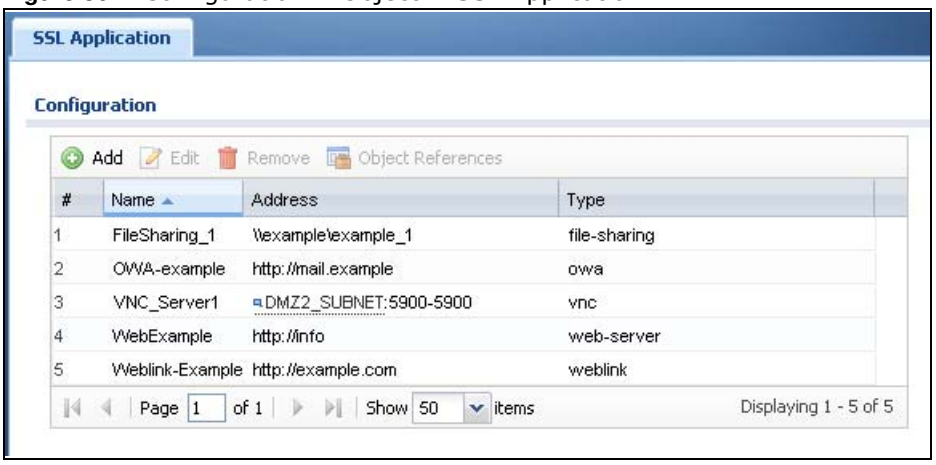
Figure 363 Example: SSL Application: Specifying a Web Site for Access



29.12.2 The SSL Application Screen

The main SSL Application screen displays a list of the configured SSL application objects. Click Configuration > Object > SSL Application in the navigation panel.

Figure 364 Configuration > Object > SSL Application



The following table describes the labels in this screen.

Table 227 Configuration > Object > SSL Application

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field displays the index number.
Name	This field displays the name of the object.
Address	This field displays the IP address/URL of the application server or the location of a file share.
Type	This field shows whether the object is a file-sharing, web-server, Outlook Web Access, Virtual Network Computing, or Remote Desktop Protocol SSL application.

29.12.2.1 Creating/Editing an SSL Application Object

You can create a web-based application that allows remote users to access an application via standard web browsers. You can also create a file sharing application that specify the name of a folder on a file server (Linux or Windows) which remote users can access. Remote users can access files using a standard web browser and files are displayed as links on the screen.

To configure an SSL application, click the Add or Edit button in the SSL Application screen and select Web Application or File Sharing in the Type field. The screen differs depending on what object type you choose.

Note: If you are creating a file sharing SSL application, you must also configure the shared folder on the file server for remote access. Refer to the document that comes with your file server.

Figure 365 Configuration > Object > SSL Application > Add/Edit: Web Application

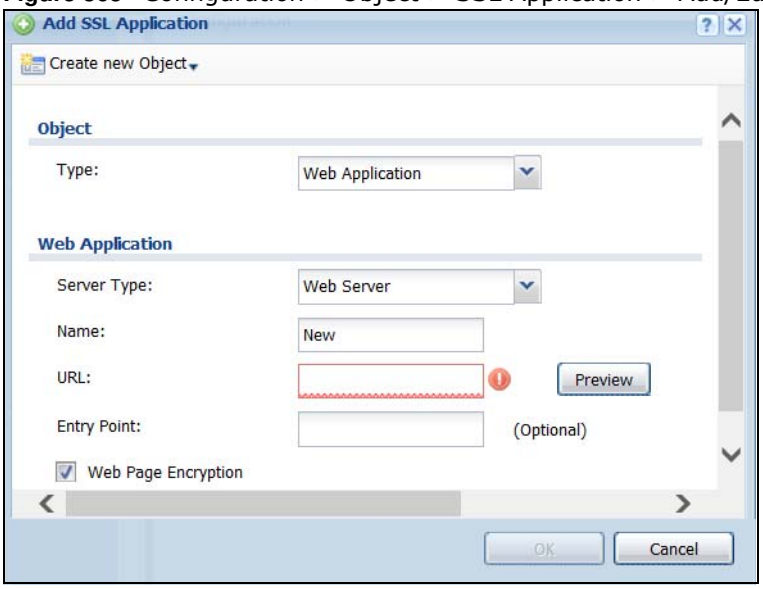
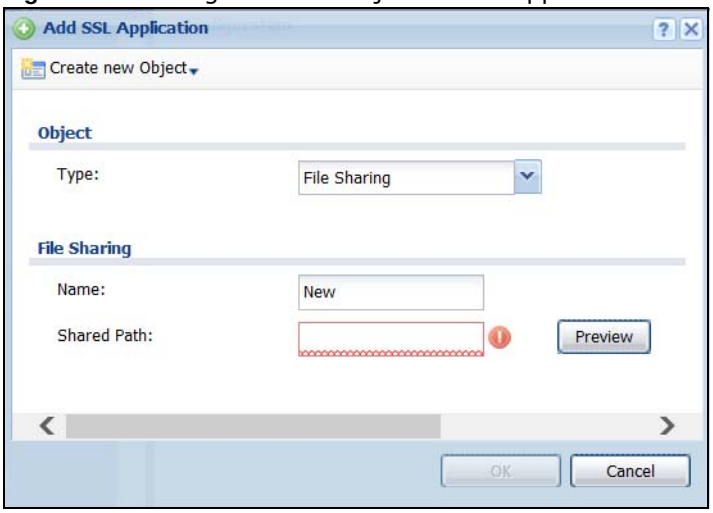


Figure 366 Configuration > Object > SSL Application > Add/Edit: File Sharing



The following table describes the labels in this screen.

Table 228 Configuration > Object > SSL Application > Add/Edit: Web Application/File Sharing

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Object	
Type	Select Web Application or File Sharing from the drop-down list box.
Web Application	

Table 228 Configuration > Object > SSL Application > Add/Edit: Web Application/File Sharing

LABEL	DESCRIPTION
Server Type	This field only appears when you choose Web Application as the object type. Specify the type of service for this SSL application. Select Web Server to allow access to the specified web site hosted on the local network. Select OWA (Outlook Web Access) to allow users to access e-mails, contacts, calenders via Microsoft Outlook-like interface using supported web browsers. The USG supports one OWA object. Select VNC to allow users to manage LAN computers that have Virtual Network Computing remote desktop server software installed. Select RDP to allow users to manage LAN computers that have Remote Desktop Protocol remote desktop server software installed. Select Weblink to create a link to a web site that you expect the SSL VPN users to commonly use.
Name	Enter a descriptive name to identify this object. You can enter up to 31 characters ("0-9", "a-z", "A-Z", "-" and "_"). Spaces are not allowed.
URL	This field only appears when you choose Web Application as the object type. This field displays if the Server Type is set to Web Server, OWA, or Weblink. Enter the Fully-Qualified Domain Name (FQDN) or IP address of the application server. Note: You must enter the "http://" or "https://" prefix. Remote users are restricted to access only files in this directory. For example, if you enter "\remote\" in this field, remote users can only access files in the "remote" directory. If a link contains a file that is not within this domain, then remote users cannot access it.
Preview	This field only appears when you choose Web Application or File Sharing as the object type. This field displays if the Server Type is set to Web Server, OWA or Weblink. Note: If your Internet Explorer or other browser screen doesn't show a preview, it may be due to your web browser security settings. You need to add the USG's IP address in the trusted sites of your web browser. For example, in Internet Explorer, click Tools > Internet Options > Security > Trusted Sites > Sites and type the USG's IP address, then click Add. For other web browsers, please check the browser help. Click Preview to access the URL you specified in a new web browser screen.
Entry Point	This field only appears when you choose Web Application as the object type. This field displays if the Server Type is set to Web Server or OWA. This field is optional. You only need to configure this field if you need to specify the name of the directory or file on the local server as the home page or home directory on the user screen.
Web Page Encryption	This field only appears when you choose Web Application as the object type. Select this option to prevent users from saving the web content.

Table 228 Configuration > Object > SSL Application > Add/Edit: Web Application/File Sharing

LABEL	DESCRIPTION
Shared Path	This field only appears when you choose File Sharing as the object type. Specify the IP address, domain name or NetBIOS name (computer name) of the file server and the name of the share to which you want to allow user access. Enter the path in one of the following formats. "\\<IP address>\<share name>" "\\<domain name>\<share name>" "\\<computer name>\<share name>" For example, if you enter "\\my-server\Tmp", this allows remote users to access all files and/or folders in the "\Tmp" share on the "my-server" computer.
OK	Click OK to save the changes and return to the main SSL Application Configuration screen.
Cancel	Click Cancel to discard the changes and return to the main SSL Application Configuration screen.

30

System

30.1 Overview

Use the system screens to configure general USG settings.

30.1.1 What You Can Do in this Chapter

- Use the System > Host Name screen (see Section 30.2 on page 539) to configure a unique name for the USG in your network.
- Use the System > USB Storage screen (see Section 30.3 on page 539) to configure the settings for the connected USB devices.
- Use the System > Date/Time screen (see Section 30.4 on page 540) to configure the date and time for the USG.
- Use the System > Console Speed screen (see Section 30.5 on page 544) to configure the console port speed when you connect to the USG via the console port using a terminal emulation program.
- Use the System > DNS screen (see Section 30.6 on page 545) to configure the DNS (Domain Name System) server used for mapping a domain name to its corresponding IP address and vice versa.
- Use the System > WWW screens (see Section 30.7 on page 554) to configure settings for HTTP or HTTPS access to the USG and how the login and access user screens look.
- Use the System > SSH screen (see Section 30.8 on page 570) to configure SSH (Secure SHell) used to securely access the USG's command line interface. You can specify which zones allow SSH access and from which IP address the access can come.
- Use the System > TELNET screen (see Section 30.9 on page 574) to configure Telnet to access the USG's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.
- Use the System > FTP screen (see Section 30.10 on page 576) to specify from which zones FTP can be used to access the USG. You can also specify from which IP addresses the access can come. You can upload and download the USG's firmware and configuration files using FTP. .
- Your USG can act as an SNMP agent, which allows a manager station to manage and monitor the USG through the network. Use the System > SNMP screen (see Section 30.11 on page 577) to configure SNMP settings, including from which zones SNMP can be used to access the USG. You can also specify from which IP addresses the access can come.
- Use the Auth. Server screen (Section 30.12 on page 581) to configure the USG to operate as a RADIUS server.
- Use the CloudCNM screen (Section 30.13 on page 583) to enable and configure management of the USG by a Central Network Management system.
- Use the System > Language screen (see Section 30.14 on page 586) to set a language for the USG's Web Configurator screens.
- Use the System > IPv6 screen (see Section 30.15 on page 586) to enable or disable IPv6 support on the USG.

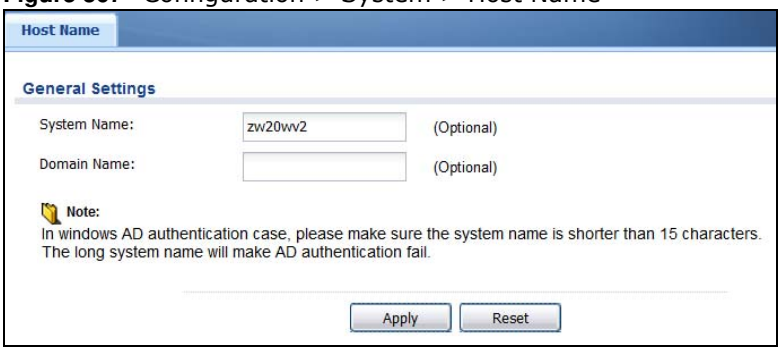
- Use the System > ZON screen (see Section 30.16 on page 587) to enable or disable the ZyXEL One Network (ZON) utility that uses ZyXEL Discovery Protocol (ZDP) for discovering and configuring ZDP-aware ZyXEL devices in the same network as the computer on which ZON is installed.

Note: See each section for related background information and term definitions.

30.2 Host Name

A host name is the unique name by which a device is known on a network. Click Configuration > System > Host Name to open the Host Name screen.

Figure 367 Configuration > System > Host Name



The following table describes the labels in this screen.

Table 229 Configuration > System > Host Name

LABEL	DESCRIPTION
System Name	Enter a descriptive name to identify your USG device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

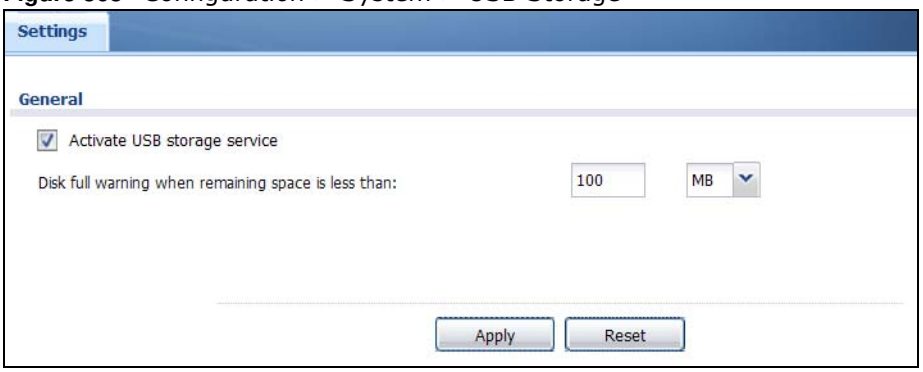
30.3 USB Storage

The USG can use a connected USB device to store the system log and other diagnostic information. Use this screen to turn on this feature and set a disk full warning limit.

Note: Only connect one USB device. It must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system.

Click Configuration > System > USB Storage to open the screen as shown next.

Figure 368 Configuration > System > USB Storage



The following table describes the labels in this screen.

Table 230 Configuration > System > USB Storage

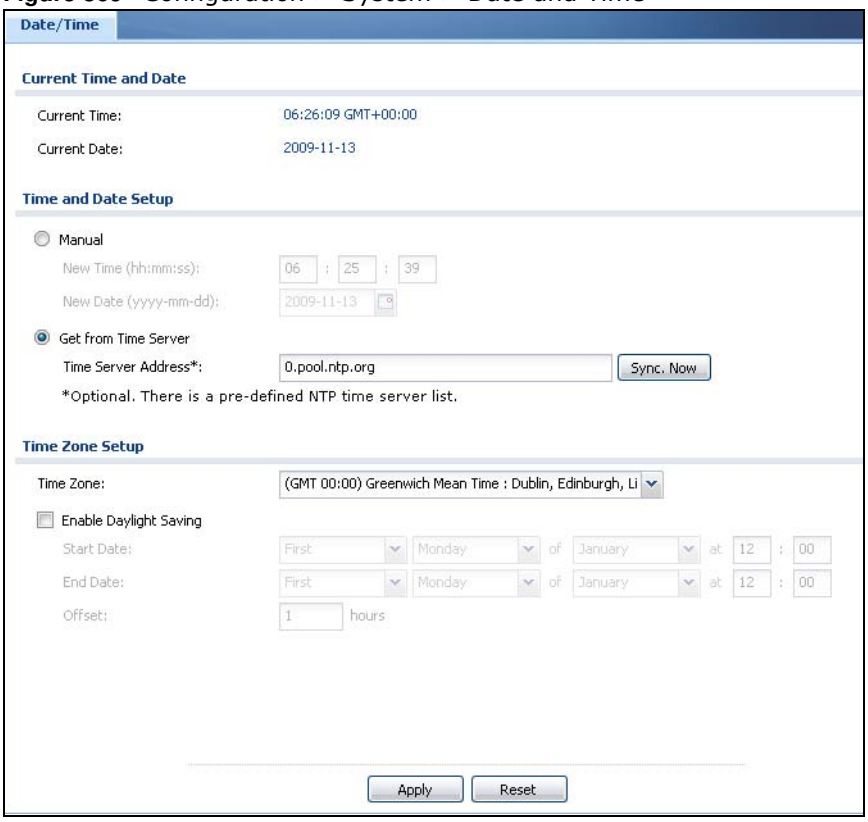
LABEL	DESCRIPTION
Activate USB storage service	Select this if you want to use the connected USB device(s).
Disk full warning when remaining space is less than	Set a number and select a unit (MB or %) to have the USG send a warning message when the remaining USB storage space is less than the value you set here.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

30.4 Date and Time

For effective scheduling and logging, the USG system time must be accurate. The USG's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

To change your USG's time based on your local time zone and date, click Configuration > System > Date/ Time. The screen displays as shown. You can manually set the USG's time and date or have the USG get the date and time from a time server.

Figure 369 Configuration > System > Date and Time



The following table describes the labels in this screen.

Table 231 Configuration > System > Date and Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your USG.
Current Date	This field displays the present date of your USG.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the USG uses the new setting once you click Apply.
New Time (hh-mm-ss)	This field displays the last updated time from the time server or the last time configured manually. When you set Time and Date Setup to Manual, enter the new time in this field and then click Apply.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set Time and Date Setup to Manual, enter the new date in this field and then click Apply.

Table 231 Configuration > System > Date and Time (continued)

LABEL	DESCRIPTION
Get from Time Server	Select this radio button to have the USG get the time and date from the time server you specify below. The USG requests time and date settings from the time server under the following circumstances. • When the USG starts up. • When you click Apply or Synchronize Now in this screen. • 24-hour intervals after starting up.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the USG get the time and date from a time server (see the Time Server Address field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Enable Daylight Saving. The at field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and type 2 in the at field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March. The time you type in the at field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected Enable Daylight Saving. The at field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and type 2 in the at field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October. The time you type in the at field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Offset	Specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments). For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

30.4.1 Pre-defined NTP Time Servers List

When you turn on the USG for the first time, the date and time start at 2003-01-01 00:00:00. The USG then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The USG continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 232 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

When the USG uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the USG goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

30.4.2 Time Server Synchronization

Click the Synchronize Now button to get the time and date from the time server you specified in the Time Server Address field.

When the Please Wait... screen appears, you may have to wait up to one minute.

Figure 370 Synchronization in Process



The Current Time and Current Date fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the View Log screen. Try re-configuring the Date/Time screen.

To manually set the USG date and time.

1. Click System > Date/Time.
2. Select Manual under Time and Date Setup.
3. Enter the USG's time in the New Time field.
4. Enter the USG's date in the New Date field.
5. Under Time Zone Setup, select your Time Zone from the list.
6. As an option you can select the Enable Daylight Saving check box to adjust the USG clock for daylight savings.

7 Click Apply.

To get the USG date and time from a time server

1 Click System > Date/ Time.

2 Select Get from Time Server under Time and Date Setup.

3 Under Time Zone Setup, select your Time Zone from the list.

4 As an option you can select the Enable Daylight Saving check box to adjust the USG clock for daylight savings.

5 Under Time and Date Setup, enter a Time Server Address (Table 232 on page 543).

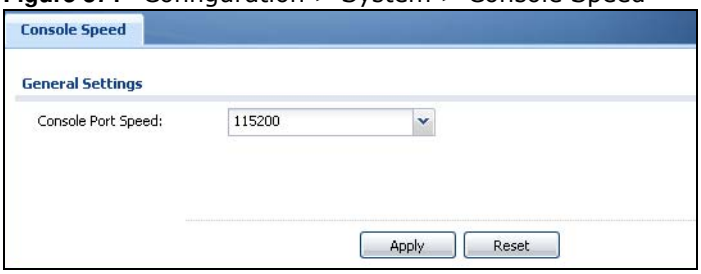
6 Click Apply.

30.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the USG via the console port using a terminal emulation program.

Click Configuration > System > Console Speed to open the Console Speed screen.

Figure 371 Configuration > System > Console Speed



The following table describes the labels in this screen.

Table 233 Configuration > System > Console Speed

LABEL	DESCRIPTION
Console Port Speed	Use the drop-down list box to change the speed of the console port. Your USG supports 9600, 19200, 38400, 57600, and 115200 bps (default) for the console port. The Console Port Speed applies to a console port connection using terminal emulation software and NOT the Console in the USG Web Configurator Status screen.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

30.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

30.6.1 DNS Server Address Assignment

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

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- If your ISP dynamically assigns the DNS server IP addresses (along with the USG's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- You can manually enter the IP addresses of other DNS servers.

30.6.2 Configuring the DNS Screen

Click Configuration > System > DNS to change your USG's DNS settings. Use the DNS screen to configure the USG to use a DNS server to resolve domain names for USG system features like VPN, DDNS and the time server. You can also configure the USG to accept or discard DNS queries. Use the Network > Interface screens to configure the DNS server information that the USG sends to the specified DHCP client devices.

A name query begins at a client computer and is passed to a resolver, a DNS client service, for resolution. The USG can be a DNS client service. The USG can resolve a DNS query locally using cached Resource Records (RR) obtained from a previous query (and kept for a period of time). If the USG does not have the requested information, it can forward the request to DNS servers. This is known as recursion.

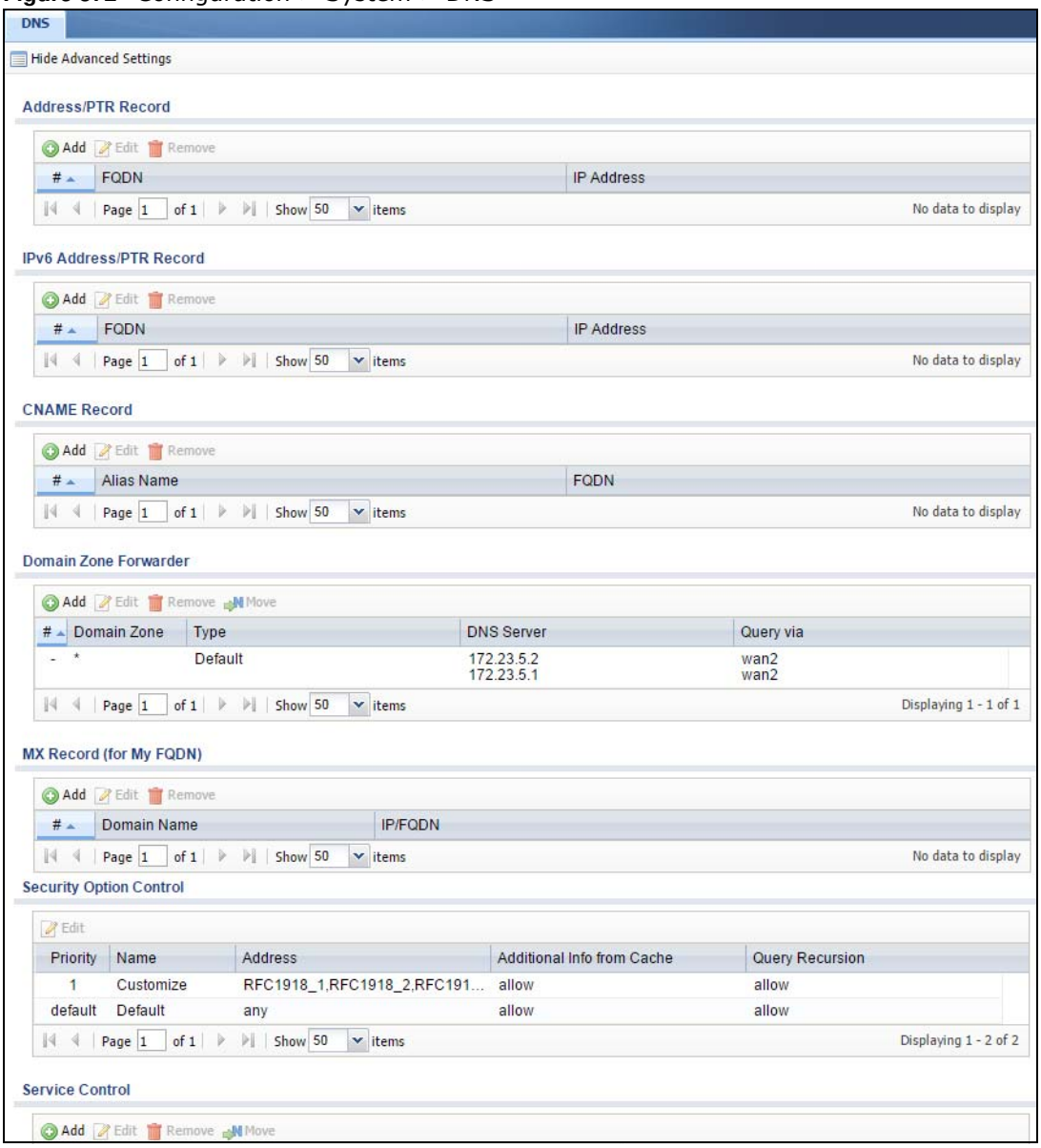
The USG can ask a DNS server to use recursion to resolve its DNS client requests. If recursion on the USG or a DNS server is disabled, they cannot forward DNS requests for resolution.

A Domain Name Server (DNS) amplification attack is a kind of Distributed Denial of Service (DDoS) attack that uses publicly accessible open DNS servers to flood a victim with DNS response traffic. An open DNS server is a DNS server which is willing to resolve recursive DNS queries from anyone on the Internet.

In a DNS amplification attack, an attacker sends a DNS name lookup request to an open DNS server with the source address spoofed as the victim's address. When the DNS server sends the DNS record response, it is sent to the victim. Attackers can request as much information as possible to maximize the amplification effect.

Configure the Security Option Control section in the Configuration > System > DNS screen (click Show Advanced Settings to display it) if you suspect the USG is being used (either by hackers or by a corrupted open DNS server) in a DNS amplification attack.

Figure 372 Configuration > System > DNS



The following table describes the labels in this screen.

Table 234 Configuration > System > DNS

LABEL	DESCRIPTION
Address/PTR Record	This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the address/PTR record.
FQDN	This is a host's fully qualified domain name.

Table 234 Configuration > System > DNS (continued)

LABEL	DESCRIPTION
IP Address	This is the IP address of a host.
CNAME Record	This record specifies an alias for a FQDN. Use this record to bind all subdomains with the same IP address as the FQDN without having to update each one individually, which increases chance for errors. See CNAME Record (Section 30.6.6 on page 549) for more details.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence. A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The USG uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.
Alias Name	Enter an Alias name. Use "*." as prefix for a wildcard domain name. For example, *.example.com.
FQDN	Enter the Fully Qualified Domain Name (FQDN).
Domain Zone Forwarder	This specifies a DNS server's IP address. The USG can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the USG needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence. A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The USG uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. A "*" means all domain zones.
Type	This displays whether the DNS server IP address is assigned by the ISP dynamically through a specified interface or configured manually (User-Defined).
DNS Server	This is the IP address of a DNS server. This field displays N/A if you have the USG get a DNS server IP address from the ISP dynamically but the specified interface is not active.
Query Via	This is the interface through which the USG sends DNS queries to the entry's DNS server. If the USG connects through a VPN tunnel, tunnel displays.
MX Record (for My FQDN)	A MX (Mail eXchange) record identifies a mail server that handles the mail for a particular domain.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.

Table 234 Configuration > System > DNS (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the MX record.
Domain Name	This is the domain name where the mail is destined for.
IP/FQDN	This is the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
Security Option Control	Click Show Advanced Settings to display this part of the screen. There are two control policies: Default and Customize.
Edit	Click either control policy and then click this button to change allow or deny actions for Query Recursion and Additional Info from Cache.
Priority	The Customize control policy is checked first and if an address object match is not found, the Default control policy is checked.
Name	You may change the name of the Customize control policy.
Address	These are the object addresses used in the control policy. RFC1918 refers to private IP address ranges. It can be modified in Object > Address.
Additional Info from Cache	This displays if the USG is allowed or denied to cache Resource Records (RR) obtained from previous DNS queries.
Query Recursion	This displays if the USG is allowed or denied to forward DNS client requests to DNS servers for resolution.
Service Control	This specifies from which computers and zones you can send DNS queries to the USG.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The ordering of your rules is important as rules are applied in sequence. The entry with a hyphen (-) instead of a number is the USG's (non-configurable) default policy. The USG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the USG will not have to use the default policy.
Zone	This is the zone on the USG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to send DNS queries.
Action	This displays whether the USG accepts DNS queries from the computer with the IP address specified above through the specified zone (Accept) or discards them (Deny).

30.6.3 Address Record

An address record contains the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com" is the top level domain. mail.myZyXEL.com.tw is also a FQDN, where "mail" is the host, "myZyXEL" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain.

The USG allows you to configure address records about the USG itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the USG receives a DNS query for an FQDN for which the USG has an address record, the USG can send the IP address in a DNS response without having to query a DNS name server.

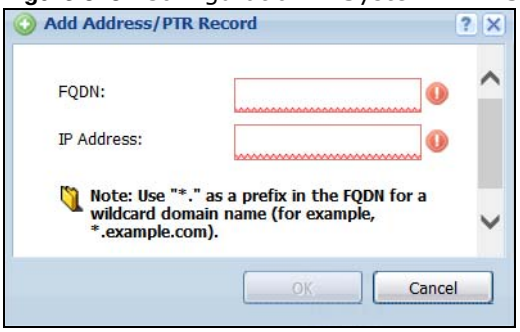
30.6.4 PTR Record

A PTR (pointer) record is also called a reverse record or a reverse lookup record. It is a mapping of an IP address to a domain name.

30.6.5 Adding an Address/PTR Record

Click the Add icon in the Address/ PTR Record table to add an address/PTR record.

Figure 373 Configuration > System > DNS > Address/PTR Record Edit



The following table describes the labels in this screen.

Table 235 Configuration > System > DNS > Address/PTR Record Edit

LABEL	DESCRIPTION
FQDN	Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
IP Address	Enter the IP address of the host in dotted decimal notation.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

30.6.6 CNAME Record

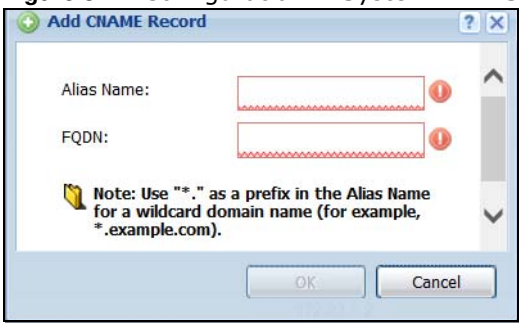
A Canonical Name Record or CNAME record is a type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name. This allows users to set up a record for a domain name which translates to an IP address, in other words, the domain name is an alias of another. This record also binds all the subdomains to the same IP address without having to create a record for each, so when the IP address is changed, all subdomain's IP address is updated as well, with one edit to the record.

For example, the domain name zyxel.com is hooked up to a record named A which translates it to 11.22.33.44. You also have several subdomains, like mail.zyxel.com, ftp.zyxel.com and you want this subdomain to point to your main domain zyxel.com. Edit the IP Address in record A and all subdomains will follow automatically. This eliminates chances for errors and increases efficiency in DNS management.

30.6.7 Adding a CNAME Record

Click the Add icon in the CNAME Record table to add a record. Use "*." as a prefix for a wildcard domain name. For example *.zyxel.com.

Figure 374 Configuration > System > DNS > CNAME Record > Add



The following table describes the labels in this screen.

Table 236 Configuration > System > DNS > CNAME Record > Add

LABEL	DESCRIPTION
Alias name	Enter an Alias Name. Use "*." as a prefix in the Alias name for a wildcard domain name (for example, *.example.com).
FQDN	Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

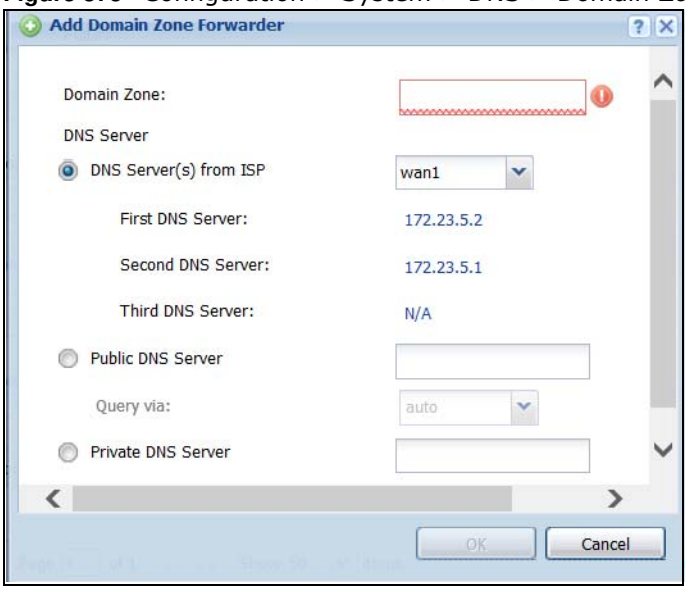
30.6.8 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The USG can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

30.6.9 Adding a Domain Zone Forwarder

Click the Add icon in the Domain Zone Forwarder table to add a domain zone forwarder record.

Figure 375 Configuration > System > DNS > Domain Zone Forwarder Add



The following table describes the labels in this screen.

Table 237 Configuration > System > DNS > Domain Zone Forwarder Add

LABEL	DESCRIPTION
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the USG receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. Enter * if all domain zones are served by the specified DNS server(s).
DNS Server	Select DNS Server(s) from ISP if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set to be a DHCP client. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. N/A displays for any DNS server IP address fields for which the ISP does not assign an IP address. Select Public DNS Server if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. The USG must be able to connect to the DNS server without using a VPN tunnel. The DNS server could be on the Internet or one of the USG's local networks. You cannot use 0.0.0.0. Use the Query via field to select the interface through which the USG sends DNS queries to a DNS server. Select Private DNS Server if you have the IP address of a DNS server to which the USG connects through a VPN tunnel. Enter the DNS server's IP address in the field to the right. You cannot use 0.0.0.0.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

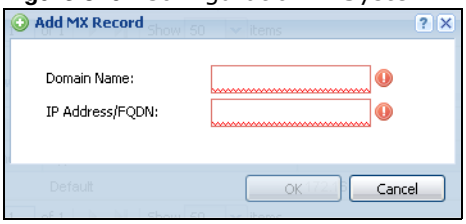
30.6.10 MX Record

A MX (Mail eXchange) record indicates which host is responsible for the mail for a particular domain, that is, controls where mail is sent for that domain. If you do not configure proper MX records for your domain or other domain, external e-mail from other mail servers will not be able to be delivered to your mail server and vice versa. Each host or domain can have only one MX record, that is, one domain is mapping to one host.

30.6.11 Adding a MX Record

Click the Add icon in the MX Record table to add a MX record.

Figure 376 Configuration > System > DNS > MX Record Add



The following table describes the labels in this screen.

Table 238 Configuration > System > DNS > MX Record Add

LABEL	DESCRIPTION
Domain Name	Enter the domain name where the mail is destined for.
IP Address/FQDN	Enter the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

30.6.12 Security Option Control

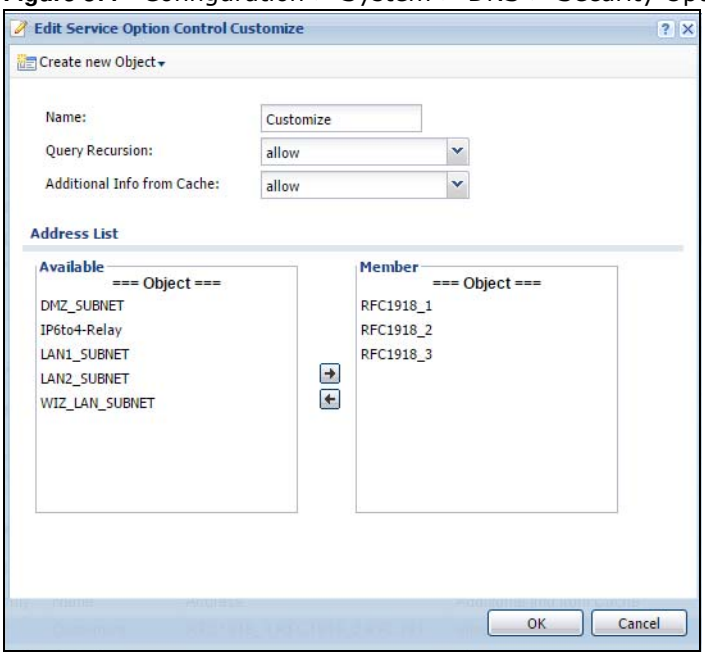
Configure the Security Option Control section in the Configuration > System > DNS screen (click Show Advanced Settings to display it) if you suspect the USG is being used by hackers in a DNS amplification attack.

One possible strategy would be to deny Query Recursion and Additional Info from Cache in the default policy and allow Query Recursion and Additional Info from Cache only from trusted DNS servers identified by address objects and added as members in the customized policy.

30.6.13 Editing a Security Option Control

Click a control policy and then click Edit to change allow or deny actions for Query Recursion and Additional Info from Cache.

Figure 377 Configuration > System > DNS > Security Option Control Edit (Customize)



The following table describes the labels in this screen.

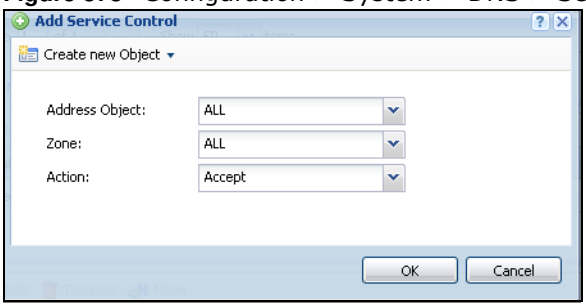
Table 239 Configuration > System > DNS > Security Option Control Edit (Customize)

LABEL	DESCRIPTION
Name	You may change the name for the customized security option control policy. The customized security option control policy is checked first and if an address object match is not found, the Default control policy is checked
Query Recursion	Choose if the USG is allowed or denied to forward DNS client requests to DNS servers for resolution. This can apply to specific open DNS servers using the address objects in a customized rule.
Additional Info from Cache	Choose if the USG is allowed or denied to cache Resource Records (RR) obtained from previous DNS queries.
Address List	Specifiying address objects is not available in the default policy as all addresses are included.
Available	This box displays address objects created in Object > Address. Select one (or more), and click the > arrow to have it (them) join the Member list of address objects that will apply to this rule. For example, you could specifiy an open DNS server suspect of sending compromised resource records by adding an address object for that server to the member list.
Member	This box displays address objects that will apply to this rule.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

30.6.14 Adding a DNS Service Control Rule

Click the Add icon in the Service Control table to add a service control rule.

Figure 378 Configuration > System > DNS > Service Control Rule Add



The following table describes the labels in this screen.

Table 240 Configuration > System > DNS > Service Control Rule Add

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select ALL to allow or deny any computer to send DNS queries to the USG. Select a predefined address object to just allow or deny the computer with the IP address that you specified to send DNS queries to the USG.
Zone	Select ALL to allow or prevent DNS queries through any zones. Select a predefined zone on which a DNS query to the USG is allowed or denied.
Action	Select Accept to have the USG allow the DNS queries from the specified computer. Select Deny to have the USG reject the DNS queries from the specified computer.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

30.7 WWW Overview

The following figure shows secure and insecure management of the USG coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

Note: To allow the USG to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-USG security policy rule to block that traffic.

To stop a service from accessing the USG, clear Enable in the corresponding service screen.

30.7.1 Service Access Limitations

A service cannot be used to access the USG when:

1. You have disabled that service in the corresponding screen.
2. The allowed IP address (address object) in the Service Control table does not match the client IP address (the USG disallows the session).

3 The IP address (address object) in the Service Control table is not in the allowed zone or the action is set to Deny.

4 There is a security policy rule that blocks it.

30.7.2 System Timeout

There is a lease timeout for administrators. The USG automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the USG for authentication again when the reauthentication time expires.

You can change the timeout settings in the User/ Group screens.

30.7.3 HTTPS

You can set the USG to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions. Specify which zones allow Web Configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

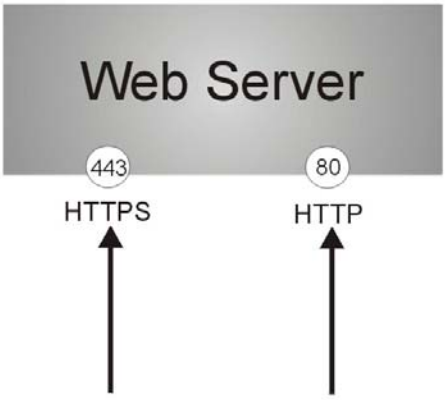
HTTPS on the USG is used so that you can securely access the USG using the Web Configurator. The SSL protocol specifies that the HTTPS server (the USG) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the USG), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select Authenticate Client Certificates in the WWW screen). Authenticate Client Certificates is optional and if selected means the HTTPS client must send the USG a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the USG.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the USG's web server.

2 HTTP connection requests from a web browser go to port 80 (by default) on the USG's web server.

Figure 379 HTTP/HTTPS Implementation



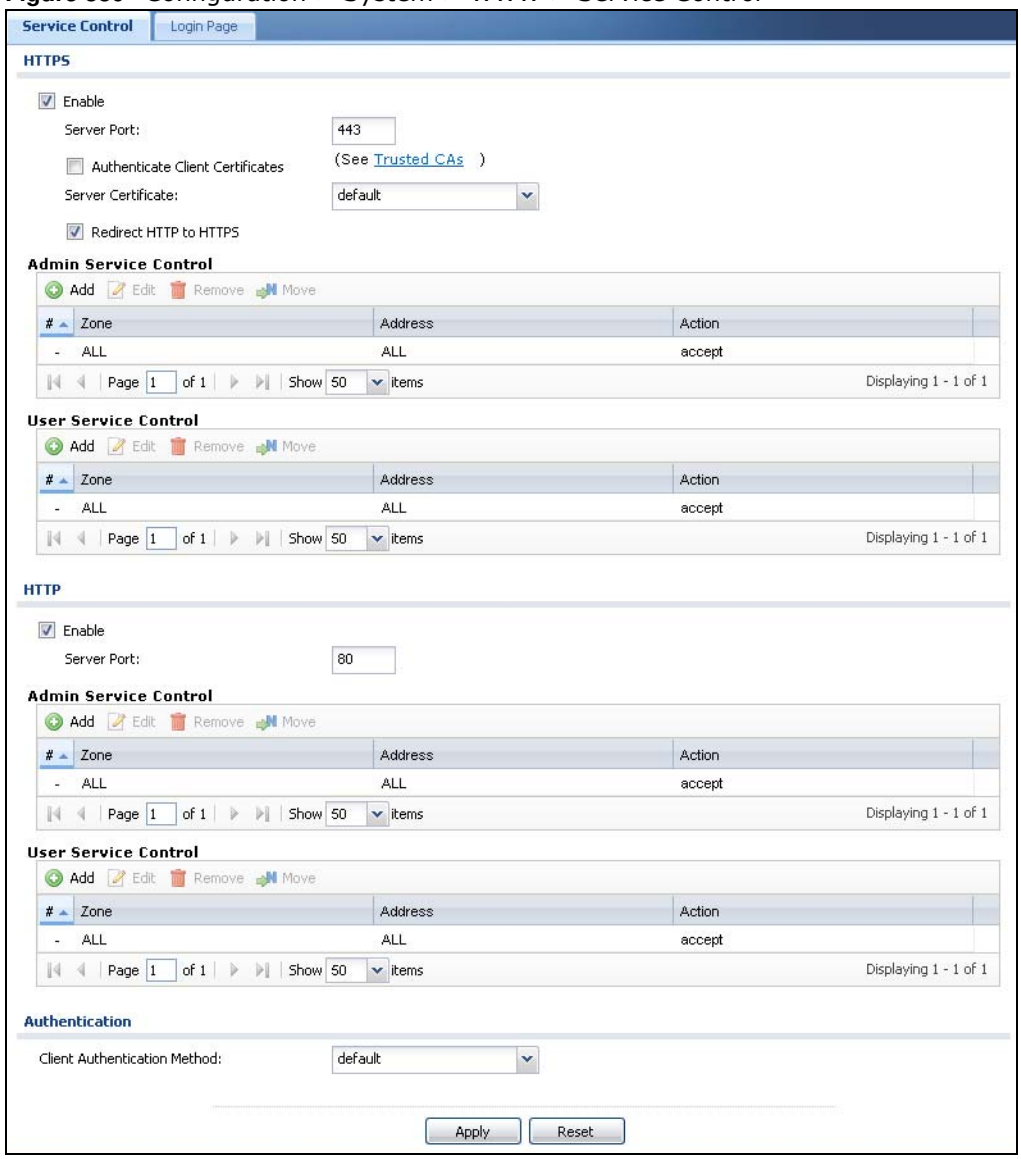
Note: If you disable HTTP in the WWW screen, then the USG blocks all HTTP connection attempts.

30.7.4 Configuring WWW Service Control

Click Configuration > System > WWW to open the WWW screen. Use this screen to specify from which zones you can access the USG using HTTP or HTTPS. You can also specify which IP addresses the access can come from.

Note: Admin Service Control deals with management access (to the Web Configurator). User Service Control deals with user access to the USG (logging into SSL VPN for example).

Figure 380 Configuration > System > WWW > Service Control



The following table describes the labels in this screen.

Table 241 Configuration > System > WWW > Service Control

LABEL	DESCRIPTION
HTTPS	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the USG Web Configurator using secure HTTPs connections.
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the USG, for example 8443, then you must notify people who need to access the USG Web Configurator to use "https://USG IP Address:8443" as the URL.

Table 241 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Authenticate Client Certificates	Select Authenticate Client Certificates (optional) to require the SSL client to authenticate itself to the USG by sending the USG a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the USG (see Section 30.7.7.5 on page 565 on importing certificates for details).
Server Certificate	Select a certificate the HTTPS server (the USG) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the My Certificates screen.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server.
Admin/User Service Control	Admin Service Control specifies from which zones an administrator can use HTTPS to manage the USG (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the USG. User Service Control specifies from which zones a user can use HTTPS to log into the USG (to log into SSL VPN for example). You can also specify the IP addresses from which the users can access the USG.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the USG's (non-configurable) default policy. The USG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the USG will not have to use the default policy.
Zone	This is the zone on the USG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the USG zone(s) configured in the Zone field (Accept) or not (Deny).
HTTP	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the USG Web Configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the USG.
Admin/User Service Control	Admin Service Control specifies from which zones an administrator can use HTTP to manage the USG (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the USG. User Service Control specifies from which zones a user can use HTTP to log into the USG (to log into SSL VPN for example). You can also specify the IP addresses from which the users can access the USG.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.

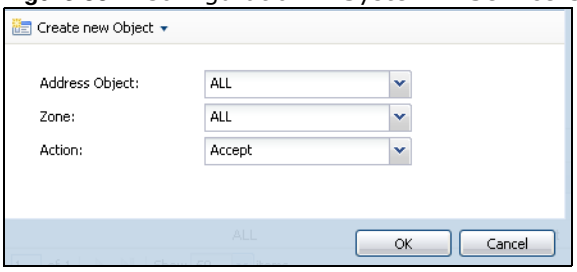
Table 241 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the USG's (non-configurable) default policy. The USG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the USG will not have to use the default policy.
Zone	This is the zone on the USG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the USG zone(s) configured in the Zone field (Accept) or not (Deny).
Authentication	
Client Authentication Method	Select a method the HTTPS or HTTP server uses to authenticate a client. You must have configured the authentication methods in the Auth. method screen.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

30.7.5 Service Control Rules

Click Add or Edit in the Service Control table in a WWW, SSH, Telnet, FTP or SNMP screen to add a service control rule.

Figure 381 Configuration > System > Service Control Rule > Edit



The following table describes the labels in this screen.

Table 242 Configuration > System > Service Control Rule > Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select ALL to allow or deny any computer to communicate with the USG using this service. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the USG using this service.

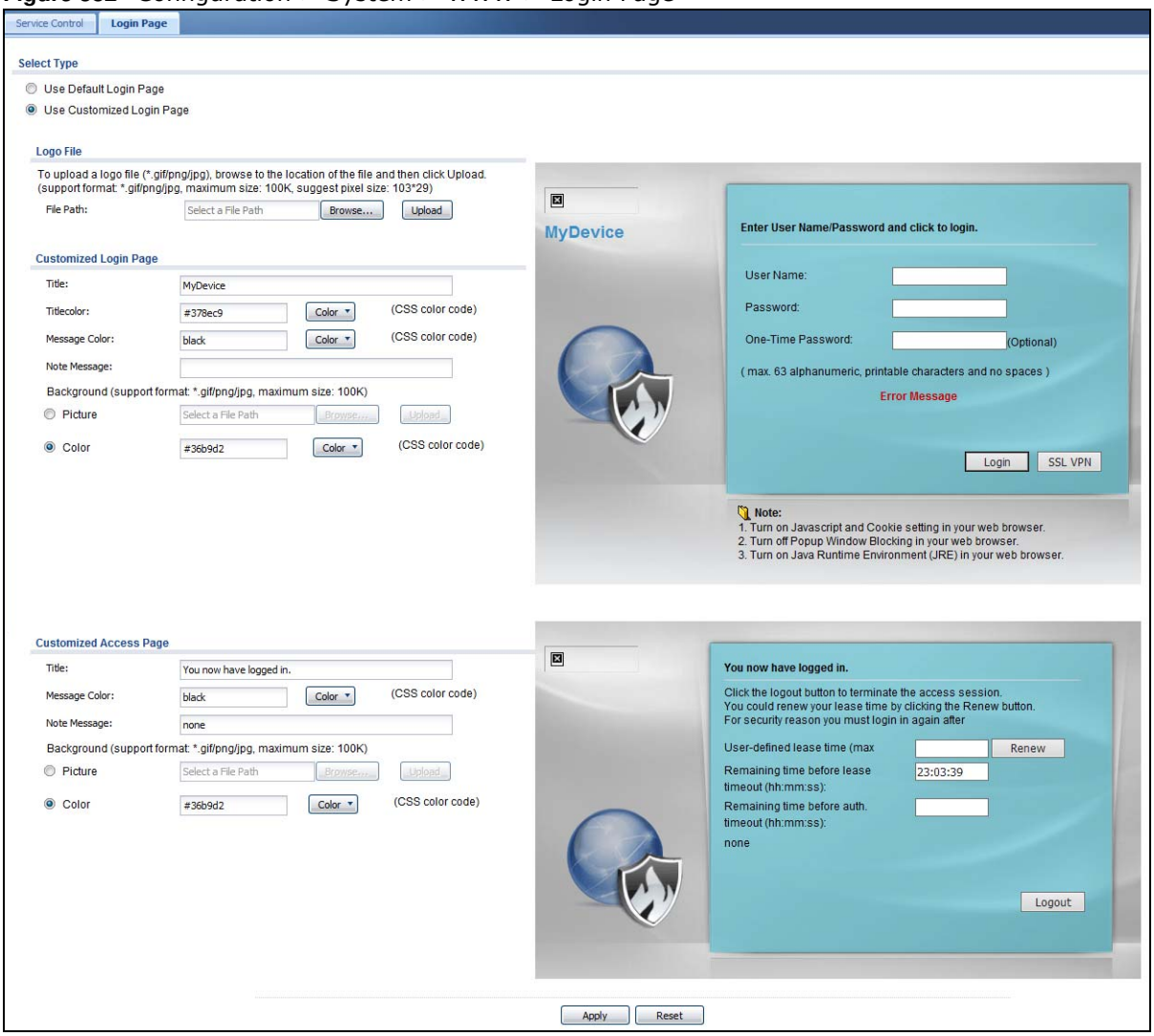
Table 242 Configuration > System > Service Control Rule > Edit

LABEL	DESCRIPTION
Zone	Select ALL to allow or prevent any USG zones from being accessed using this service. Select a predefined USG zone on which a incoming service is allowed or denied.
Action	Select Accept to allow the user to access the USG from the specified computers. Select Deny to block the user's access to the USG from the specified computers.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

30.7.6 Customizing the WWW Login Page

Click Configuration > System > WWW > Login Page to open the Login Page screen. Use this screen to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.

Figure 382 Configuration > System > WWW > Login Page



The following figures identify the parts you can customize in the login and access pages.

Figure 383 Login Page Customization

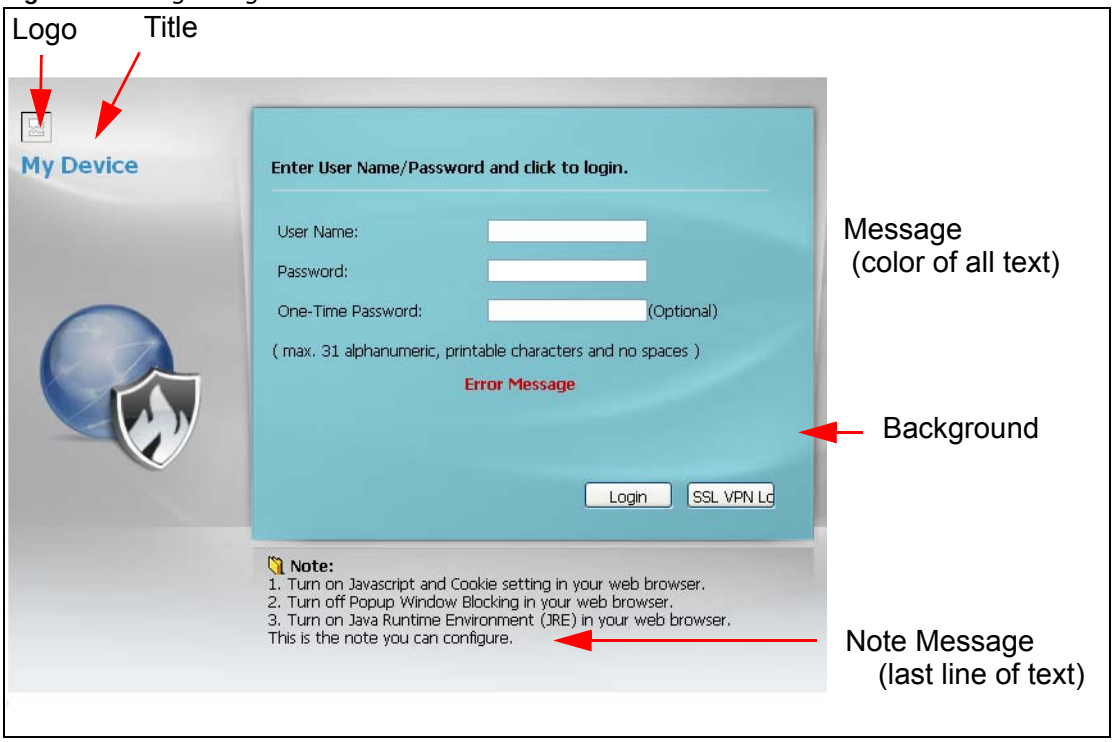
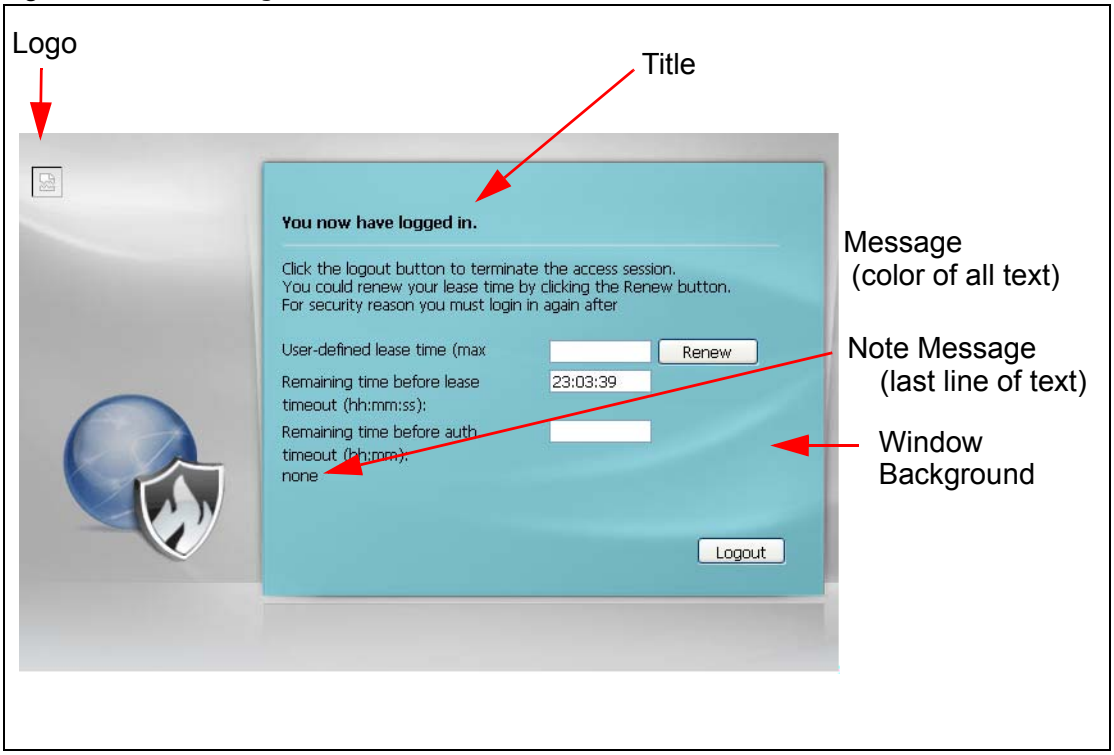


Figure 384 Access Page Customization



You can specify colors in one of the following ways:

- Click Color to display a screen of web-safe colors from which to choose.

- Enter the name of the desired color.
- Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use "#000000" for black.
- Enter "rgb" followed by red, green, and blue values in parenthesis and separate by commas. For example, use "rgb(0,0,0)" for black.

Your desired color should display in the preview screen on the right after you click in another field, click Apply, or press [ENTER]. If your desired color does not display, your browser may not support it. Try selecting another color.

The following table describes the labels in the screen.

Table 243 Configuration > System > WWW > Login Page

LABEL	DESCRIPTION
Select Type	Select whether the Web Configurator uses the default login screen or one that you customize in the rest of this screen.
Logo File	You can upload a graphic logo to be displayed on the upper left corner of the Web Configurator login screen and access page. Specify the location and file name of the logo graphic or click Browse to locate it. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. Click Upload to transfer the specified graphic file from your computer to the USG.
Customized Login Page	Use this section to set how the Web Configurator login screen looks.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Title Color	Specify the color of the screen's title text.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display at the bottom of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Background	Set how the screen background looks. To use a graphic, select Picture and upload a graphic. Specify the location and file name of the logo graphic or click Browse to locate it. The picture's size cannot be over 438 x 337 pixels. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select Color and specify the color.
Customized Access Page	Use this section to customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display below the title. Use up to 64 printable ASCII characters. Spaces are allowed.

Table 243 Configuration > System > WWW > Login Page

LABEL	DESCRIPTION
Background	Set how the window's background looks. To use a graphic, select Picture and upload a graphic. Specify the location and file name of the logo graphic or click Browse to locate it. The picture's size cannot be over 438 x 337 pixels. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select Color and specify the color.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

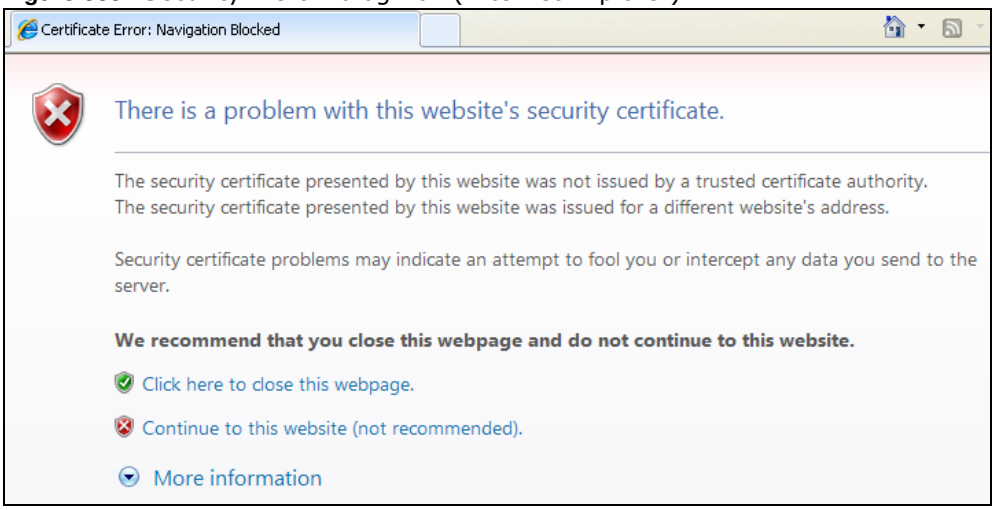
30.7.7 HTTPS Example

If you haven't changed the default HTTPS port on the USG, then in your browser enter "https://USG IP Address/" as the web site address where "USG IP Address" is the IP address or domain name of the USG you wish to access.

30.7.7.1 Internet Explorer Warning Messages

When you attempt to access the USG HTTPS server, you will see the error message shown in the following screen.

Figure 385 Security Alert Dialog Box (Internet Explorer)



Select Continue to this website to proceed to the Web Configurator login screen. Otherwise, select Click here to close this webpage to block the access.

30.7.7.2 Mozilla Firefox Warning Messages

When you attempt to access the USG HTTPS server, a The Connection is Untrusted screen appears as shown in the following screen. Click Technical Details if you want to verify more information about the certificate from the USG.

Select I Understand the Risks and then click Add Exception to add the USG to the security exception list. Click Confirm Security Exception.

Figure 386 Security Certificate 1 (Firefox)

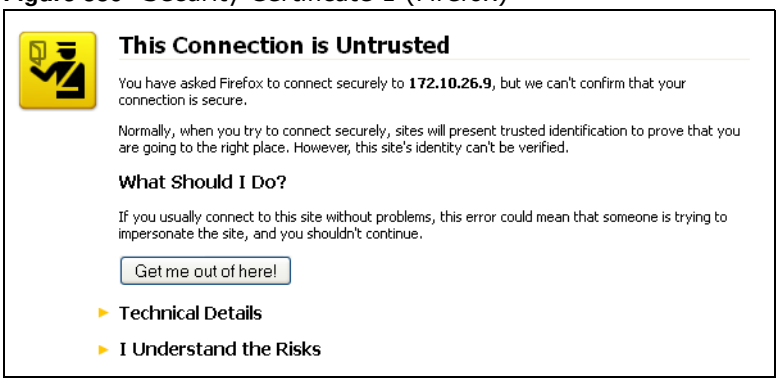
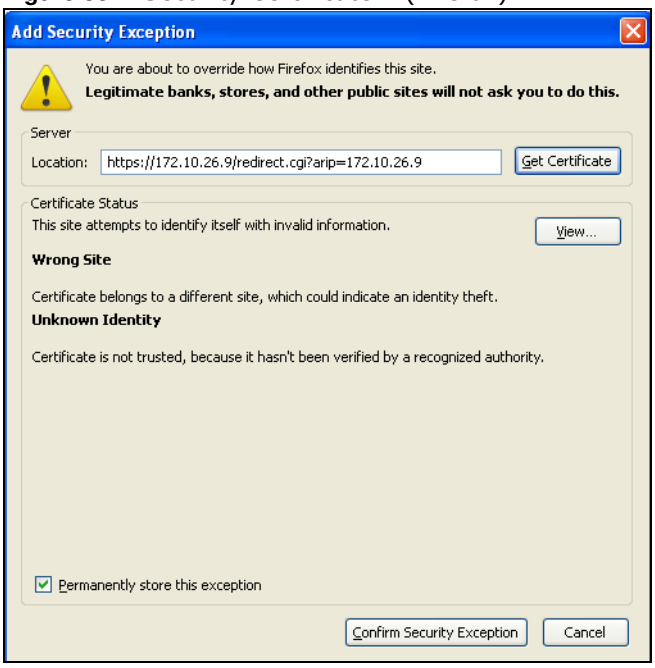


Figure 387 Security Certificate 2 (Firefox)



30.7.7.3 Avoiding Browser Warning Messages

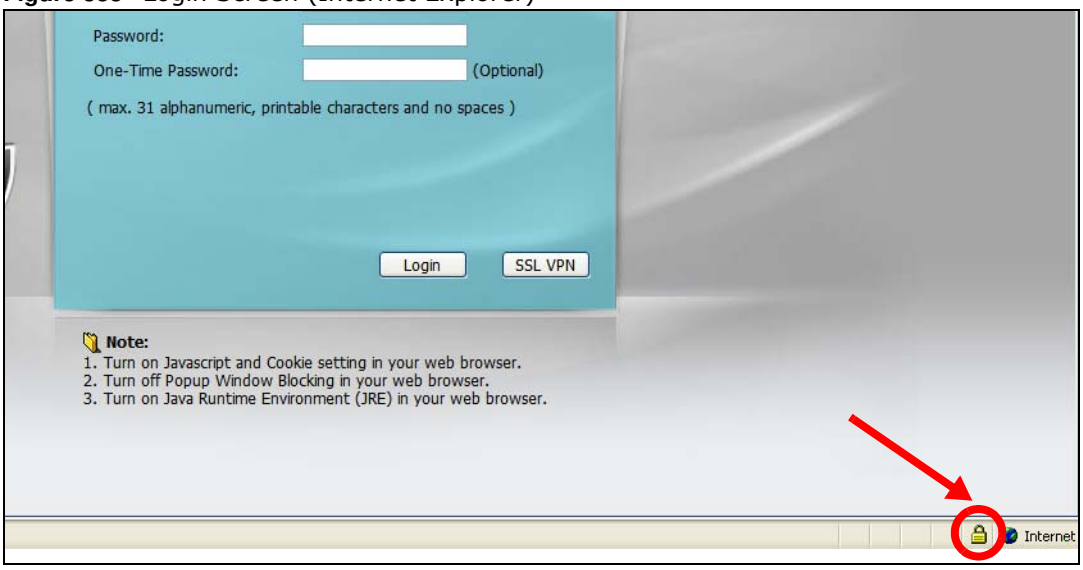
Here are the main reasons your browser displays warnings about the USG's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the USG's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the USG's factory default certificate is the USG itself since the certificate is a self-signed certificate.
- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate.

30.7.7.4 Login Screen

After you accept the certificate, the USG login screen appears. The lock displayed in the bottom of the browser status bar denotes a secure connection.

Figure 388 Login Screen (Internet Explorer)



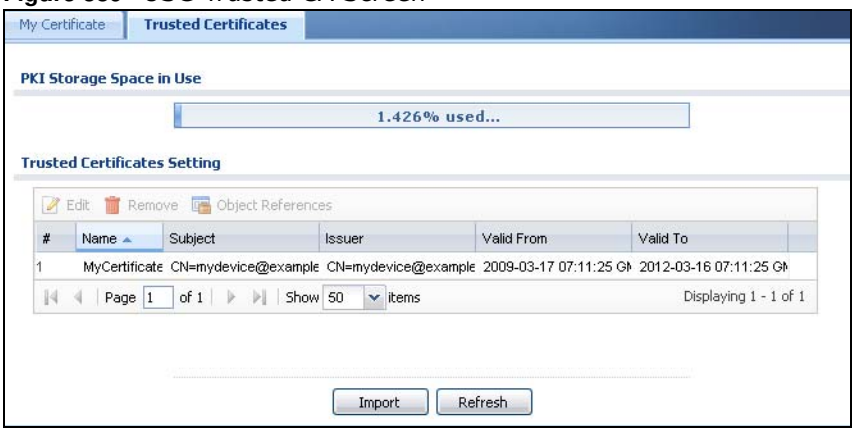
30.7.7.5 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if Authenticate Client Certificates is selected on the USG.

You must have imported at least one trusted CA to the USG in order for the Authenticate Client Certificates to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the USG (see the USG's Trusted CA Web Configurator screen).

Figure 389 USG Trusted CA Screen



The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

30.7.7.5.1 Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 390 CA Certificate Example



2 Click Install Certificate and follow the wizard as shown earlier in this appendix.

30.7.7.5.2 Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

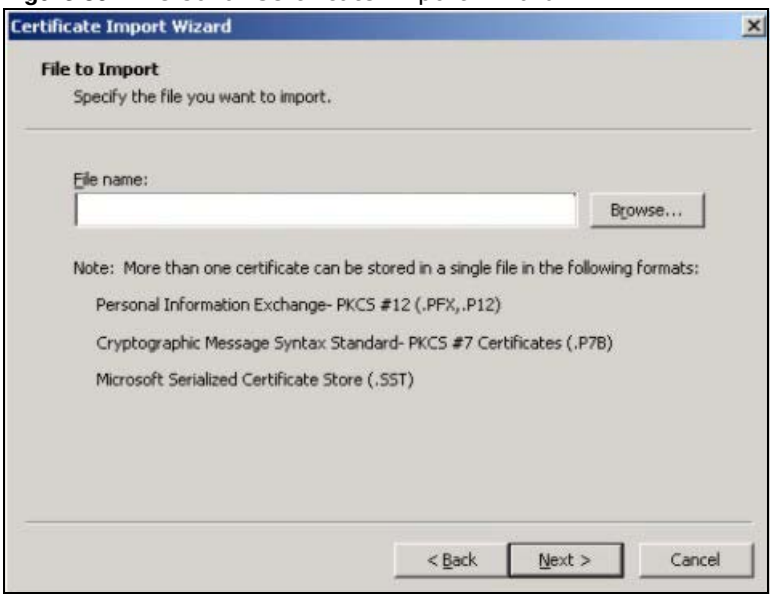
1 Click Next to begin the wizard.

Figure 391 Personal Certificate Import Wizard 1



2 The file name and path of the certificate you double-clicked should automatically appear in the File name text box. Click Browse if you wish to import a different certificate.

Figure 392 Personal Certificate Import Wizard 2



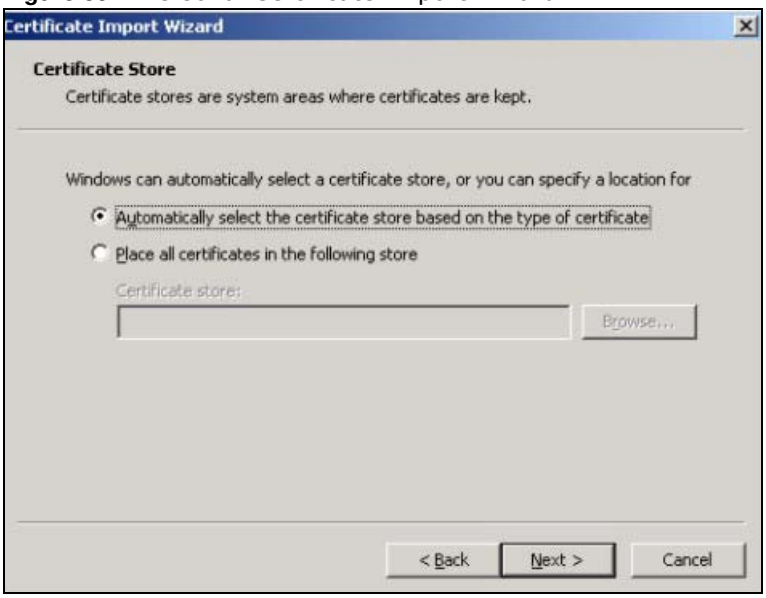
3 Enter the password given to you by the CA.

Figure 393 Personal Certificate Import Wizard 3



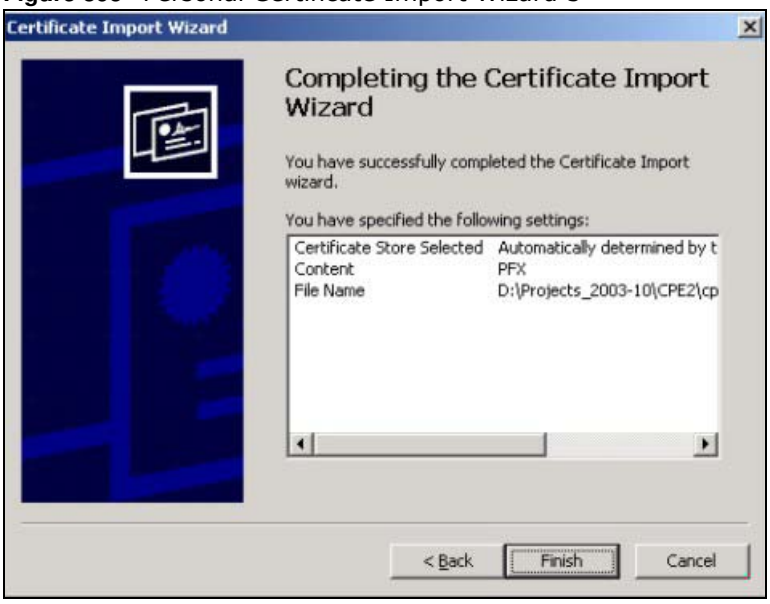
4 Have the wizard determine where the certificate should be saved on your computer or select Place all certificates in the following store and choose a different location.

Figure 394 Personal Certificate Import Wizard 4



5 Click Finish to complete the wizard and begin the import process.

Figure 395 Personal Certificate Import Wizard 5



6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 396 Personal Certificate Import Wizard 6



30.7.7.6 Using a Certificate When Accessing the USG Example

Use the following procedure to access the USG via HTTPS.

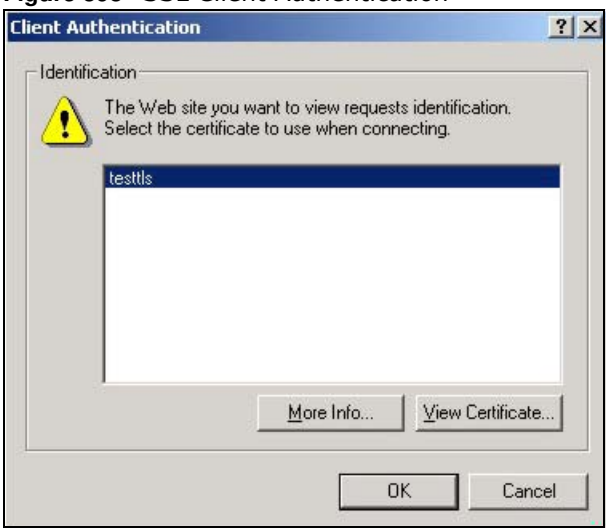
1 Enter 'https://USG IP Address/ in your browser's web address field.

Figure 397 Access the USG Via HTTPS



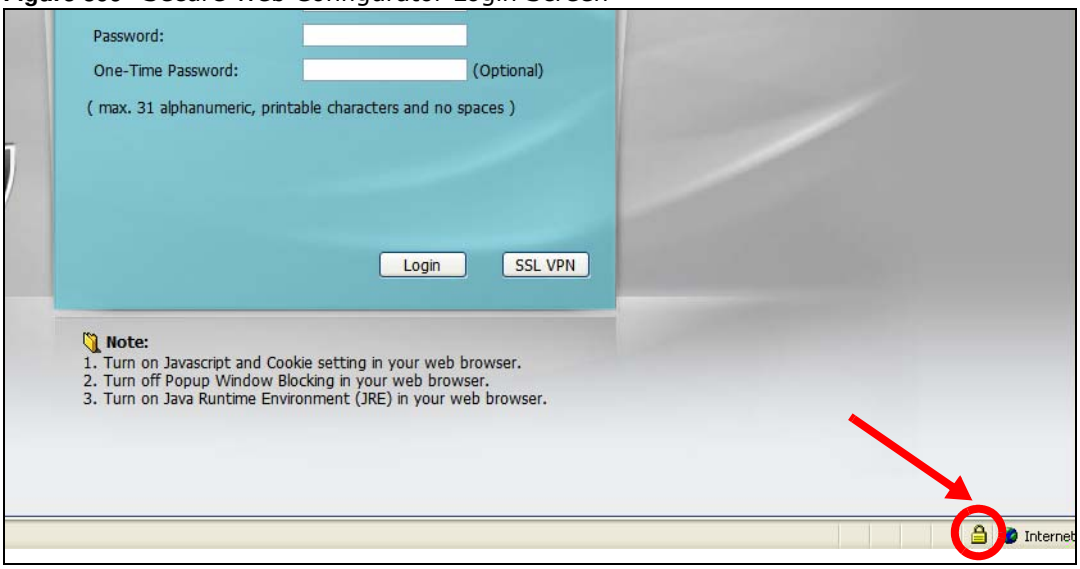
2 When Authenticate Client Certificates is selected on the USG, the following screen asks you to select a personal certificate to send to the USG. This screen displays even if you only have a single certificate as in the example.

Figure 398 SSL Client Authentication



3 You next see the Web Configurator login screen.

Figure 399 Secure Web Configurator Login Screen



30.8 SSH

You can use SSH (Secure SHell) to securely access the USG's command line interface. Specify which zones allow SSH access and from which IP address the access can come.

SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer A on the Internet uses SSH to securely connect to the WAN port of the USG for a management session.

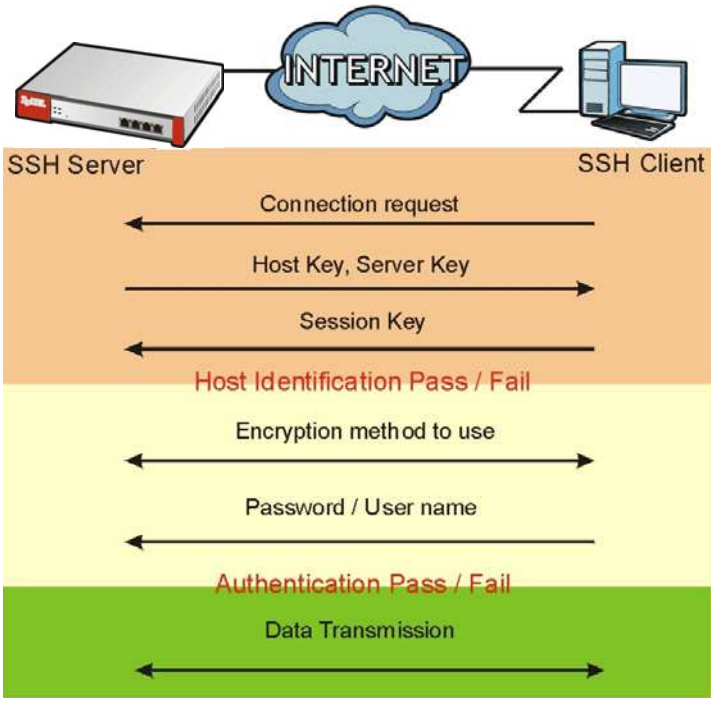
Figure 400 SSH Communication Over the WAN Example



30.8.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

Figure 401 How SSH v1 Works Example



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

30.8.2 SSH Implementation on the USG

Your USG supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the USG for management using port 22 (by default).

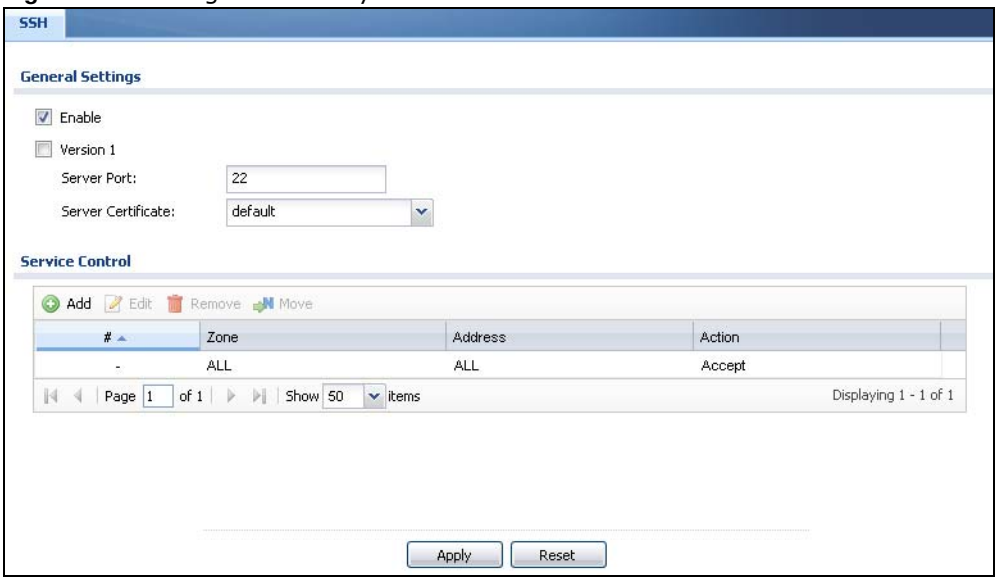
30.8.3 Requirements for Using SSH

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

30.8.4 Configuring SSH

Click Configuration > System > SSH to change your USG's Secure Shell settings. Use this screen to specify from which zones SSH can be used to manage the USG. You can also specify from which IP addresses the access can come.

Figure 402 Configuration > System > SSH



The following table describes the labels in this screen.

Table 244 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the USG CLI using this service.
Version 1	Select the check box to have the USG use both SSH version 1 and version 2 protocols. If you clear the check box, the USG uses only SSH version 2 protocol.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the USG for SSH connections. You must have certificates already configured in the My Certificates screen.
Service Control	This specifies from which computers you can access which USG zones.

Table 244 Configuration > System > SSH (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 242 on page 559 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule.
Zone	This is the zone on the USG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the USG zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

30.8.5 Secure Telnet Using SSH Examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the USG. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

30.8.5.1 Example 1: Microsoft Windows

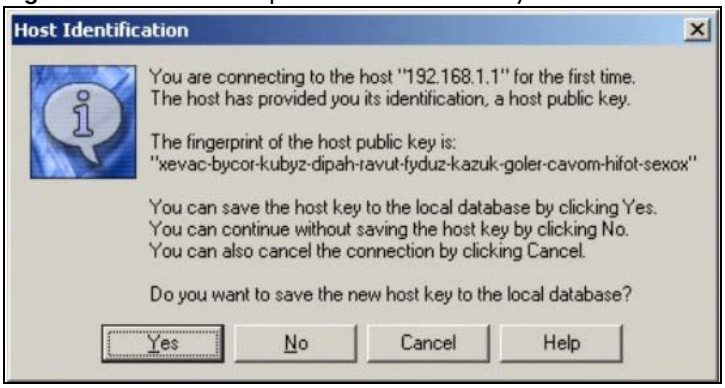
This section describes how to access the USG using the Secure Shell Client program.

1 Launch the SSH client and specify the connection information (IP address, port number) for the USG.

2 Configure the SSH client to accept connection using SSH version 1.

3 A window displays prompting you to store the host key in you computer. Click Yes to continue.

Figure 403 SSH Example 1: Store Host Key



Enter the password to log in to the USG. The CLI screen displays next.

30.8.5.2 Example 2: Linux

This section describes how to access the USG using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the USG.

Enter "`telnet 192.168.1.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the USG (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the USG.

Figure 404 SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "`ssh -1 192.168.1.1`". This command forces your computer to connect to the USG using SSH version 1. If this is the first time you are connecting to the USG using SSH, a message displays prompting you to save the host information of the USG. Type "`yes`" and press [ENTER].

Then enter the password to log in to the USG.

Figure 405 SSH Example 2: Log in

```
$ ssh -1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
```

3 The CLI screen displays next.

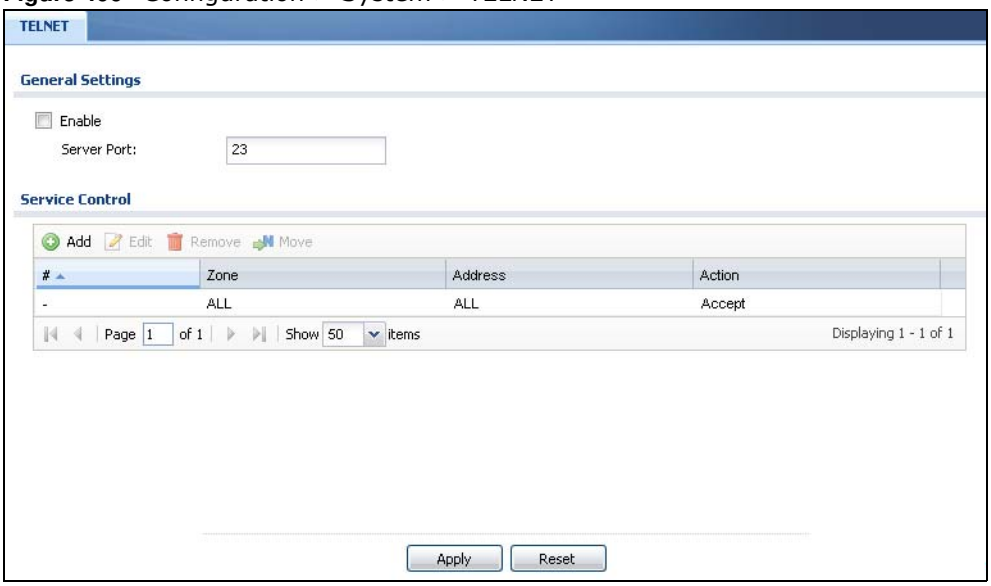
30.9 Telnet

You can use Telnet to access the USG's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.

30.9.1 Configuring Telnet

Click Configuration > System > TELNET to configure your USG for remote Telnet access. Use this screen to specify from which zones Telnet can be used to manage the USG. You can also specify from which IP addresses the access can come.

Figure 406 Configuration > System > TELNET



The following table describes the labels in this screen.

Table 245 Configuration > System > TELNET

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the USG CLI using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Control	This specifies from which computers you can access which USG zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 242 on page 559 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the USG's (non-configurable) default policy. The USG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the USG will not have to use the default policy.
Zone	This is the zone on the USG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the USG zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

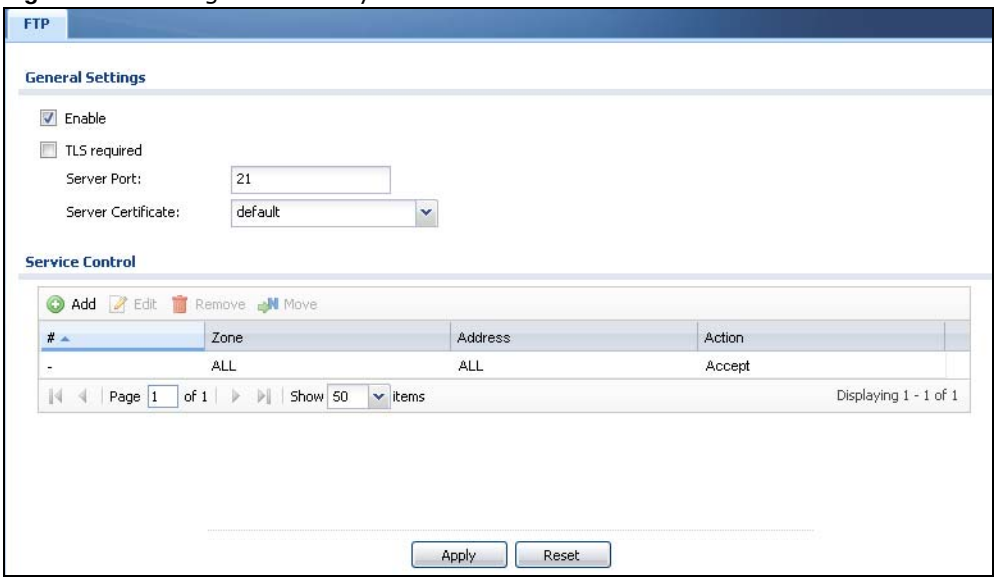
30.10 FTP

You can upload and download the USG's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

30.10.1 Configuring FTP

To change your USG's FTP settings, click Configuration > System > FTP tab. The screen appears as shown. Use this screen to specify from which zones FTP can be used to access the USG. You can also specify from which IP addresses the access can come.

Figure 407 Configuration > System > FTP



The following table describes the labels in this screen.

Table 246 Configuration > System > FTP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the USG using this service.
TLS required	Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the USG for FTP connections. You must have certificates already configured in the My Certificates screen.
Service Control	This specifies from which computers you can access which USG zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 242 on page 559 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.

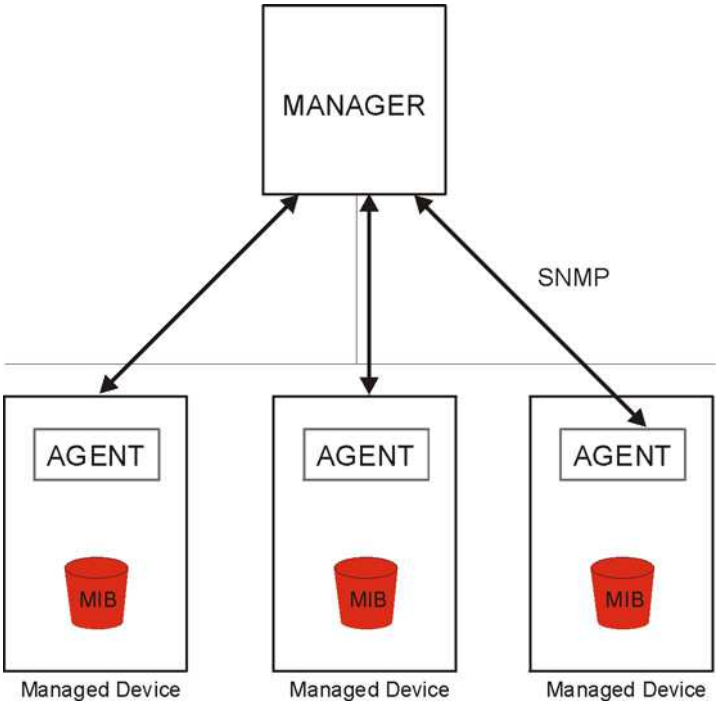
Table 246 Configuration > System > FTP (continued)

LABEL	DESCRIPTION
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the USG's (non-configurable) default policy. The USG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the USG will not have to use the default policy.
Zone	This is the zone on the USG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the USG zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

30.11 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your USG supports SNMP agent functionality, which allows a manager station to manage and monitor the USG through the network. The USG supports SNMP version one (SNMPv1), version two (SNMPv2c) and version 3 (SNMPv3). The next figure illustrates an SNMP management operation.

Figure 408 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 USG). 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.

30.11.1 SNMPv3 and Security

SNMPv3 enhances security for SNMP management using authentication and encryption. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

30.11.2 Supported MIBs

The USG supports MIB II that is defined in RFC-1213 and RFC-1215. The USG also supports private MIBs (zywall.mib and zyxel-zywall-ZLD-Common.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the USG's MIBs from www.zyxel.com.

30.11.3 SNMP Traps

The USG will send traps to the SNMP manager when any one of the following events occurs.

Table 247 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the USG is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.

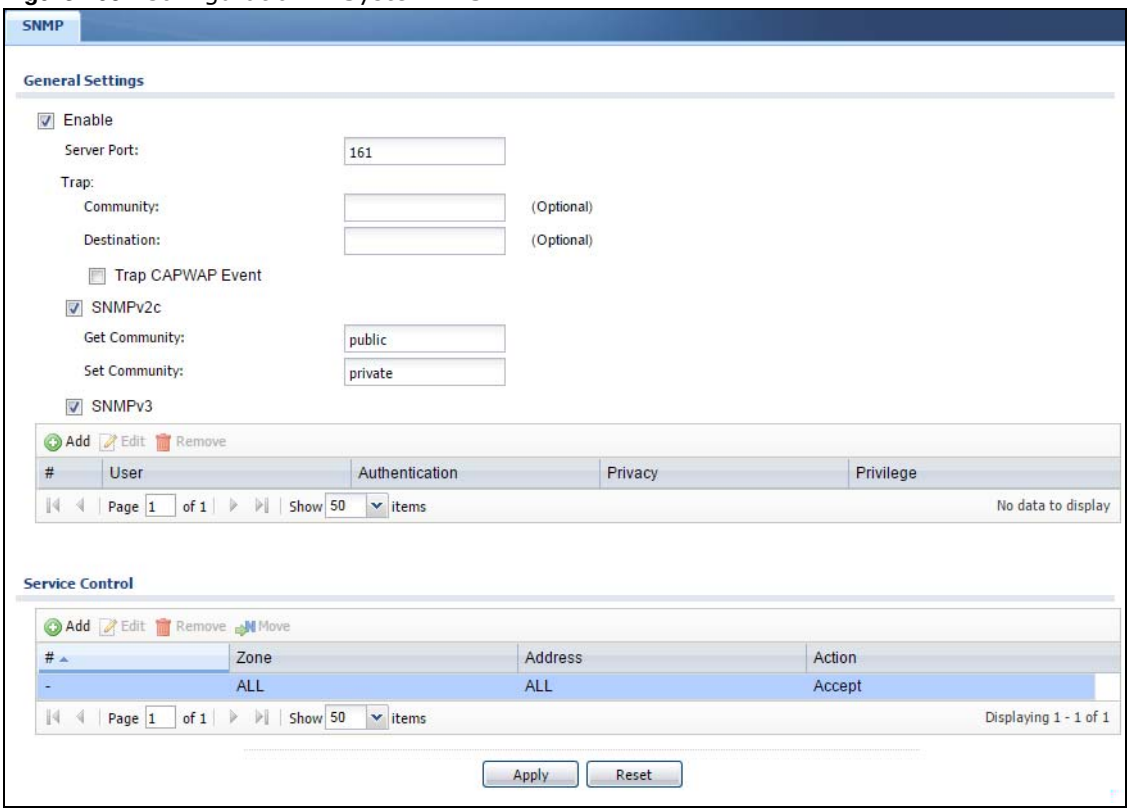
Table 247 SNMP Traps (continued)

OBJECT LABEL	OBJECT ID	DESCRIPTION
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
vpnTunnelDisconnected	1.3.6.1.4.1.890.1.6.22.2.3	This trap is sent when an IPSec VPN tunnel is disconnected.
vpnTunnelName	1.3.6.1.4.1.890.1.6.22.2.2.1.1	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IPSec SA name.
vpnIKEName	1.3.6.1.4.1.890.1.6.22.2.2.1.2	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IKE SA name.
vpnTunnelSPI	1.3.6.1.4.1.890.1.6.22.2.2.1.3	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the security parameter index (SPI) of the disconnected VPN tunnel.

30.11.4 Configuring SNMP

To change your USG's SNMP settings, click Configuration > System > SNMP tab. The screen appears as shown. Use this screen to configure your SNMP settings, including from which zones SNMP can be used to access the USG. You can also specify from which IP addresses the access can come.

Figure 409 Configuration > System > SNMP



The following table describes the labels in this screen.

Table 248 Configuration > System > SNMP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the USG using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
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.
SNMPv2c	Select the SNMP version for the USG. The SNMP version on the USG must match the version on the SNMP manager.
Get Community	Enter the Get Community, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community, which is the password for incoming Set requests from the management station. The default is private and allows all requests.
SNMPv3	Select the SNMP version for the USG. The SNMP version on the USG must match the version on the SNMP manager. SNMPv3 (RFCs 3413 to 3415) provides secure access by authenticating and encrypting data packets over the network. The USG uses your login password as the SNMPv3 authentication and encryption passphrase. Note: Your login password must consist of at least 8 printable characters for SNMPv3. An error message will display if your login password has fewer characters.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the entry.
User	This displays the name of the user object to be sent to the SNMP manager along with the SNMP v3 trap.
Authentication	This displays the authentication algorithm used for this entry. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy	This displays the encryption method for SNMP communication from this user. Methods available are: • DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Privlege	This displays the access rights to MIBs. • Read-Write - The associated user can create and edit the MIBs on the USG, except the user account. • Read-Only - The associated user can only collect information from the USG MIBs.
Service Control	This specifies from which computers you can access which USG zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 242 on page 559 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.

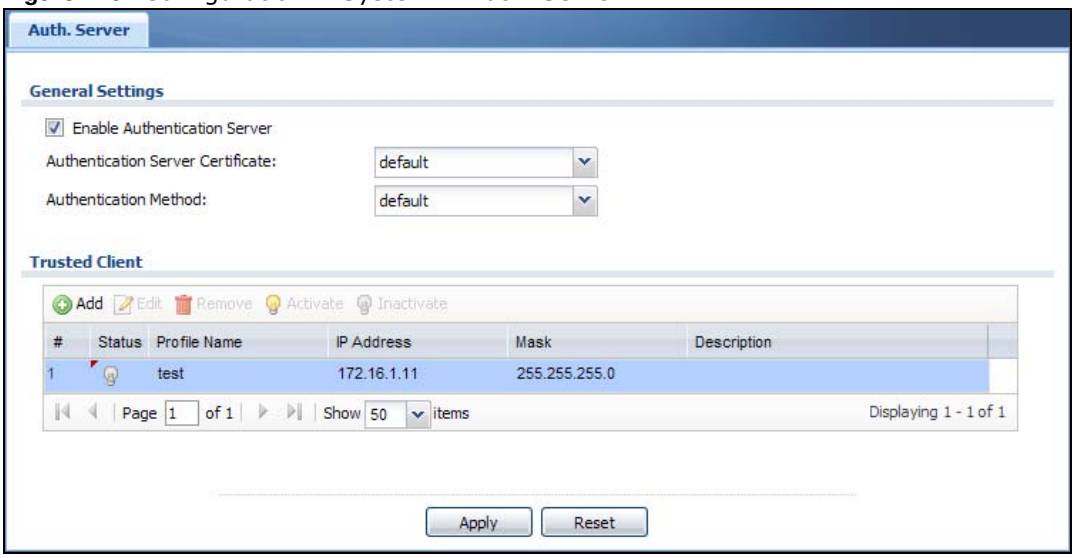
Table 248 Configuration > System > SNMP (continued)

LABEL	DESCRIPTION
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the USG's (non-configurable) default policy. The USG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the USG will not have to use the default policy.
Zone	This is the zone on the USG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the USG zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

30.12 Authentication Server

You can set the USG to work as a RADIUS server to exchange messages with a RADIUS client, such as an AP for user authentication and authorization. Click Configuration > System > Auth. Server tab. The screen appears as shown. Use this screen to enable the authentication server feature of the USG and specify the RADIUS client's IP address.

Figure 410 Configuration > System > Auth. Server



The following table describes the labels in this screen.

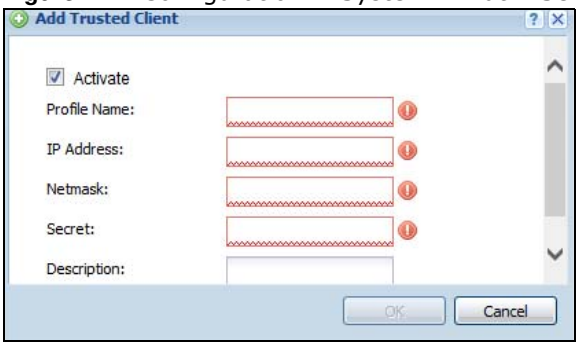
Table 249 Configuration > System > Auth. Server

LABEL	DESCRIPTION
Enable Authentication Server	Select the check box to have the USG act as a RADIUS server.
Authentication Server Certificate	Select the certificate whose corresponding private key is to be used to identify the USG to the RADIUS client. You must have certificates already configured in the My Certificates screen.
Authentication Method	Select an authentication method if you have created any in the Configuration > Object > Auth. Method screen.
Trusted Client	Use this section to configure trusted clients in the USG RADIUS server database.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The USG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This is the index number of the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field indicates the name assigned to the profile.
IP Address	This is the IP address of the RADIUS client that is allowed to exchange messages with the USG.
Mask	This is the subnet mask of the RADIUS client.
Description	This is the description of the RADIUS client.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

30.12.1 Add/Edit Trusted RADIUS Client

Click Configuration > System > Auth. Server to display the Auth. Server screen. Click the Add icon or an Edit icon to display the following screen. Use this screen to create a new entry or edit an existing one.

Figure 411 Configuration > System > Auth. Server > Add/Edit



The following table describes the labels in this screen.

Table 250 Configuration > System > Auth. Server > Add/Edit

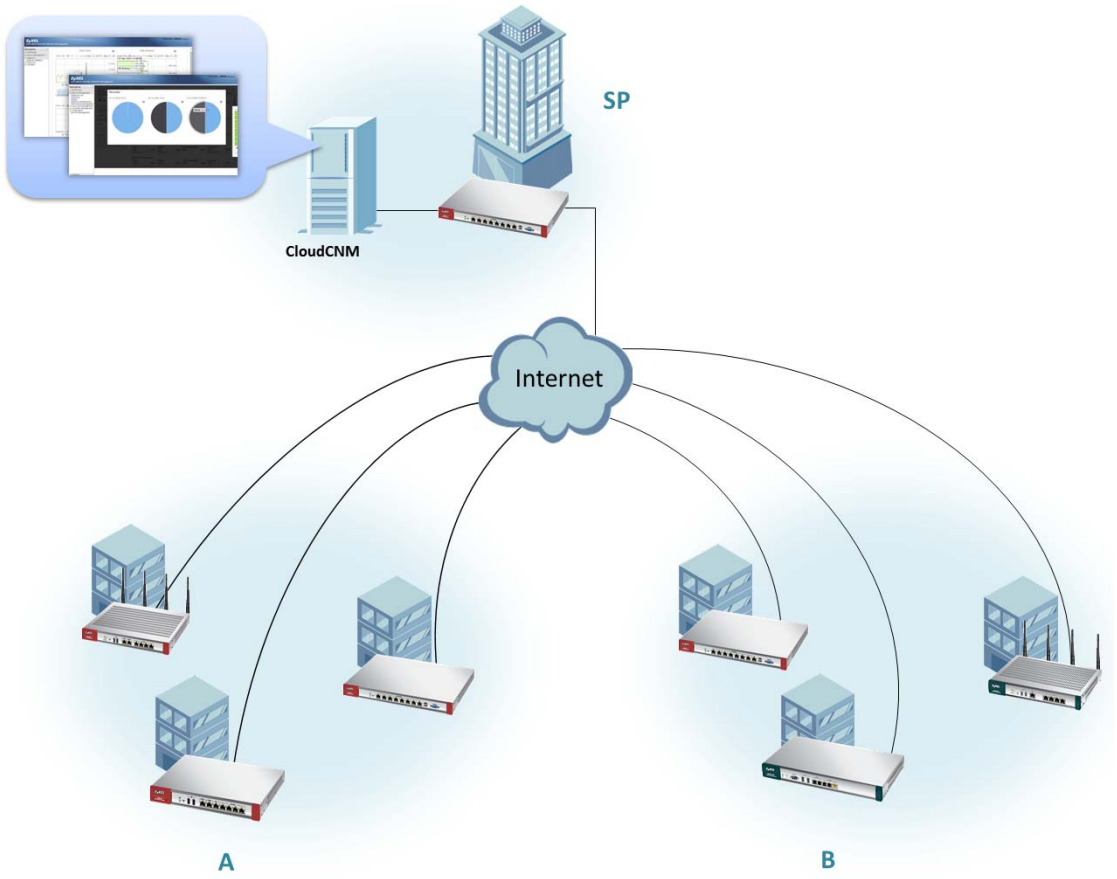
LABEL	DESCRIPTION
Activate	Select this check box to make this profile active.
Profile Name	Enter a descriptive name (up to 31 alphanumerical characters) for identification purposes.
IP Address	Enter the IP address of the RADIUS client that is allowed to exchange messages with the USG.
Netmask	Enter the subnet mask of the RADIUS client.
Secret	Enter a password (up to 64 alphanumeric characters) as the key to be shared between the USG and the RADIUS client. The key is not sent over the network. This key must be the same on the external authentication server and the USG.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

30.13 CloudCNM Screen

CloudCNM is a cloud-based network management system that allows management and monitoring of ZyWALL/USG/UAG security gateways with firmware that supports the TR-069 protocol.

In the following figure, SP is the management service provider, while A and B are sites with devices being managed by SP.

Figure 412 CloudCNM Example Network Topology



CloudCNM features include:

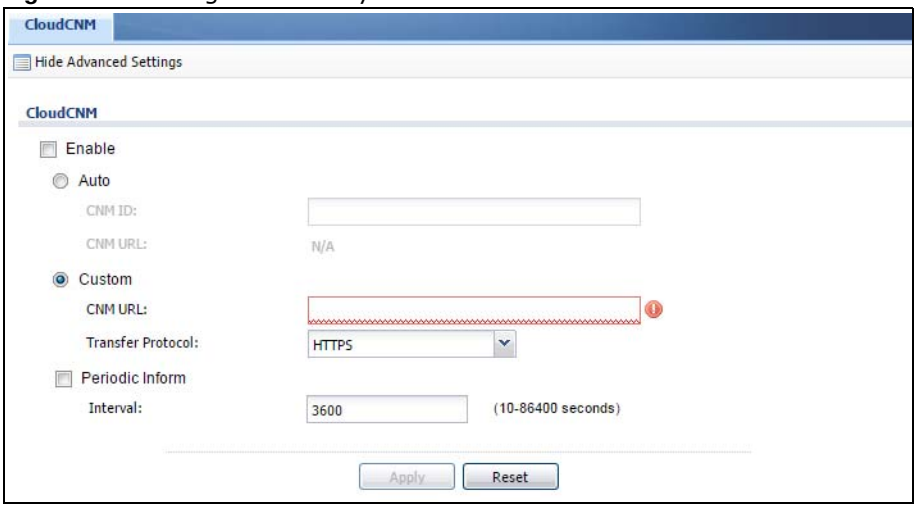
- Batch import of managed devices at one time using one CSV file
- See an overview of all managed devices and system information in one place
- Monitor and manage devices
- Install firmware to multiple devices of the same model at one time
- Backup and restore device configuration
- View the location of managed devices on a map
- Receive notification for events and alarms, such as when a device goes down
- Graphically monitor individual devices and see related statistics
- Directly access a device for remote configuration
- Create four types of administrators with different privileges
- Perform Site-to-Site, Hub & Spoke, Fully-meshed and Remote Access VPN provisioning.

To allow CloudCNM management of your USG:

- You must have a CloudCNM license with CNM ID number or a CloudCNM URL identifying the server.
- The USG must be able to communicate with the CloudCNM server.

You must configure Configuration > System > CloudCNM to allow the USG to find the CloudCNM server.

Figure 413 Configuration > System > CloudCNM



The following table describes the labels in this screen.

Table 251 Configuration > System > CloudCNM

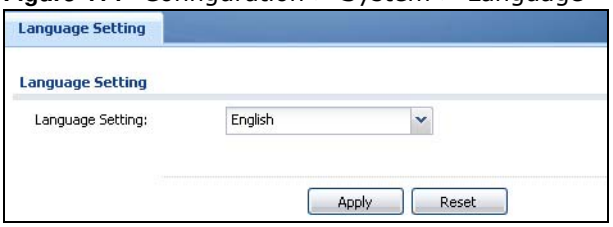
LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable	Select this to allow management of the USG by CloudCNM.
Auto	Select this if your CloudCNM server can access MyZyXEL.com and you have a CNM ID from the CloudCNM license.
CNM ID	Enter the CNM ID exactly as on the CloudCNM license.
CNM URL	MyZyXEL.com associates the CNM ID with the CNM URL which identifies the server on which CloudCNM is installed. Therefore you don't need to enter the CNM URL when you select Auto.
Custom	Select this if your CloudCNM server cannot access MyZyXEL.com.
CNM URL	If your USG server cannot access MyZyXEL.com, then select Custom and enter the IPv4 IP address of the CloudCNM server followed by the port number (default 7547 for HTTPS or 7549 for HTPP) in CNM URL. For example, if you installed CloudCNM on a server with IP address 1.1.1.1, then enter 1.1.1.1:7547 or 1.1.1.1:7549 as the CNM URL.
Transfer Protocol	Choose the CNM URL protocol: HTTP or HTTPS. If you enter 1.1.1.1:7547 as the CNM URL, you must choose HTTPS as the Transfer Protocol, and then the whole CNM URL is https://1.1.1.1:7547. If you enter 1.1.1.1:7549 as the CNM URL, you must choose HTTP as the Transfer Protocol, and then the whole CNM URL is http://1.1.1.1:7549.
Periodic Inform	Enable this to have the USG inform the CloudCNM server of its presence at regular intervals.
Interval	Type how often the USG should inform CloudCNM server of its presence.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

Note: See the CloudCNM User Guide for more information on CloudCNM.

30.14 Language Screen

Click Configuration > System > Language to open the following screen. Use this screen to select a display language for the USG's Web Configurator screens.

Figure 414 Configuration > System > Language



The following table describes the labels in this screen.

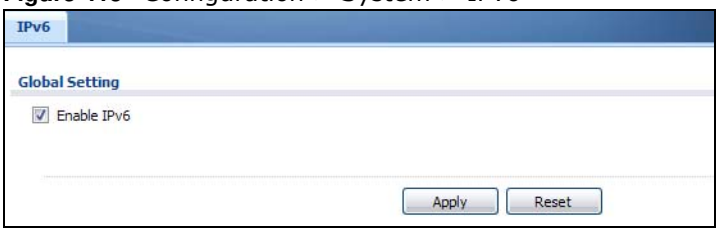
Table 252 Configuration > System > Language

LABEL	DESCRIPTION
Language Setting	Select a display language for the USG's Web Configurator screens. You also need to open a new browser session to display the screens in the new language.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

30.15 IPv6 Screen

Click Configuration > System > IPv6 to open the following screen. Use this screen to enable IPv6 support for the USG's Web Configurator screens.

Figure 415 Configuration > System > IPv6



The following table describes the labels in this screen.

Table 253 Configuration > System > IPv6

LABEL	DESCRIPTION
Enable IPv6	Select this to have the USG support IPv6 and make IPv6 settings be available on the screens that the functions support, such as the Configuration > Network > Interface > Ethernet, VLAN, and Bridge screens. The USG discards all IPv6 packets if you clear this check box.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

30.16 ZyXEL One Network (ZON) Utility

The ZyXEL One Network (ZON) utility uses the ZyXEL Discovery Protocol (ZDP) for discovering and configuring ZDP-aware ZyXEL devices in the same broadcast domain as the computer on which ZON is installed.

The ZON Utility issues requests via ZDP and in response to the query, the ZyXEL device responds with basic information including IP address, firmware version, location, system and model name. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on a computer.

The following figure shows the ZON Utility screen.

Figure 416 ZON Utility Screen



In the ZON Utility, select a device and then use the icons to perform actions. The following table describes the icons numbered from left to right in the ZON Utility screen.

Table 254 ZON Utility Icons

ICON	DESCRIPTION
1 IP configuration	Change the selected device's IP address. This is not supported by the USG at the time of writing.
2 Renew IP	Update a DHCP-assigned dynamic IP address. This is not supported by the USG at the time of writing.
3 Reboot Device	Use this icon to restart the selected device(s). This may be useful when troubleshooting or upgrading new firmware.
4 Flash Locator LED	Use this icon to locate the selected device by causing its Locator LED to blink. This is not available on the USG at the time of writing.
5 Web GUI	Use this to access the selected device web configurator from your browser. You will need a username and password to log in.
6 Firmware Upgrade	Use this icon to upgrade new firmware to selected device(s) of the same model. Make sure you have downloaded the firmware from the ZyXEL website to your computer and unzipped it in advance.
7 Change Admin Password	Use this icon to change the admin password of the selected device. You must know the current admin password before changing to a new one.
8 ZAC	Use this icon to run the ZyXEL AP Configurator of the selected AP. This is not supported by the USG at the time of writing.
9 Discovery	You should use this icon first to display all connected devices in the same network as your computer.
10 Save Configuration	Use this icon to save configuration changes to permanent memory on a selected device. This is not needed by the USG at the time of writing.
11 Settings	Use this icon to select a network adaptor for the computer on which the ZON utility is installed, and the utility language.

The following table describes the fields in the ZON Utility main screen.

Table 255 ZON Utility Fields

LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.
IP Address	This field displays the IP address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility.
System Name	This field displays the system name of the discovered device.
Location	This field displays where the discovered device is.
Status	This field displays whether changes to the discovered device have been done successfully. As the USG does not support IP Configuration, Renew IP address and Flash Locator LED, this field displays "Update failed", "Not support Renew IP address" and "Not support Flash Locator LED" respectively.

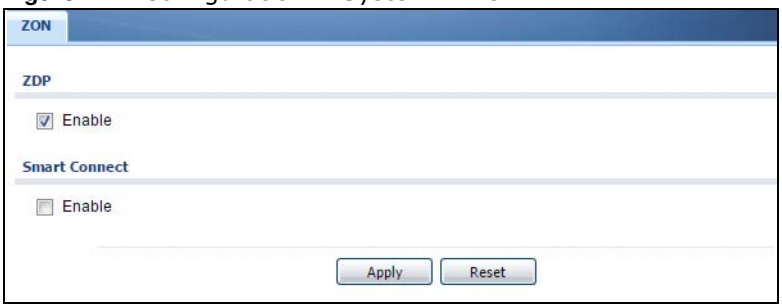
30.16.1 ZyXEL One Network (ZON) System Screen

Enable ZDP (ZON) and Smart Connect (Ethernet Neighbor) in the System > ZON screen.

See Monitor > System Status > Ethernet Neighbor for information on using Smart Connect (Link Layer Discovery Protocol (LLDP)) for discovering and configuring LLDP-aware devices in the same broadcast domain as the USG that you're logged into using the web configurator.

The following figure shows the System > ZON screen.

Figure 417 Configuration > System > ZON



The following table describes the labels in this screen.

Table 256 Configuration > System > ZON

LABEL	DESCRIPTION
ZDP	ZyXEL Discovery Protocol (ZDP) is the protocol that the ZyXEL One Network (ZON) utility uses for discovering and configuring ZDP-aware ZyXEL devices in the same broadcast domain as the computer on which ZON is installed.
Enable	Select to activate ZDP discovery on the USG.
Smart Connect	Smart Connect uses Link Layer Discovery Protocol (LLDP) for discovering and configuring LLDP-aware devices in the same broadcast domain as the USG that you're logged into using the web configurator.
Enable	Select to activate LLDP discovery on the USG. See also Monitor > System Status > Ethernet Discovery.

Table 256 Configuration > System > ZON

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

31

Log and Report

31.1 Overview

Use these screens to configure daily reporting and log settings.

31.1.1 What You Can Do In this Chapter

- Use the Email Daily Report screen (Section 31.2 on page 590) to configure where and how to send daily reports and what reports to send.
- Use the Log Setting screens (Section 31.3 on page 592) to specify settings for recording log messages and alerts, e-mailing them, storing them on a connected USB storage device, and sending them to remote syslog servers.

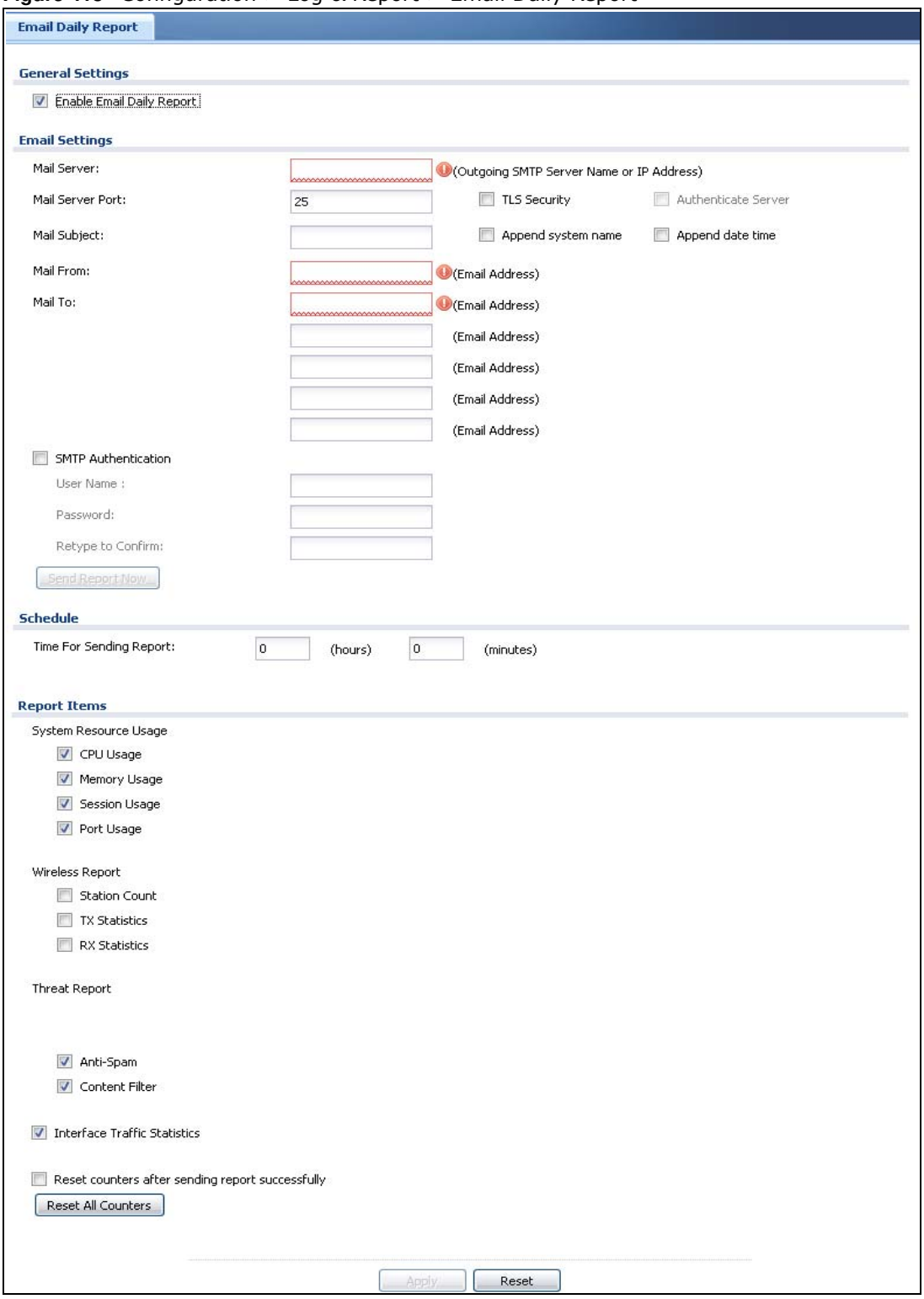
31.2 Email Daily Report

Use the Email Daily Report screen to start or stop data collection and view various statistics about traffic passing through your USG.

Note: Data collection may decrease the USG's traffic throughput rate.

Click Configuration > Log & Report > Email Daily Report to display the following screen. Configure this screen to have the USG e-mail you system statistics every day.

Figure 418 Configuration > Log & Report > Email Daily Report



The following table describes the labels in this screen.

Table 257 Configuration > Log & Report > Email Daily Report

LABEL	DESCRIPTION
Enable Email Daily Report	Select this to send reports by e-mail every day.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
TLS Security	Select Transport Layer Security (TLS) if you want encrypted communications between the mail server and the USG.
Authenticate Server	If you choose TLS Security, you may also select this to have the USG authenticate the mail server in the TLS handshake.
Mail Subject	Type the subject line for outgoing e-mail from the USG.
Append system name	Select Append system name to add the USG's system name to the subject.
Append date time	Select Append date time to add the USG's system date and time to the subject.
Mail From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Mail To	Type the e-mail address (or addresses) to which the outgoing e-mail is delivered.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the SMTP Authentication check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the SMTP Authentication check box. Type the password to provide to the SMTP server when the log is e-mailed.
Retype to Confirm	Type the password again to make sure that you have entered is correctly.
Send Report Now	Click this button to have the USG send the daily e-mail report immediately.
Time for sending report	Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
Report Items	Select the information to include in the report. Types of information include System Resource Usage, Wireless Report, Threat Report, and Interface Traffic Statistics. Select Reset counters after sending report successfully if you only want to see statistics for a 24 hour period.
Reset All Counters	Click this to discard all report data and start all of the counters over at zero.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

31.3 Log Setting Screens

The Log Setting screens control log messages and alerts. A log message stores the information for viewing or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The USG provides a system log and supports e-mail profiles and remote syslog servers. View the system log in the MONITOR > Log screen. Use the e-mail profiles to mail log messages to the

specific destinations. You can also have the USG store system logs on a connected USB storage device. The other four logs are stored on specified syslog servers.

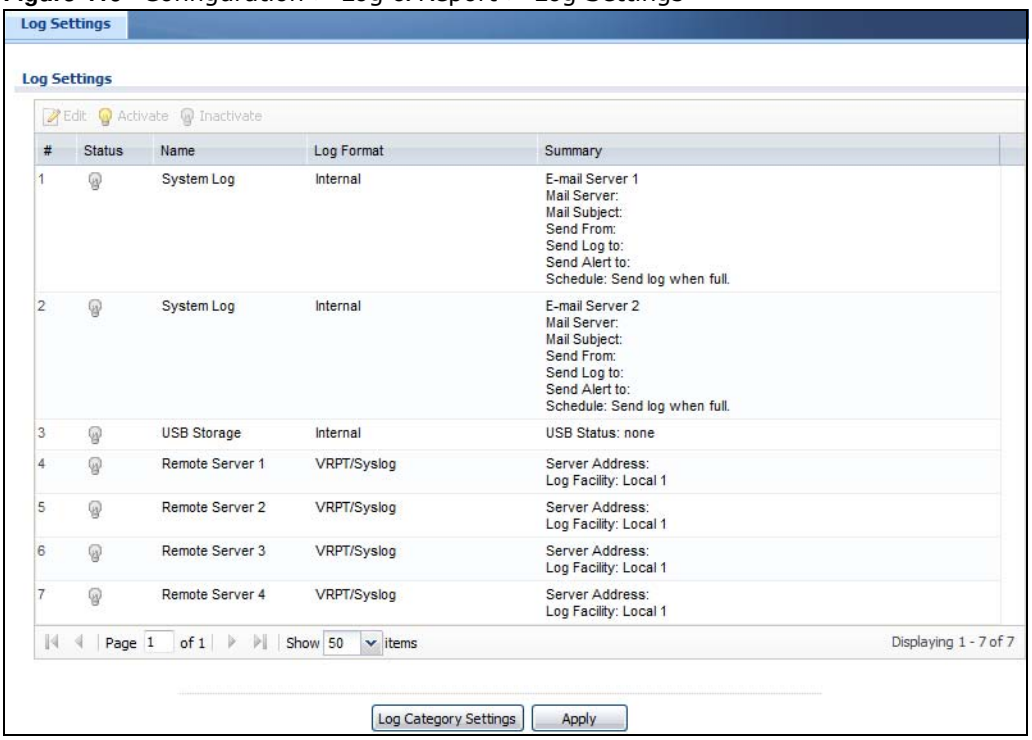
The Log Setting screens control what information the USG saves in each log. You can also specify which log messages to e-mail for the system log, and where and how often to e-mail them. These screens also set for which events to generate alerts and where to email the alerts.

The first Log Setting screen provides a settings summary. Use the Edit screens to configure settings such as log categories, e-mail addresses, and server names for any log. Use the Log Category Settings screen to edit what information is included in the system log, USB storage, e-mail profiles, and remote servers.

31.3.1 Log Settings

To access this screen, click Configuration > Log & Report > Log Settings.

Figure 419 Configuration > Log & Report > Log Settings



The following table describes the labels in this screen.

Table 258 Configuration > Log & Report > Log Settings

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This field is a sequential value, and it is not associated with a specific log.
Name	This field displays the type of log setting entry (system log, logs stored on a USB storage device connected to the USG, or one of the remote servers).

Table 258 Configuration > Log & Report > Log Settings (continued)

LABEL	DESCRIPTION
Log Format	This field displays the format of the log. Internal - system log; you can view the log on the View Log tab. VRPT/ Syslog - ZyXEL's Vantage Report, syslog-compatible format. CEF/ Syslog - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log. Please see Section 31.3.2 on page 594 for more information.
Log Category Settings	Click this button to open the Log Category Settings Edit screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

31.3.2 Edit System Log Settings

The Log Settings Edit screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Go to the Log Settings screen (see Section 31.3.1 on page 593), and click the system log Edit icon.

Figure 420 Configuration > Log & Report > Log Setting > Edit (System Log)

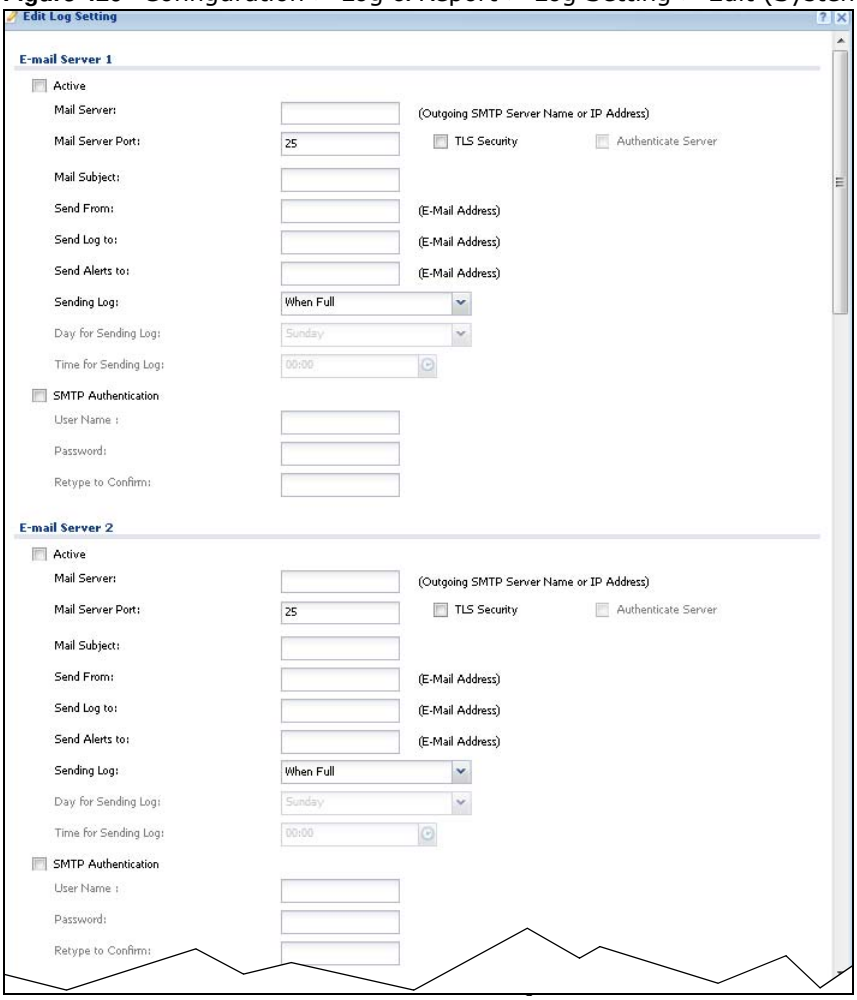
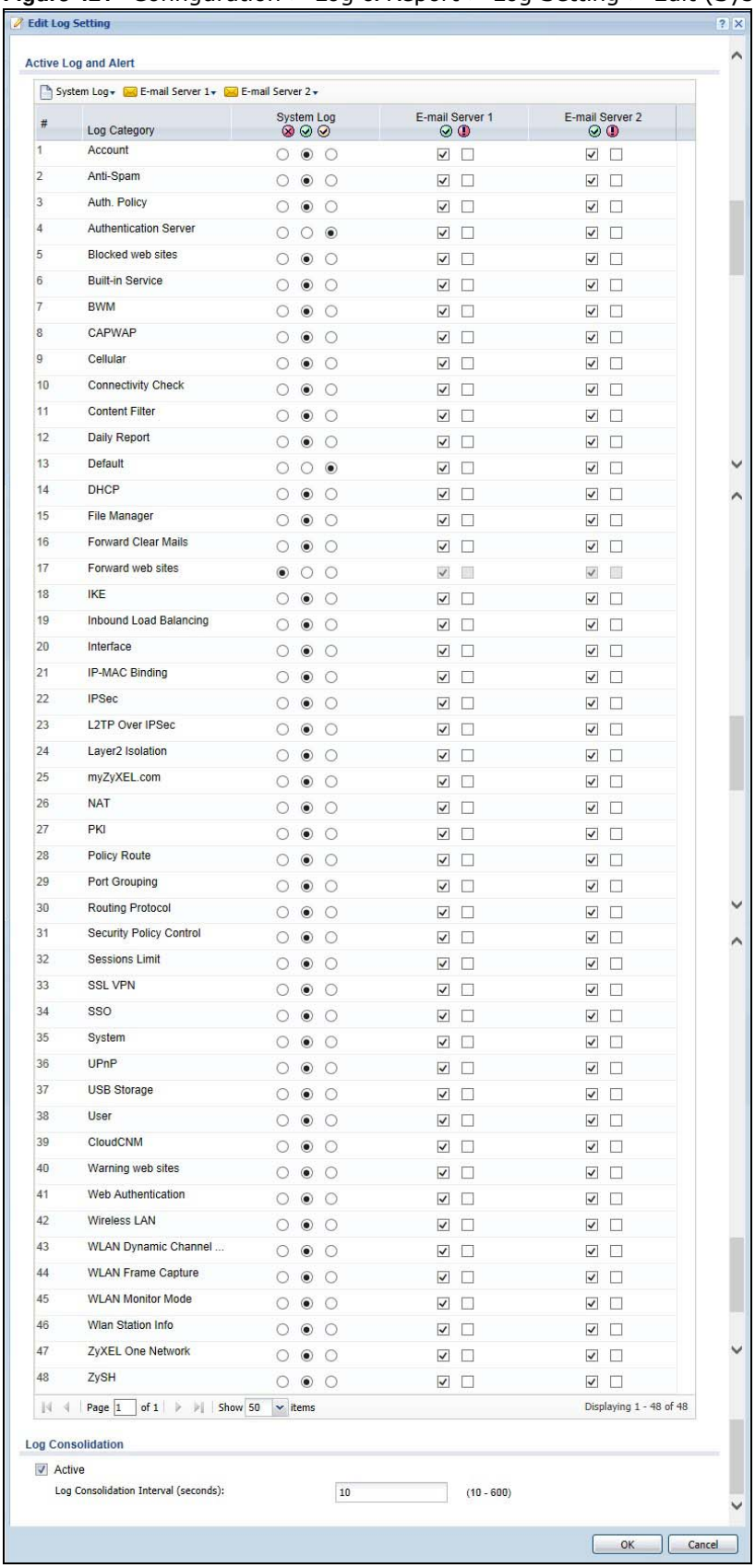


Figure 421 Configuration > Log & Report > Log Setting > Edit (System Log)



The following table describes the labels in this screen.

Table 259 Configuration > Log & Report > Log Setting > Edit (System Log)

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the Active Log and Alert section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Type the subject line for the outgoing e-mail.
Send From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Send Log To	Type the e-mail address to which the outgoing e-mail is delivered.
Send Alerts To	Type the e-mail address to which alerts are delivered.
Sending Log	Select how often log information is e-mailed. Choices are: When Full, Hourly and When Full, Daily and When Full, and Weekly and When Full.
Day for Sending Log	This field is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed.
Time for Sending Log	This field is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the SMTP Authentication check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the SMTP Authentication check box. Type the password to provide to the SMTP server when the log is e-mailed.
Retype to Confirm	Type the password again to make sure that you have entered is correctly.
Active Log and Alert	
System Log	Use the System Log drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. enable normal logs (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the USG will e-mail logs to them. enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories. The USG does not e-mail debugging information, even if this setting is selected.
E-mail Server 1	Use the E-Mail Server 1 drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the System Log drop-down list to disable all logs overrides your e-mail server 1 settings. enable normal logs (green check mark) - e-mail log messages for all categories to e-mail server 1. enable alert logs (red exclamation point) - e-mail alerts for all categories to e-mail server 1.

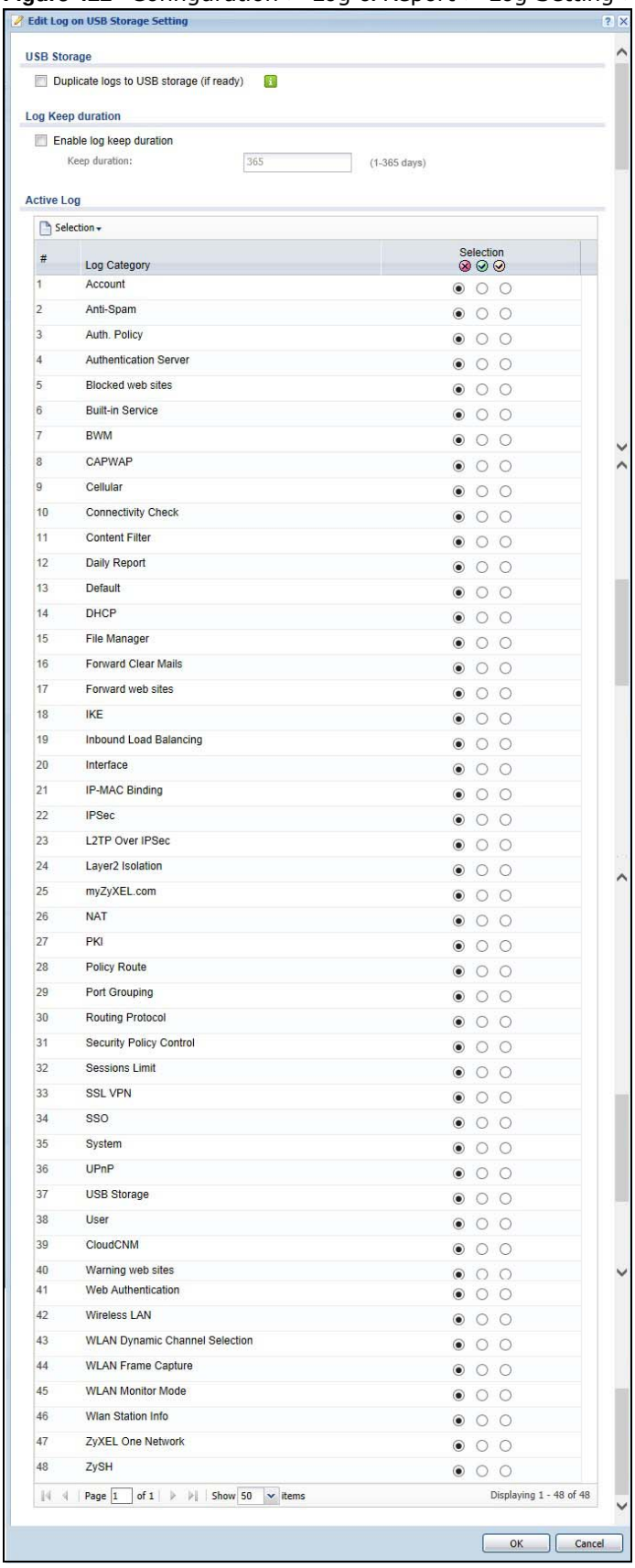
Table 259 Configuration > Log & Report > Log Setting > Edit (System Log) (continued)

LABEL	DESCRIPTION
E-mail Server 2	Use the E-Mail Server 2 drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the System Log drop-down list to disable all logs overrides your e-mail server 2 settings. enable normal logs (green check mark) - e-mail log messages for all categories to e-mail server 2. enable alert logs (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
System log	Select which events you want to log by Log Category. There are three choices: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - create log messages and alerts from this category enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information from this category; the USG does not e-mail debugging information, however, even if this setting is selected.
E-mail Server 1	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in E-Mail Server 1. The USG does not e-mail debugging information, even if it is recorded in the System log.
E-mail Server 2	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in E-Mail Server 2. The USG does not e-mail debugging information, even if it is recorded in the System log.
Log Consolidation	
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified Log Consolidation Interval. In the View Log tab, the text "[count=*x*]", where *x* is the number of original log messages, is appended at the end of the Message field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=*x*]", where *x* is the number of original log messages, appended at the end of the Message field.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

31.3.3 Edit Log on USB Storage Setting

The Edit Log on USB Storage Setting screen controls the detailed settings for saving logs to a connected USB storage device. Go to the Log Setting Summary screen (see Section 31.3.1 on page 593), and click the USB storage Edit icon.

Figure 422 Configuration > Log & Report > Log Setting > Edit (USB Storage)



The following table describes the labels in this screen.

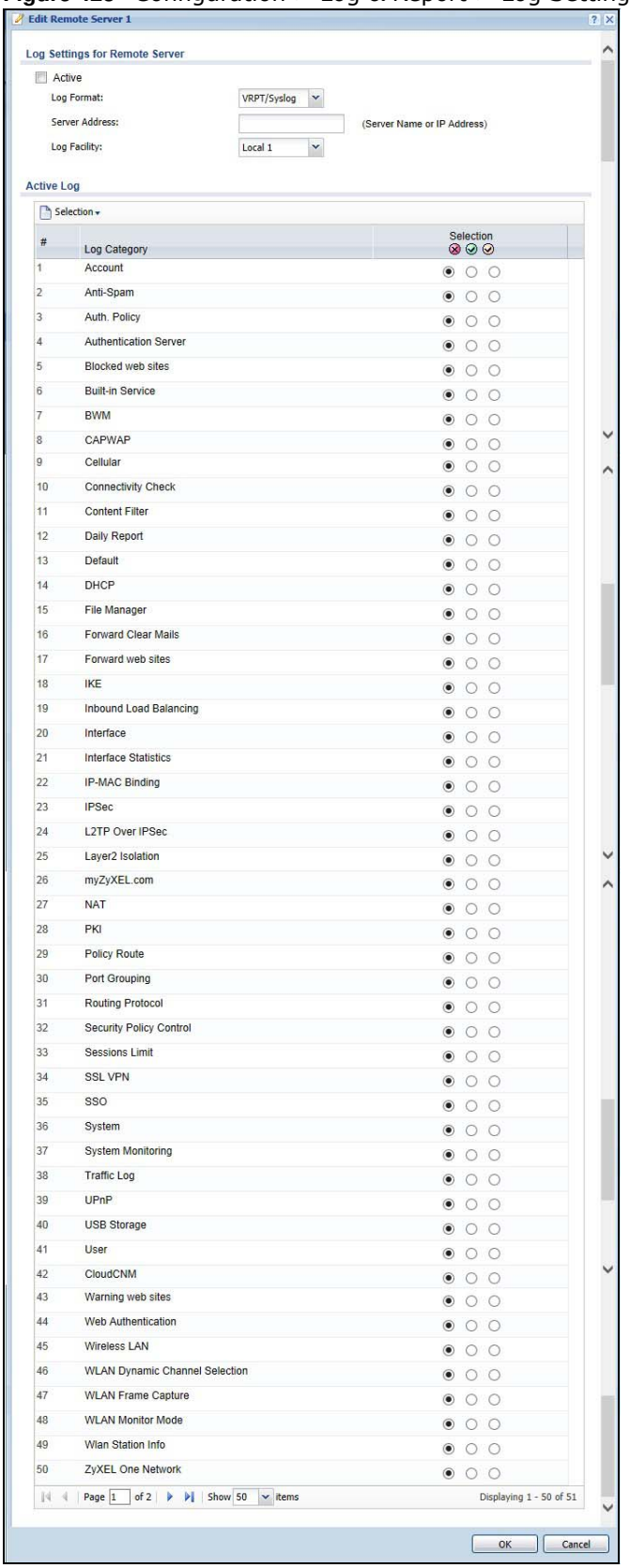
Table 260 Configuration > Log & Report > Log Setting > Edit (USB Storage)

LABEL	DESCRIPTION
USB Storage	
Duplicate logs to USB storage (if ready)	Select this to have the USG save a copy of its system logs to a connected USB storage device. Use the Active Log section to specify what kinds of messages to include.
Log Keep duration	
Enable log keep duration	Select this and enter the number of days you want the USG to store a log in Keep duration before deleting it forever from the USG.
Active Log	
Selection	Use the Selection drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not send the remote server logs for any log category. enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories. enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific entry.
Log Category	This field displays each category of messages. The Default category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each Log Category (except All Logs; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - log regular information and alerts from this category enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

31.3.4 Edit Remote Server Log Settings

The Log Settings Edit screen controls the detailed settings for each log in the remote server (syslog). Go to the Log Settings Summary screen (see Section 31.3.1 on page 593), and click a remote server Edit icon.

Figure 423 Configuration > Log & Report > Log Setting > Edit (Remote Server)



The following table describes the labels in this screen.

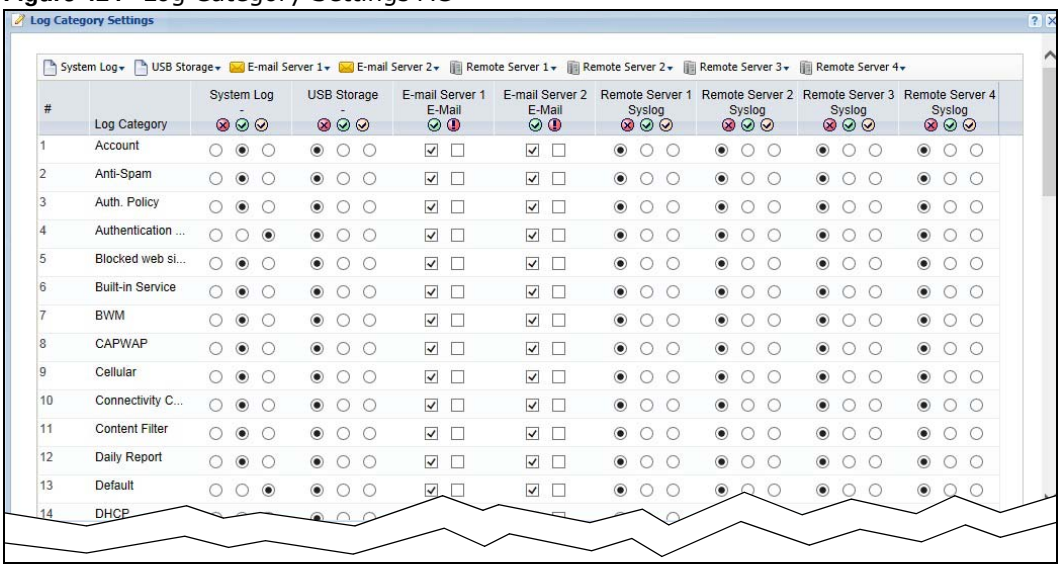
Table 261 Configuration > Log & Report > Log Setting > Edit (Remote Server)

LABEL	DESCRIPTION
Log Settings for Remote Server	
Active	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the Active Log section.
Log Format	This field displays the format of the log information. It is read-only. VRPT/ Syslog - ZyXEL's Vantage Report, syslog-compatible format. CEF/ Syslog - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Selection	Use the Selection drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not send the remote server logs for any log category. enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories. enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each Log Category (except All Logs; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - log regular information and alerts from this category enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

31.3.5 Log Category Settings Screen

The Log Category Settings screen allows you to view and to edit what information is included in the system log, USB storage, e-mail profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is e-mailed or remote server names). To access this screen, go to the Log Settings screen (see Section 31.3.1 on page 593), and click the Log Category Settings button.

Figure 424 Log Category Settings AC



This screen provides a different view and a different way of indicating which messages are included in each log and each alert. Please see Section 31.3.2 on page 594, where this process is discussed. (The Default category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 262 Configuration > Log & Report > Log Setting > Log Category Settings

LABEL	DESCRIPTION
System Log	Use the System Log drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. enable normal logs (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the USG will e-mail logs to them. enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories. The USG does not e-mail debugging information, even if this setting is selected.
USB Storage	Use the USB Storage drop-down list to change the log settings for saving logs to a connected USB storage device. disable all logs (red X) - do not log any information for any category to a connected USB storage device. enable normal logs (green check mark) - create log messages and alerts for all categories and save them to a connected USB storage device. enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories and save them to a connected USB storage device.

Table 262 Configuration > Log & Report > Log Setting > Log Category Settings (continued)

LABEL	DESCRIPTION
E-mail Server 1	Use the E-Mail Server 1 drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the System Log drop-down list to disable all logs overrides your e-mail server 1 settings. enable normal logs (green check mark) - e-mail log messages for all categories to e-mail server 1. enable alert logs (red exclamation point) - e-mail alerts for all categories to e-mail server 1.
E-mail Server 2	Use the E-Mail Server 2 drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the System Log drop-down list to disable all logs overrides your e-mail server 2 settings. enable normal logs (green check mark) - e-mail log messages for all categories to e-mail server 2. enable alert logs (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
Remote Server 1~4	For each remote server, use the Selection drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not send the remote server logs for any log category. enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories. enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
System Log	Select which events you want to log by Log Category. There are three choices: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - create log messages and alerts from this category enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information from this category; the USG does not e-mail debugging information, however, even if this setting is selected.
USB Storage	Select which event log categories to save to a connected USB storage device. There are three choices: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - save log messages and alerts from this category enable normal logs and debug logs (yellow check mark) - save log messages, alerts, and debugging information from this category.
E-mail Server 1 E-mail	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in E-Mail Server 1. The USG does not e-mail debugging information, even if it is recorded in the System log.

Table 262 Configuration > Log & Report > Log Setting > Log Category Settings (continued)

LABEL	DESCRIPTION
E-mail Server 2 E-mail	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in E-Mail Server 2. The USG does not e-mail debugging information, even if it is recorded in the System log.
Remote Server 1~4	For each remote server, select what information you want to log from each Log Category (except All Logs; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - log regular information and alerts from this category enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

32

File Manager

32.1 Overview

Configuration files define the USG's settings. Shell scripts are files of commands that you can store on the USG and run when you need them. You can apply a configuration file or run a shell script without the USG restarting. You can store multiple configuration files and shell script files on the USG. You can edit configuration files or shell scripts in a text editor and upload them to the USG. Configuration files use a .conf extension and shell scripts use a .zysh extension.

32.1.1 What You Can Do in this Chapter

- Use the Configuration File screen (see Section 32.2 on page 607) to store and name configuration files. You can also download configuration files from the USG to your computer and upload configuration files from your computer to the USG.
- Use the Firmware Package screen (see Section 32.3 on page 611) to check your current firmware version and upload firmware to the USG.
- Use the Shell Script screen (see Section 32.4 on page 613) to store, name, download, upload and run shell script files.

32.1.2 What you Need to Know

Configuration Files and Shell Scripts

When you apply a configuration file, the USG uses the factory default settings for any features that the configuration file does not include. When you run a shell script, the USG only applies the commands that it contains. Other settings do not change.

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

Figure 425 Configuration File / Shell Script: Example

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

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

Table 263 Configuration Files and Shell Scripts in the USG

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI Configuration mode. • Runs the commands in the configuration file.	• Goes into CLI Privilege mode. • Runs the commands in the shell script.

You have to run the example in Figure 425 on page 606 as a shell script because the first command is run in Privilege mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in Configuration mode.

Comments in Configuration Files or Shell Scripts

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

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

Note: "exit" or "!'" must follow sub commands if it is to make the USG exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

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

```
!
interface ge1
# this interface is a DHCP client
!
```

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

```
! this is from Joe
# on 2008/04/05
interface ge1
ip address dhcp
!
```

Errors in Configuration Files or Shell Scripts

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

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

32.2 The Configuration File Screen

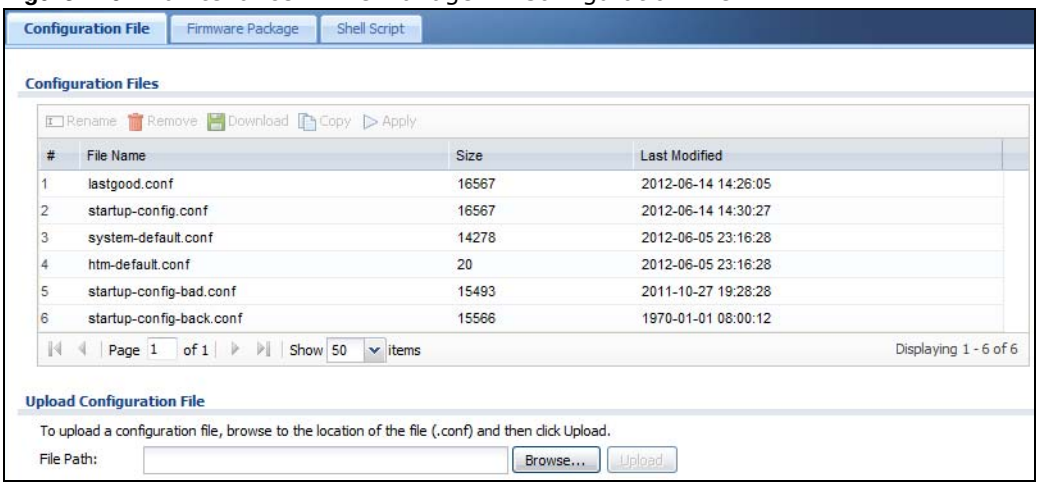
Click Maintenance > File Manager > Configuration File to open the Configuration File screen. Use the Configuration File screen to store, run, and name configuration files. You can also download configuration files from the USG to your computer and upload configuration files from your computer to the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

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

Configuration File Flow at Restart

- If there is not a `startup-config.conf` when you restart the USG (whether through a management interface or by physically turning the power off and back on), the USG uses the `system-default.conf` configuration file with the USG's default settings.
- If there is a `startup-config.conf`, the USG checks it for errors and applies it. If there are no errors, the USG uses it and copies it to the `lastgood.conf` configuration file as a back up file. If there is an error, the USG generates a log and copies the `startup-config.conf` configuration file to the `startup-config-bad.conf` configuration file and tries the existing `lastgood.conf` configuration file. If there isn't a `lastgood.conf` configuration file or it also has an error, the USG applies the `system-default.conf` configuration file.
- You can change the way the `startup-config.conf` file is applied. Include the `setenv-startup stop-on-error off` command. The USG ignores any errors in the `startup-config.conf` file and applies all of the valid commands. The USG still generates a log for any errors.

Figure 426 Maintenance > File Manager > Configuration File



Do not turn off the USG while configuration file upload is in progress.

The following table describes the labels in this screen.

Table 264 Maintenance > File Manager > Configuration File

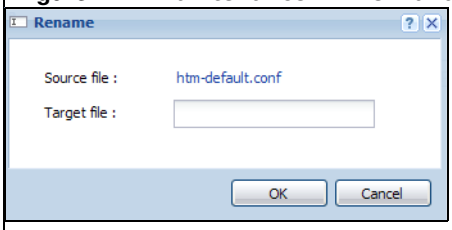
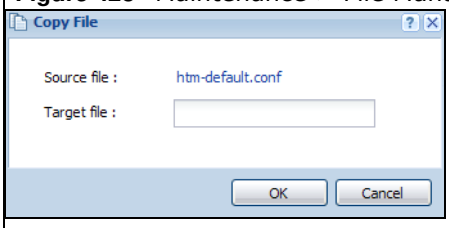
LABEL	DESCRIPTION
Rename	Use this button to change the label of a configuration file on the USG. You can only rename manually saved configuration files. You cannot rename the lastgood.conf, system-default.conf and startup-config.conf files. You cannot rename a configuration file to the name of another configuration file in the USG. Click a configuration file's row to select it and click Rename to open the Rename File screen. **Figure 427** Maintenance > File Manager > Configuration File > Rename  Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.
Remove	Click a configuration file's row to select it and click Remove to delete it from the USG. You can only delete manually saved configuration files. You cannot delete the system-default.conf, startup-config.conf and lastgood.conf files. A pop-up window asks you to confirm that you want to delete the configuration file. Click OK to delete the configuration file or click Cancel to close the screen without deleting the configuration file.
Download	Click a configuration file's row to select it and click Download to save the configuration to your computer.
Copy	Use this button to save a duplicate of a configuration file on the USG. Click a configuration file's row to select it and click Copy to open the Copy File screen. **Figure 428** Maintenance > File Manager > Configuration File > Copy  Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.

Table 264 Maintenance > File Manager > Configuration File (continued)

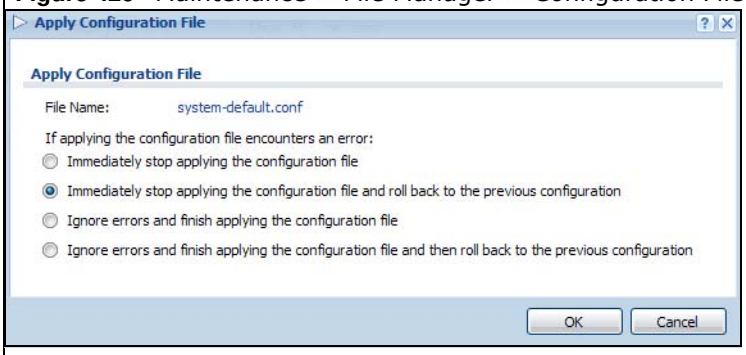
LABEL	DESCRIPTION
Apply	Use this button to have the USG use a specific configuration file. Click a configuration file's row to select it and click Apply to have the USG use that configuration file. The USG does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures. The following screen gives you options for what the USG is to do if it encounters an error in the configuration file. **Figure 429** Maintenance > File Manager > Configuration File > Apply  Immediately stop applying the configuration file - this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device. Immediately stop applying the configuration file and roll back to the previous configuration - this gets the USG started with a fully valid configuration file as quickly as possible. Ignore errors and finish applying the configuration file - this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the USG apply most of your configuration and you can refer to the logs for what to fix. Ignore errors and finish applying the configuration file and then roll back to the previous configuration - this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the USG with a fully valid configuration file. Click OK to have the USG start applying the configuration file or click Cancel to close the screen
#	This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific address. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.

Table 264 Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
File Name	This column displays the label that identifies a configuration file. You cannot delete the following configuration files or change their file names. The system-default.conf file contains the USG's default settings. Select this file and click Apply to reset all of the USG settings to the factory defaults. This configuration file is included when you upload a firmware package. The startup-config.conf file is the configuration file that the USG is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The USG applies configuration changes made in the Web Configurator to the configuration file when you click Apply or OK. It applies configuration changes made via commands when you use the write command. The lastgood.conf is the most recently used (valid) configuration file that was saved when the device last restarted. If you upload and apply a configuration file with an error, you can apply lastgood.conf to return to a valid configuration.
Size	This column displays the size (in KB) of a configuration file.
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File	The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your USG You cannot upload a configuration file named system-default.conf or lastgood.conf. If you upload startup-config.conf, it will replace the current configuration and immediately apply the new settings.
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. 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.

32.3 The Firmware Package Screen

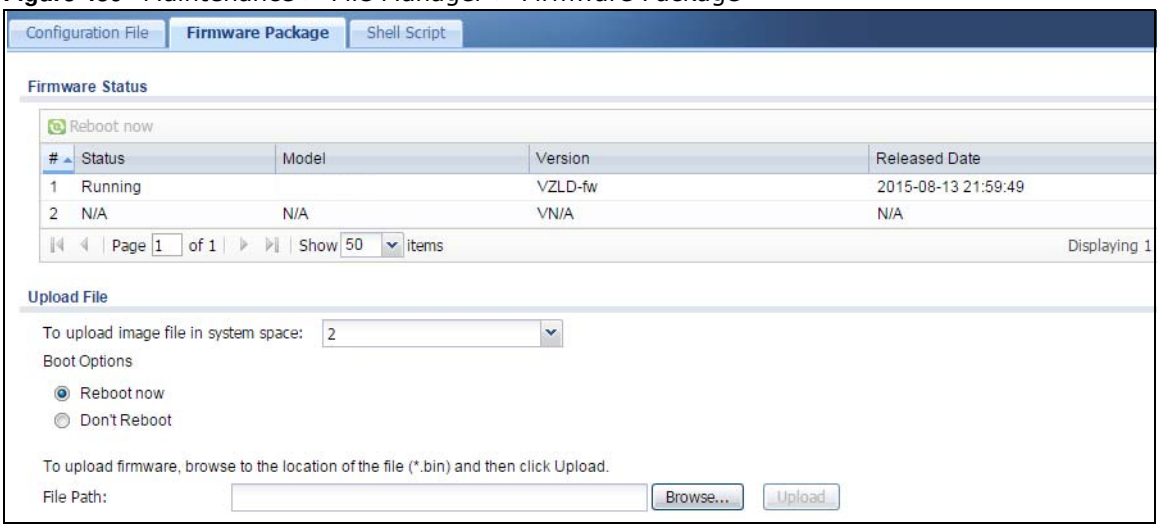
Click Maintenance > File Manager > Firmware Package to open the Firmware Package screen. Use the Firmware Package screen to check your current firmware version and upload firmware to the USG. You can upload firmware to be the Running firmware or Standby firmware.

Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

Find the firmware package at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "zywall.bin".

The firmware update can take up to five minutes. Do not turn off or reset the USG while the firmware update is in progress!

Figure 430 Maintenance > File Manager > Firmware Package



The following table describes the labels in this screen.

Table 265 Maintenance > File Manager > Firmware Package

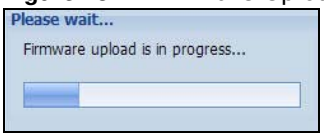
LABEL	DESCRIPTION
Firmware Status	
Reboot Now	Click the Reboot Now button to restart the USG. If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot. If you want the Standby firmware to be the Running firmware, then select the Standby firmware row and click Reboot Now. Wait a few minutes until the login screen appears. If the login screen does not appear, clear your browser cache and refresh the screen or type the IP address of the USG in your Web browser again. You can also use the CLI command `reboot` to restart the USG.
#	This displays the system space (partition) index number where the firmwarm is located. The firmware can be either Standby or Running; only one firmware can be running at any one time.
Status	This indicates whether the firmware is Running, or not running but already uploaded to the USG and is on Standby. It displays N/A if there is no firmware uploaded to that system space.
Model	This is the model name of the device which the firmware is running on.
Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
Upload File	
To upload image file in system space	Click the To upload image file in system space pull-down menu and select 1 or 2. The default is the Standby system space, so if you want to upload new firmware to be the Running firmware, then select the correct system space.
Boot Options	If you upload firmware to the Running system space, the USG will reboot automatically. If you upload firmware to the Standby system space, you have the option to Reboot now or Don't Reboot.
Reboot now	If you select Reboot now, then the firmware upload to Standby system space will become the Running firmware after you click Upload and the upload process completes.

Table 265 Maintenance > File Manager > Firmware Package (continued)

LABEL	DESCRIPTION
Don't Reboot	If you choose Don't Reboot, then the firmware upload to Standby system space will be the Standby firmware after you click Upload and the upload process completes. If you want the Standby firmware to be the Running firmware, then select the Standby firmware row in Firmware Status and click Reboot Now.
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 a few minutes.

After you see the Firmware Upload in Process screen, wait a few minutes before logging into the USG again.

Figure 431 Firmware Upload In Process



Note: The USG automatically reboots after a successful upload.

The USG automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 432 Network



After five minutes, log in again and check your new firmware version in the Dashboard screen.

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

Figure 433 Firmware Upload Error



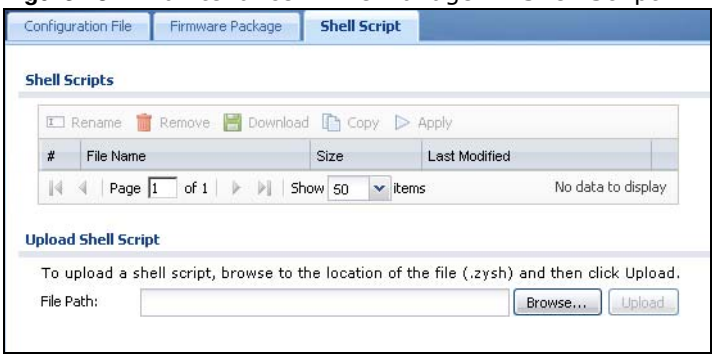
32.4 The Shell Script Screen

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

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

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

Figure 434 Maintenance > File Manager > Shell Script



Each field is described in the following table.

Table 266 Maintenance > File Manager > Shell Script

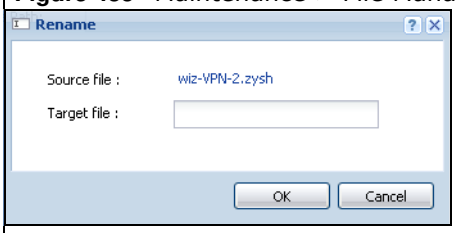
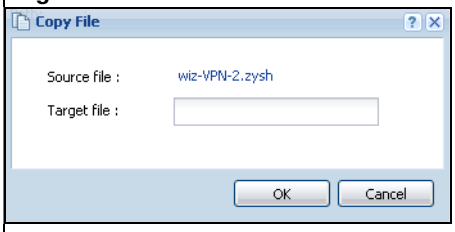
LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the USG. You cannot rename a shell script to the name of another shell script in the USG. Click a shell script's row to select it and click Rename to open the Rename File screen. **Figure 435** Maintenance > File Manager > Shell Script > Rename  Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.
Remove	Click a shell script file's row to select it and click Remove to delete the shell script file from the USG. A pop-up window asks you to confirm that you want to delete the shell script file. Click OK to delete the shell script file or click Cancel to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click Download to save the configuration to your computer.

Table 266 Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
Copy	Use this button to save a duplicate of a shell script file on the USG. Click a shell script file's row to select it and click Copy to open the Copy File screen. **Figure 436** Maintenance > File Manager > Shell Script > Copy  Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the USG use a specific shell script file. Click a shell script file's row to select it and click Apply to have the USG use that shell script file. You may need to wait awhile for the USG to finish applying the commands.
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your USG.
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .zysh file you want to upload.
Upload	Click Upload to begin the upload process. This process may take up to several minutes.

33

Diagnostics

33.1 Overview

Use the diagnostics screens for troubleshooting.

33.1.1 What You Can Do in this Chapter

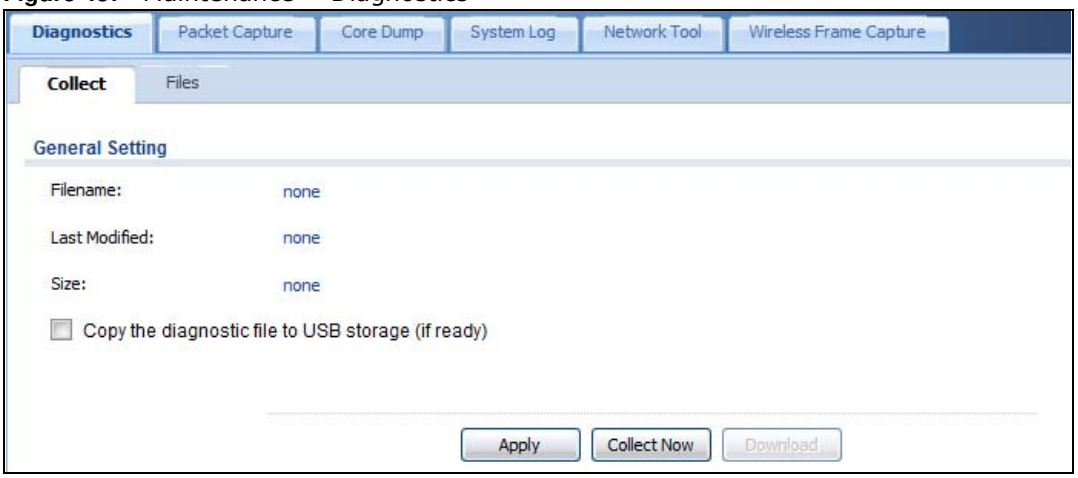
- Use the Diagnostics screen (see Section 33.2 on page 616) to generate a file containing the USG's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- Use the Packet Capture screens (see Section 33.3 on page 618) to capture packets going through the USG.
- The Core Dump screens (Section 33.4 on page 621) save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes) so you can send the file to customer support for troubleshooting.
- The System Log screens (Section 33.5 on page 623) download files of system logs from a connected USB storage device to your computer.
- Use the Network Tool screen (see Section 33.6 on page 623) to ping an IP address or trace the route packets take to a host.
- Use the Wireless Frame Capture screens (see Section 33.7 on page 624) to capture network traffic going through the AP interfaces connected to your USG.

33.2 The Diagnostic Screen

The Diagnostic screen provides an easy way for you to generate a file containing the USG's configuration and diagnostic information. You may need to send this file to customer support for troubleshooting.

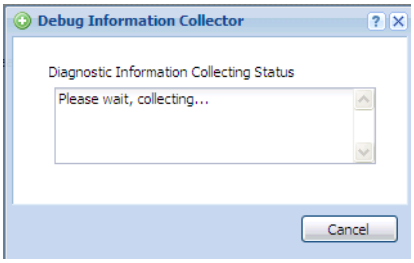
Click Maintenance > Diagnostics to open the Diagnostic screen.

Figure 437 Maintenance > Diagnostics



The following table describes the labels in this screen.

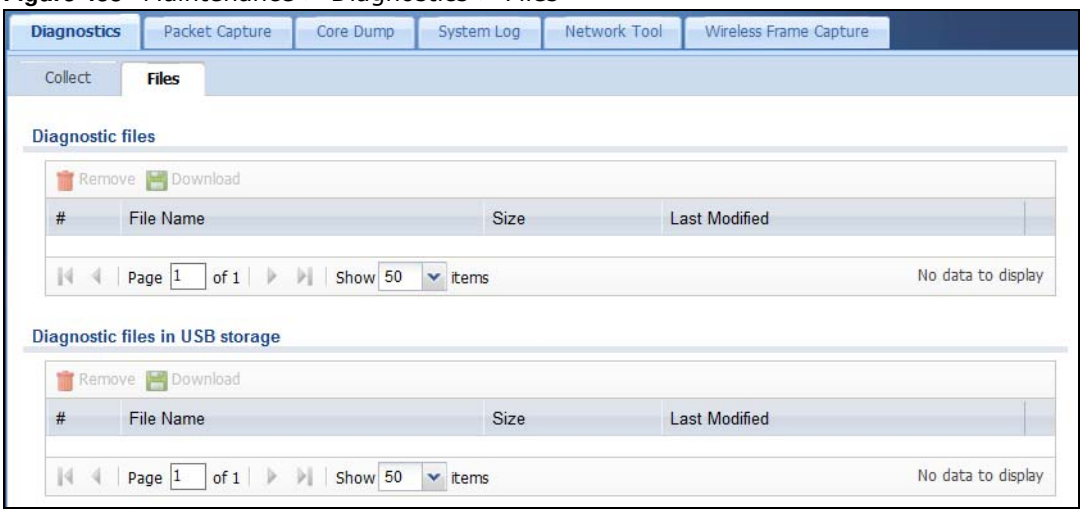
Table 267 Maintenance > Diagnostics

LABEL	DESCRIPTION
Filename	This is the name of the most recently created diagnostic file.
Last modified	This is the date and time that the last diagnostic file was created. The format is yyyy-mm-dd hh:mm:ss.
Size	This is the size of the most recently created diagnostic file.
Copy the diagnostic file to USB storage (if ready)	Select this to have the USG create an extra copy of the diagnostic file to a connected USB storage device.
Apply	Click Apply to save your changes.
Collect Now	Click this to have the USG create a new diagnostic file. Wait while information is collected. 
Download	Click this to save the most recent diagnostic file to a computer.

33.2.1 The Diagnostics Files Screen

Click Maintenance > Diagnostics > Files to open the diagnostic files screen. This screen lists the files of diagnostic information the USG has collected and stored on the USG or a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 438 Maintenance > Diagnostics > Files



The following table describes the labels in this screen.

Table 268 Maintenance > Diagnostics > Files

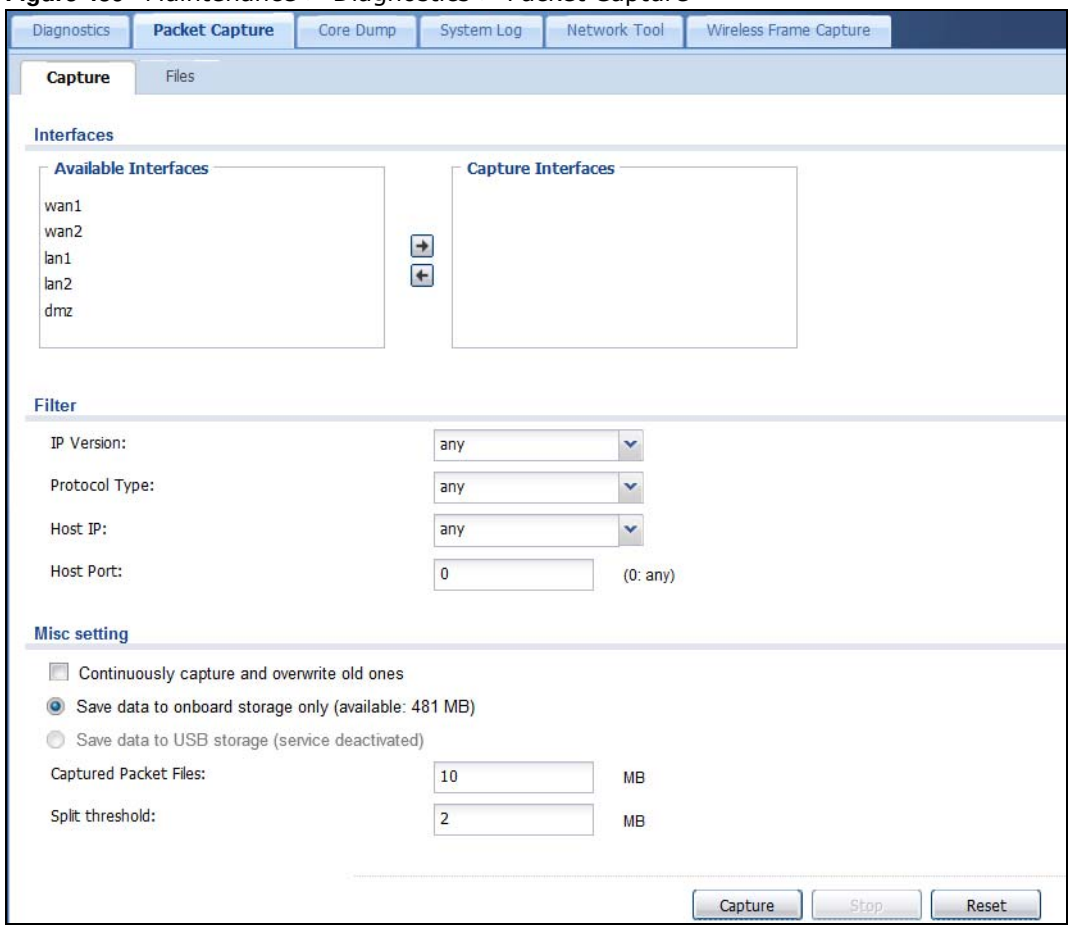
LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the USG. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

33.3 The Packet Capture Screen

Use this screen to capture network traffic going through the USG's interfaces. Studying these packet captures may help you identify network problems. Click Maintenance > Diagnostics > Packet Capture to open the packet capture screen.

Note: New capture files overwrite existing files of the same name. Change the File Suffix field's setting to avoid this.

Figure 439 Maintenance > Diagnostics > Packet Capture



The following table describes the labels in this screen.

Table 269 Maintenance > Diagnostics > Packet Capture

LABEL	DESCRIPTION
Interfaces	Enabled interfaces (except for virtual interfaces) appear under Available Interfaces. Select interfaces for which to capture packets and click the right arrow button to move them to the Capture Interfaces list. Use the [Shift] and/or [Ctrl] key to select multiple objects.
Filter	
IP Version	Select the version of IP for which to capture packets. Select any to capture packets for all IP versions.
Protocol Type	Select the protocol of traffic for which to capture packets. Select any to capture packets for all types of traffic.
Host IP	Select a host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.
Host Port	This field is configurable when you set the IP Type to any, tcp, or udp. Specify the port number of traffic to capture.
Misc setting	
Continuously capture and overwrite old ones	Select this to have the USG keep capturing traffic and overwriting old packet capture entries when the available storage space runs out.

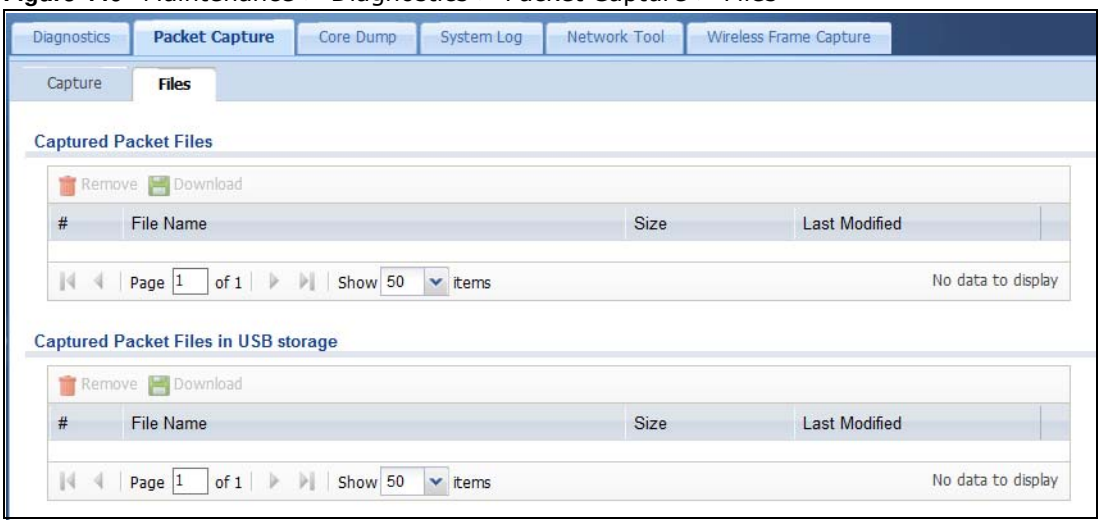
Table 269 Maintenance > Diagnostics > Packet Capture (continued)

LABEL	DESCRIPTION
Save data to onboard storage only	Select this to have the USG only store packet capture entries on the USG. The available storage size is displayed as well. Note: The USG reserves some onboard storage space as a buffer.
Save data to USB storage	Select this to have the USG store packet capture entries only on a USB storage device connected to the USG if the USG allows this. Status: Unused - the connected USB storage device was manually unmounted by using the Remove Now button or for some reason the USG cannot mount it. none - no USB storage device is connected. service deactivated - USB storage feature is disabled (in Configuration > Object > USB Storage), so the USG cannot use a connected USB device to store system logs and other diagnostic information. available - you can have the USG use the USB storage device. The available storage capacity also displays. Note: The USG reserves some USB storage space as a buffer.
Captured Packet Files	When saving packet captures only to the USG's onboard storage, specify a maximum limit in megabytes for the total combined size of all the capture files on the USG. When saving packet captures to a connected USB storage device, specify a maximum limit in megabytes for each capture file. Note: If you have existing capture files and have not selected the **Continuously capture and overwrite old ones** option, you may need to set this size larger or delete existing capture files. The valid range depends on the available onboard/USB storage size. The USG stops the capture and generates the capture file when either the file reaches this size or the time period specified in the Duration field expires.
Split threshold	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the USG starts another packet capture file.
Capture	Click this button to have the USG capture packets according to the settings configured in this screen. You can configure the USG while a packet capture is in progress although you cannot modify the packet capture settings. The USG's throughput or performance may be affected while a packet capture is in progress. After the USG finishes the capture it saves a separate capture file for each selected interface. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more packet captures will fail.
Stop	Click this button to stop a currently running packet capture and generate a separate capture file for each selected interface.
Reset	Click this button to return the screen to its last-saved settings.

33.3.1 The Packet Capture Files Screen

Click Maintenance > Diagnostics > Packet Capture > Files to open the packet capture files screen. This screen lists the files of packet captures stored on the USG or a connected USB storage device. You can download the files to your computer where you can study them using a packet analyzer (also known as a network or protocol analyzer) such as Wireshark.

Figure 440 Maintenance > Diagnostics > Packet Capture > Files



The following table describes the labels in this screen.

Table 270 Maintenance > Diagnostics > Packet Capture > Files

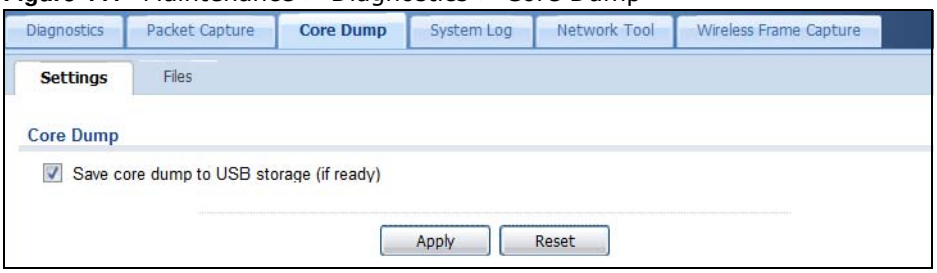
LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the USG or the connected USB storage device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file. The file name format is interface name-file suffix.cap.
Size	This column displays the size (in bytes) of a configuration file.
Last Modified	This column displays the date and time that the individual files were saved.

33.4 The Core Dump Screen

Use the Core Dump screen to have the USG save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes). You may need to send this file to customer support for troubleshooting.

Click Maintenance > Diagnostics > Core Dump to open the following screen.

Figure 441 Maintenance > Diagnostics > Core Dump



The following table describes the labels in this screen.

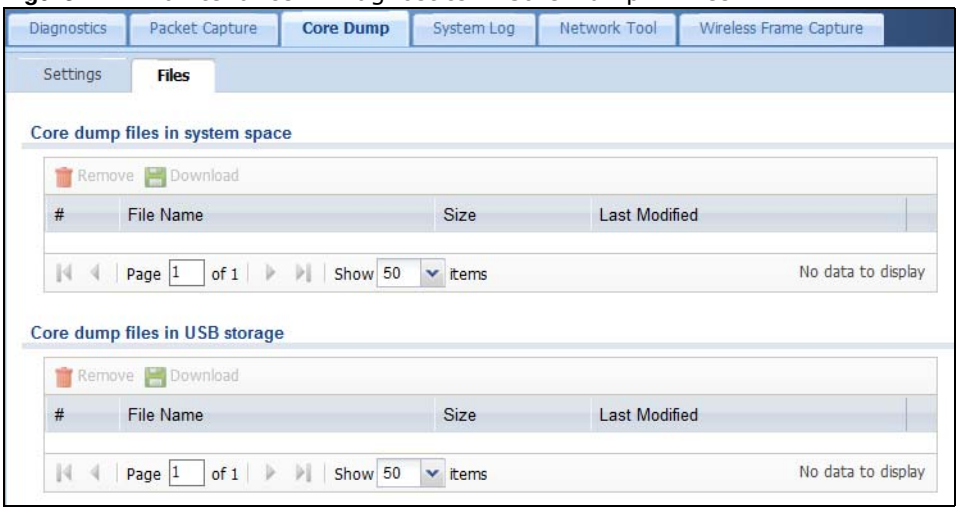
Table 271 Maintenance > Diagnostics > Core Dump

LABEL	DESCRIPTION
Save core dump to USB storage (if ready)	Select this to have the USG save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes). If you clear this option the USG only saves
Apply	Click Apply to save the changes.
Reset	Click Reset to return the screen to its last-saved settings.

33.4.1 The Core Dump Files Screen

Click Maintenance > Diagnostics > Core Dump > Files to open the core dump files screen. This screen lists the core dump files stored on the USG or a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 442 Maintenance > Diagnostics > Core Dump > Files



The following table describes the labels in this screen.

Table 272 Maintenance > Diagnostics > Core Dump > Files

LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the USG. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each core dump file entry. The total number of core dump files that you can save depends on the file sizes and the available flash storage space.

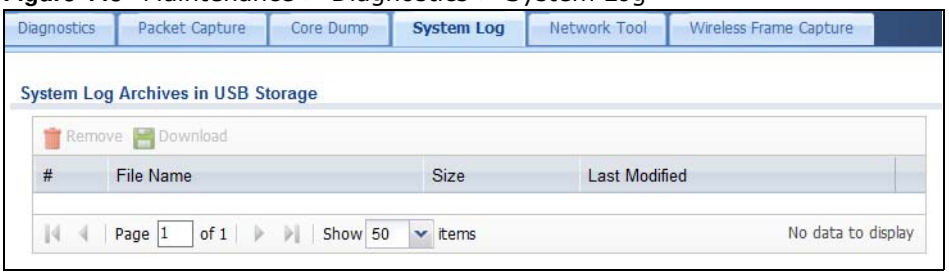
Table 272 Maintenance > Diagnostics > Core Dump > Files (continued)

LABEL	DESCRIPTION
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

33.5 The System Log Screen

Click Maintenance > Diagnostics > System Log to open the system log files screen. This screen lists the files of system logs stored on a connected USB storage device. The files are in comma separated value (csv) format. You can download them to your computer and open them in a tool like Microsoft's Excel.

Figure 443 Maintenance > Diagnostics > System Log



The following table describes the labels in this screen.

Table 273 Maintenance > Diagnostics > System Log

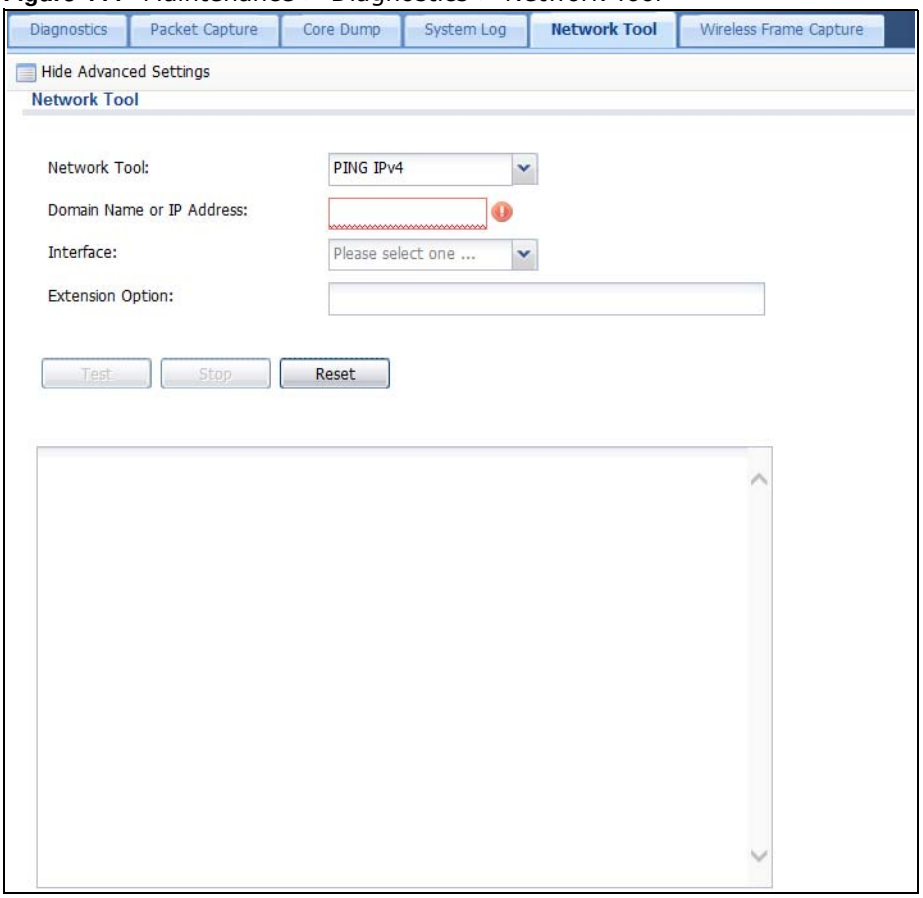
LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the USG. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

33.6 The Network Tool Screen

Use this screen to ping or traceroute an IP address.

Click Maintenance > Diagnostics > Network Tool to display this screen.

Figure 444 Maintenance > Diagnostics > Network Tool



The following table describes the labels in this screen.

Table 274 Maintenance > Diagnostics > Network Tool

LABEL	DESCRIPTION
Network Tool	Select PING IPv4 to ping the IP address that you entered. Select TRACEROUTE IPv4 to perform the traceroute function. This determines the path a packet takes to the specified computer.
Domain Name or IP Address	Type the IPv4 address of a computer that you want to perform ping or traceroute in order to test a connection.
Test	Click this button to start to ping or run a traceroute.
Stop	Click this button to terminate the current ping operation or traceroute.
Reset	Click this button to return the screen to its last-saved settings.

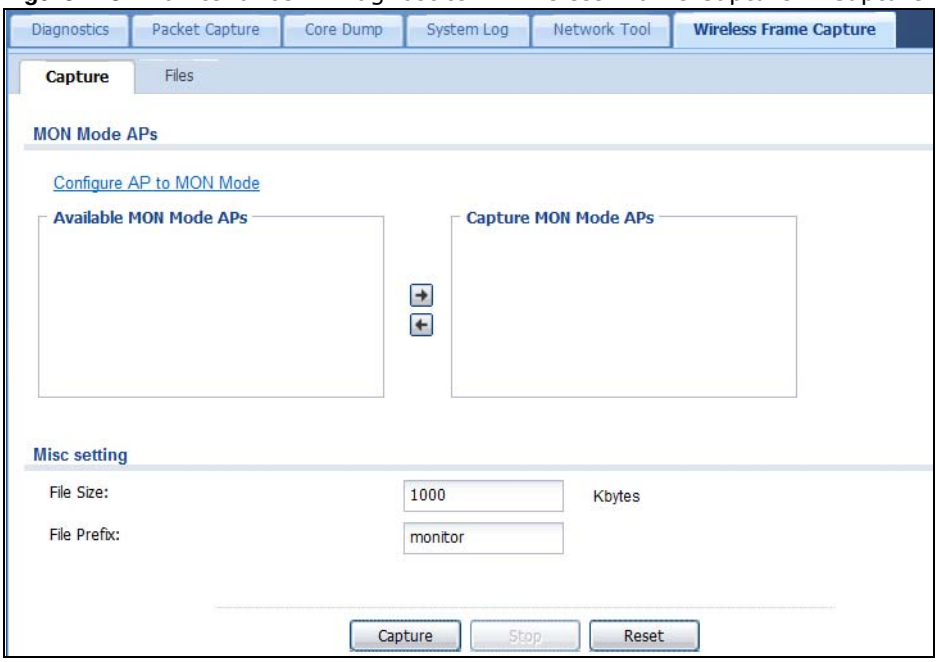
33.7 The Wireless Frame Capture Screen

Use this screen to capture wireless network traffic going through the AP interfaces connected to your USG. Studying these frame captures may help you identify network problems.

Click Maintenance > Diagnostics > Wireless Frame Capture to display this screen.

Note: New capture files overwrite existing files of the same name. Change the File Prefix field's setting to avoid this.

Figure 445 Maintenance > Diagnostics > Wireless Frame Capture > Capture



The following table describes the labels in this screen.

Table 275 Maintenance > Diagnostics > Wireless Frame Capture > Capture

LABEL	DESCRIPTION
MON Mode APs	
Configure AP to MON Mode	Click this to go the Configuration > Wireless > AP Management screen, where you can set one or more APs to monitor mode.
Available MON Mode APs	This column displays which APs on your wireless network are currently configured for monitor mode. Use the arrow buttons to move APs off this list and onto the Captured MON Mode APs list.
Capture MON Mode APs	This column displays the monitor-mode configured APs selected to for wireless frame capture.
Misc Setting	
File Size	Specify a maximum size limit in kilobytes for the total combined size of all the capture files on the USG, including any existing capture files and any new capture files you generate. Note: If you have existing capture files you may need to set this size larger or delete existing capture files. The valid range is 1 to 50000. The USG stops the capture and generates the capture file when either the file reaches this size.

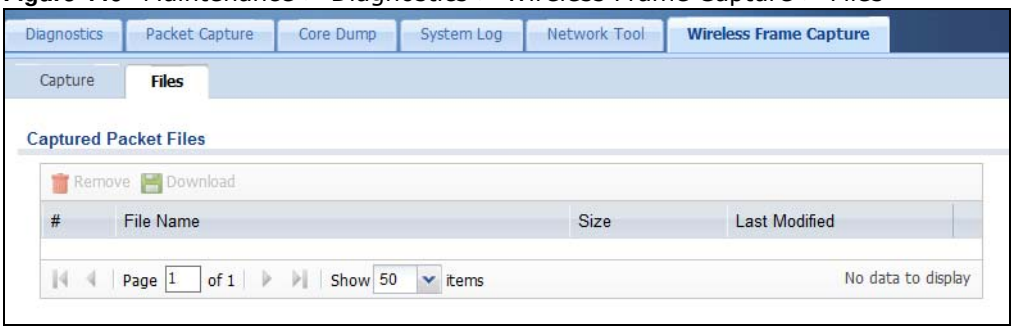
Table 275 Maintenance > Diagnostics > Wireless Frame Capture > Capture (continued)

LABEL	DESCRIPTION
File Prefix	Specify text to add to the front of the file name in order to help you identify frame capture files. You can modify the prefix to also create new frame capture files each time you perform a frame capture operation. Doing this does no overwrite existing frame capture files. The file format is: [file prefix].cap. For example, "monitor.cap".
Capture	Click this button to have the USG capture frames according to the settings configured in this screen. You can configure the USG while a frame capture is in progress although you cannot modify the frame capture settings. The USG's throughput or performance may be affected while a frame capture is in progress. After the USG finishes the capture it saves a combined capture file for all APs. The total number of frame capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more frame captures will fail.
Stop	Click this button to stop a currently running frame capture and generate a combined capture file for all APs.
Reset	Click this button to return the screen to its last-saved settings.

33.7.1 The Wireless Frame Capture Files Screen

Click Maintenance > Diagnostics > Wireless Frame Capture > Files to open this screen. This screen lists the files of wireless frame captures the USG has performed. You can download the files to your computer where you can study them using a packet analyzer (also known as a network or protocol analyzer) such as Wireshark.

Figure 446 Maintenance > Diagnostics > Wireless Frame Capture > Files



The following table describes the labels in this screen.

Table 276 Maintenance > Diagnostics > Wireless Frame Capture > Files

LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the USG. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.

Table 276 Maintenance > Diagnostics > Wireless Frame Capture > Files (continued)

LABEL	DESCRIPTION
File Name	This column displays the label that identifies the file. The file name format is interface name-file suffix.cap.
Size	This column displays the size (in bytes) of a configuration file.
Last Modified	This column displays the date and time that the individual files were saved.

34

Packet Flow Explore

34.1 Overview

Use this to get a clear picture on how the USG determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot any related problems.

34.1.1 What You Can Do in this Chapter

- Use the Routing Status screen (see Section 34.2 on page 628) to view the overall routing flow and each routing function's settings.
- Use the SNAT Status screen (see Section 34.3 on page 633) to view the overall source IP address conversion (SNAT) flow and each SNAT function's settings.

34.2 The Routing Status Screen

The Routing Status screen allows you to view the current routing flow and quickly link to specific routing settings. Click a function box in the Routing Flow section, the related routes (activated) will display in the Routing Table section. To access this screen, click Maintenance > Packet Flow Explore.

The order of the routing flow may vary depending on whether you:

- Select use policy route to override direct route in the CONFIGURATION > Network > Routing > Policy Route screen.
- Use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.
- Select use policy routes to control dynamic IPSec rules in the CONFIGURATION > VPN > IPSec VPN > VPN Connection screen.

Note: Once a packet matches the criteria of a routing rule, the USG takes the corresponding action and does not perform any further flow checking.

Figure 447 Maintenance > Packet Flow Explore > Routing Status (Direct Route)

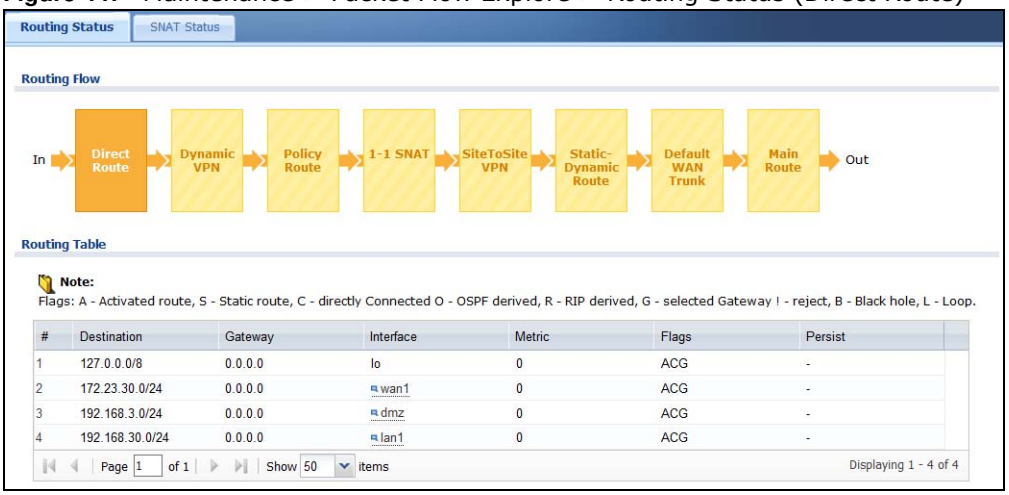


Figure 448 Maintenance > Packet Flow Explore > Dynamic VPN

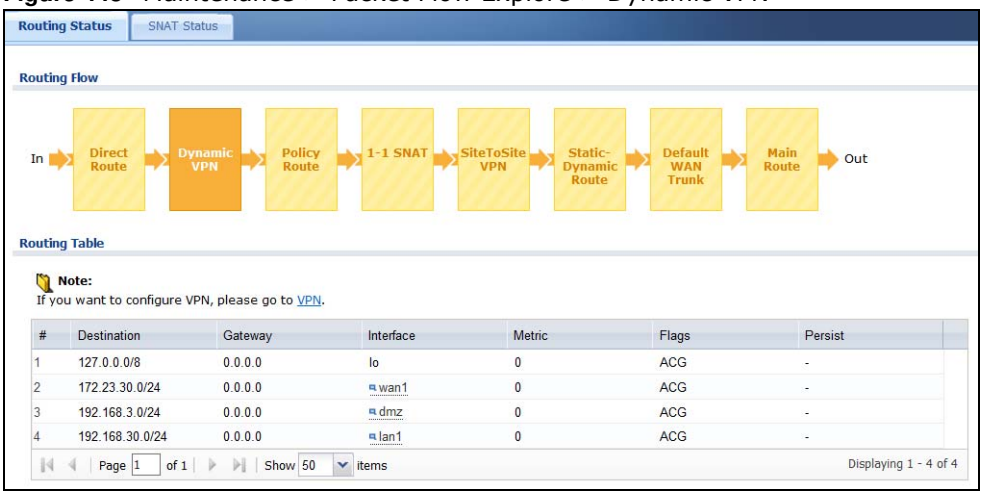


Figure 449 Maintenance > Packet Flow Explore > Routing Status (Policy Route)

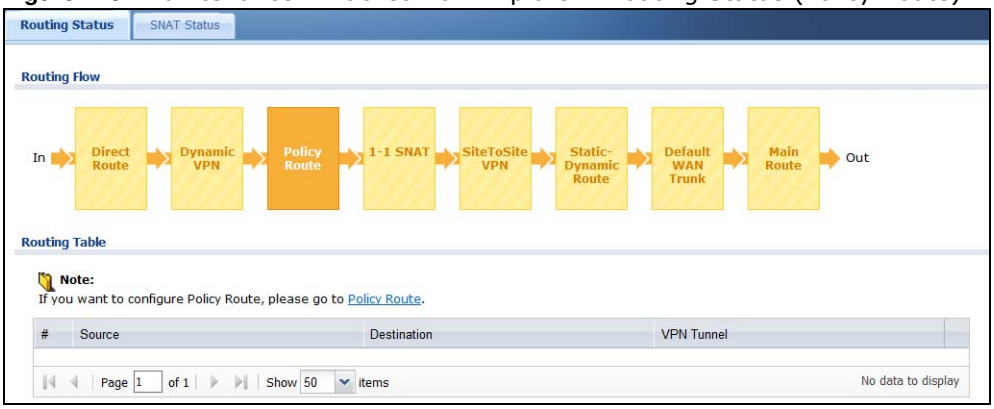


Figure 450 Maintenance > Packet Flow Explore > Routing Status (1-1 SNAT)

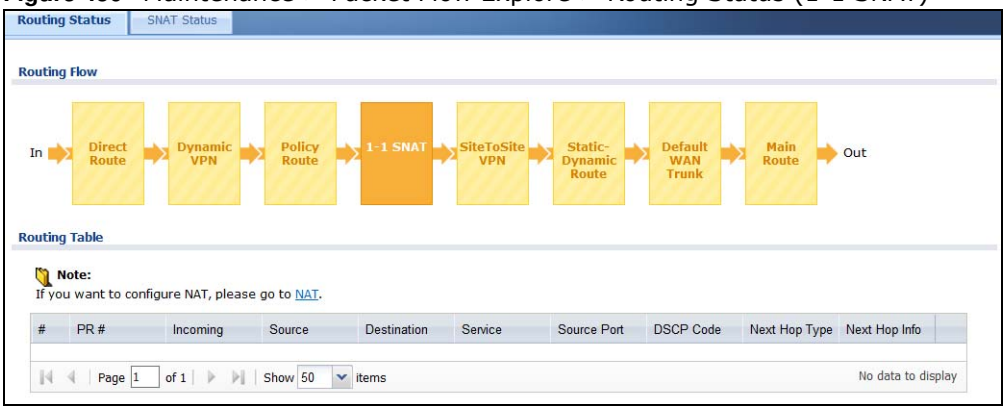


Figure 451 Maintenance > Packet Flow Explore > Routing Status (SiteToSite VPN)

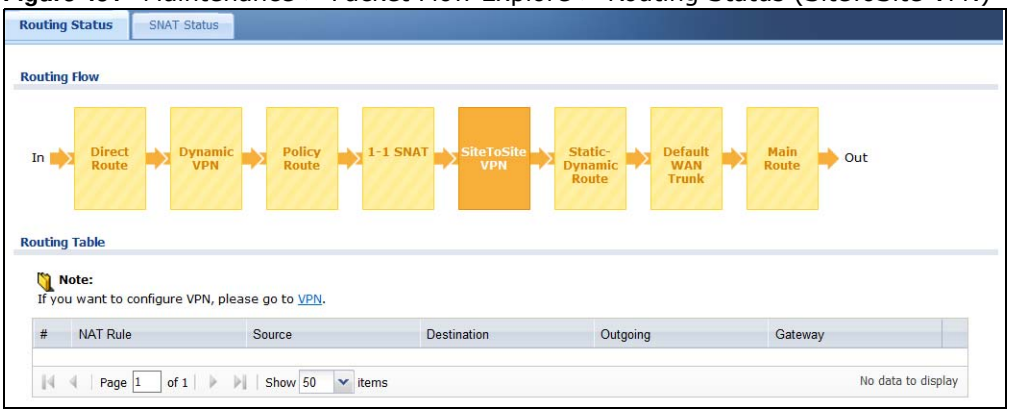


Figure 452 Maintenance > Packet Flow Explore > Routing Status (Dynamic VPN)

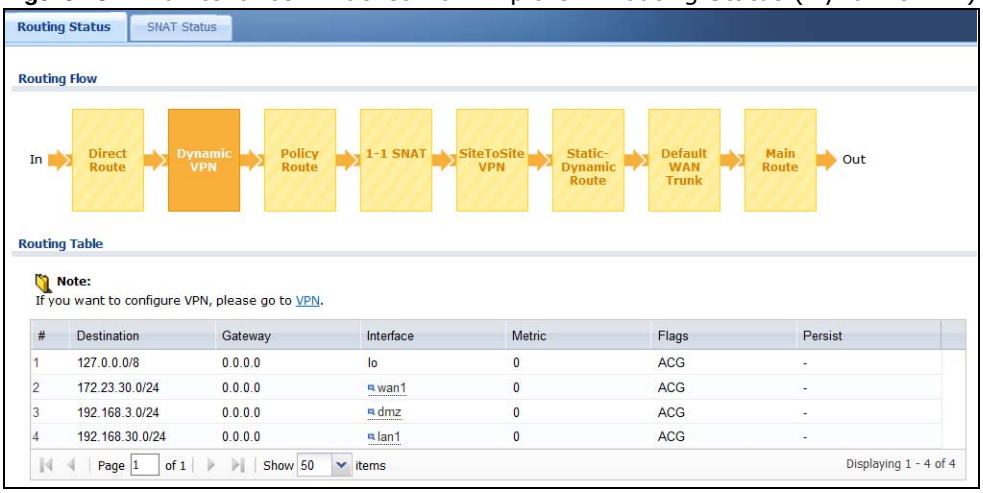


Figure 453 Maintenance > Packet Flow Explore > Routing Status (Static-Dynamic Route)

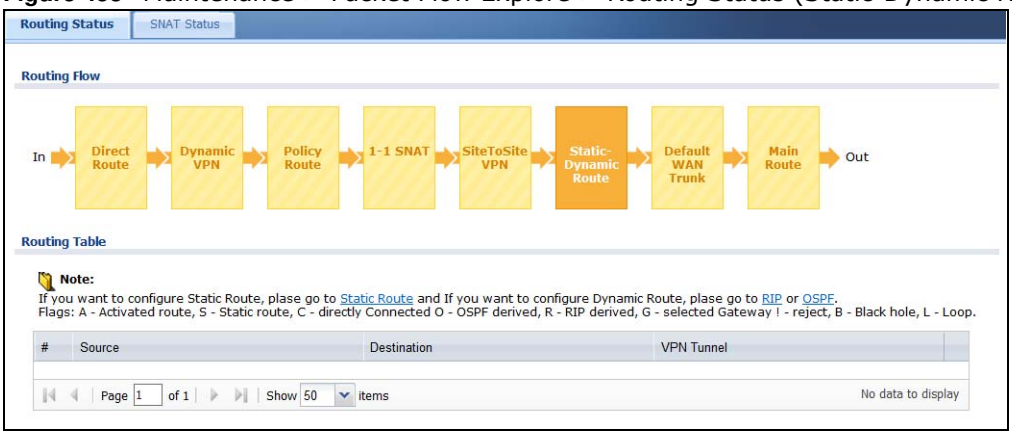


Figure 454 Maintenance > Packet Flow Explore > Routing Status (Default WAN Trunk)

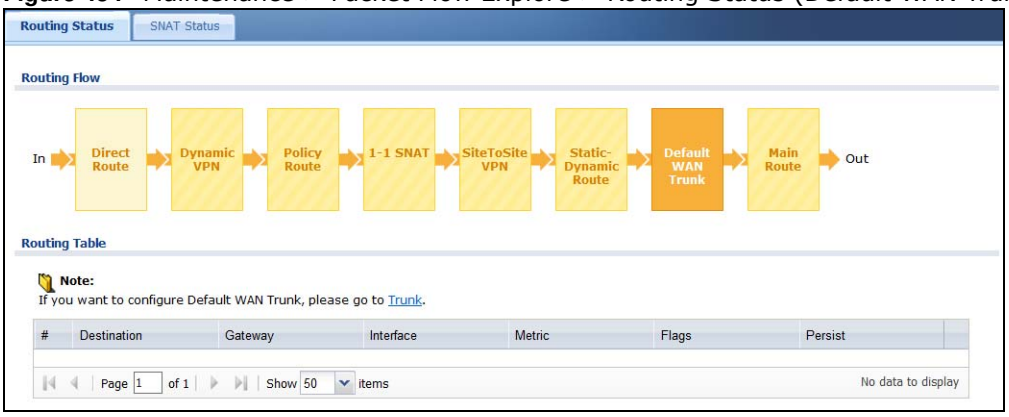
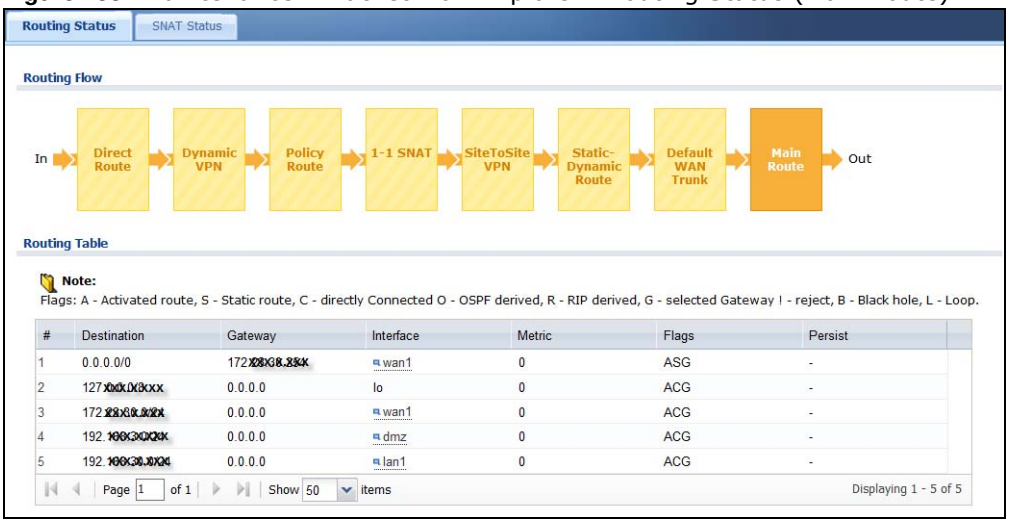


Figure 455 Maintenance > Packet Flow Explore > Routing Status (Main Route)



The following table describes the labels in this screen.

Table 277 Maintenance > Packet Flow Explore > Routing Status

LABEL	DESCRIPTION
Routing Flow	This section shows you the flow of how the USG determines where to route a packet. Click a function box to display the related settings in the Routing Table section.
Routing Table	This section shows the corresponding settings according to the function box you click in the Routing Flow section.
The following fields are available if you click Direct Route, Static-Dynamic Route, or Main Route in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Destination	This is the destination IP address of a route.
Gateway	This is the IP address of the next-hop gateway or the interface through which the traffic is routed.
Interface	This is the name of an interface associated with the route.
Metric	This is the route's priority among the displayed routes.
Flags	This indicates additional information for the route. The possible flags are: • A - this route is currently activated • S - this is a static route • C - this is a direct connected route • O - this is a dynamic route learned through OSPF • R - this is a dynamic route learned through RIP • G - the route is to a gateway (router) in the same network. • ! - this is a route which forces a route lookup to fail. • B - this is a route which discards packets. • L - this is a recursive route.
Persist	This is the remaining time of a dynamically learned route. The USG removes the route after this time period is counted down to zero.
The following fields are available if you click Policy Route in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
PR #	This is the number of an activated policy route. If you have configured a schedule for the route, this screen only displays the route at the scheduled time.
Incoming	This is the interface on which the packets are received.
Source	This is the source IP address(es) from which the packets are sent.
Destination	This is the destination IP address(es) to which the packets are transmitted.
Service	This is the name of the service object. any means all services.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. See Section 10.2 on page 229 for more information.
Next Hop Type	This is the type of the next hop to which packets are directed.
Next Hop Info	• This is the main route if the next hop type is Auto. • This is the interface name and gateway IP address if the next hop type is Interface / GW. • This is the tunnel name if the next hop type is VPN Tunnel. • This is the trunk name if the next hop type is Trunk.
The following fields are available if you click 1-1 SNAT in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated 1:1 or Many 1:1 NAT rule in the NAT table.
Source	This is the original source IP address(es). any means any IP address.
Destination	This is the original destination IP address(es). any means any IP address.

Table 277 Maintenance > Packet Flow Explore > Routing Status (continued)

LABEL	DESCRIPTION
Outgoing	This is the name of an interface which transmits packets out of the USG.
Gateway	This is the IP address of the gateway in the same network of the outgoing interface.
The following fields are available if you click Dynamic VPN or SiteToSite VPN in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the IP address(es) of the local VPN network.
Destination	This is the IP address(es) for the remote VPN network.
VPN Tunnel	This is the name of the VPN tunnel.
The following fields are available if you click Default WAN Trunk in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the source IP address(es) from which the packets are sent. any means any IP address.
Destination	This is the destination IP address(es) to which the packets are transmitted. any means any IP address.
Trunk	This is the name of the WAN trunk through which the matched packets are transmitted.

34.3 The SNAT Status Screen

The SNAT Status screen allows you to view and quickly link to specific source NAT (SNAT) settings. Click a function box in the SNAT Flow section, the related SNAT rules (activated) will display in the SNAT Table section. To access this screen, click Maintenance > Packet Flow Explore > SNAT Status.

The order of the SNAT flow may vary depending on whether you:

- select use default SNAT in the CONFIGURATION > Network > Interface > Trunk screen.
- use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.

Note: Once a packet matches the criteria of an SNAT rule, the USG takes the corresponding action and does not perform any further flow checking.

Figure 456 Maintenance > Packet Flow Explore > SNAT Status (Policy Route SNAT)

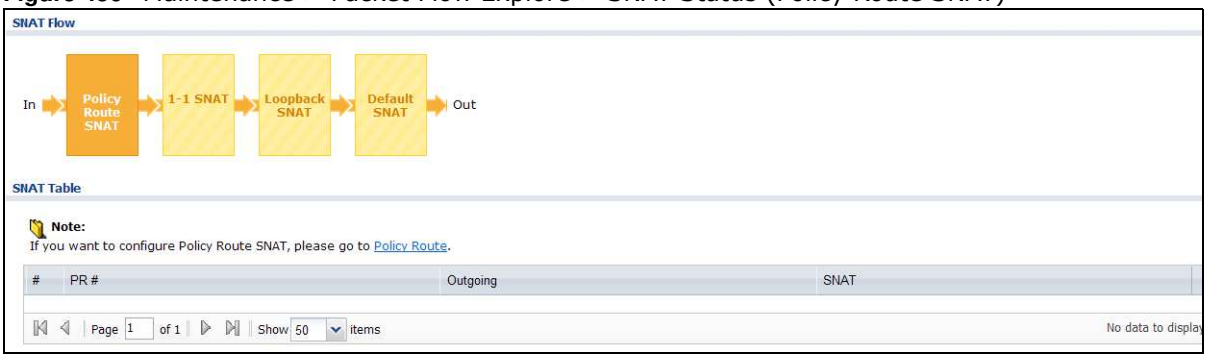


Figure 457 Maintenance > Packet Flow Explore > SNAT Status (1-1 SNAT)

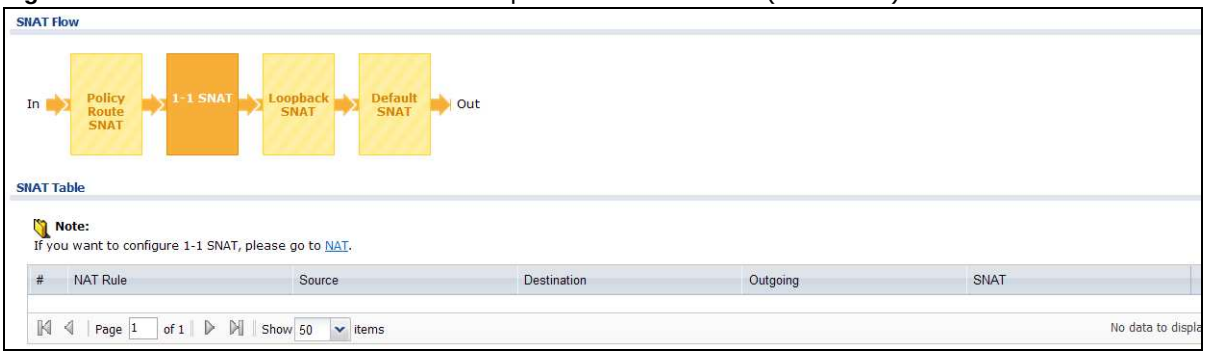


Figure 458 Maintenance > Packet Flow Explore > SNAT Status (Loopback SNAT)

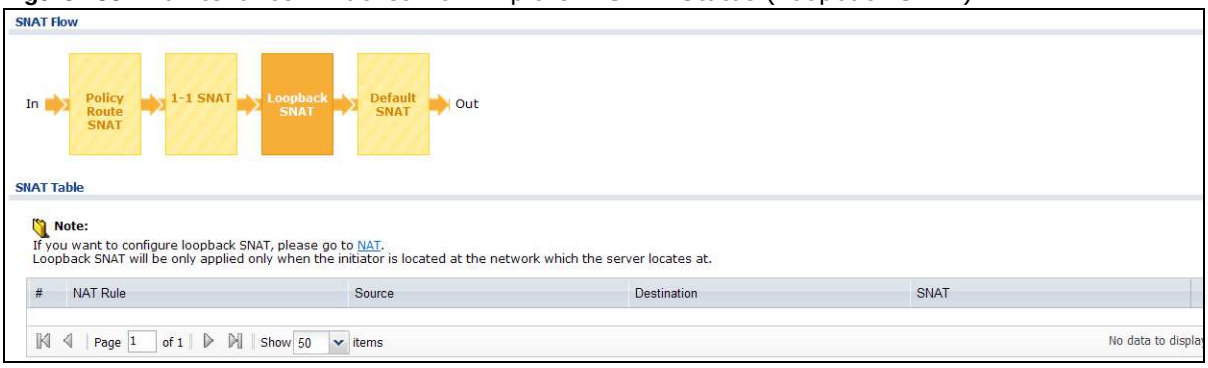
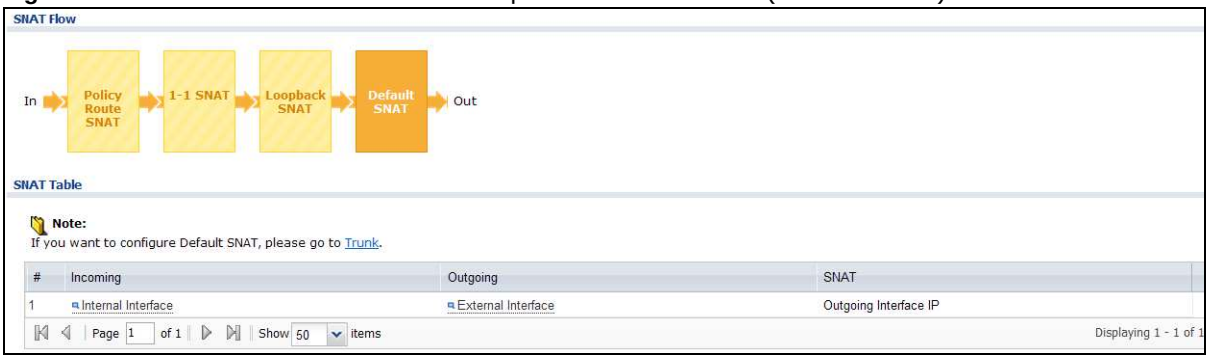


Figure 459 Maintenance > Packet Flow Explore > SNAT Status (Default SNAT)



The following table describes the labels in this screen.

Table 278 Maintenance > Packet Flow Explore > SNAT Status

LABEL	DESCRIPTION
SNAT Flow	This section shows you the flow of how the USG changes the source IP address for a packet according to the rules you have configured in the USG. Click a function box to display the related settings in the SNAT Table section.
SNAT Table	The table fields in this section vary depending on the function box you select in the SNAT Flow section.
The following fields are available if you click Policy Route SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
PR #	This is the number of an activated policy route which uses SNAT.
Outgoing	This is the outgoing interface that the route uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click 1-1 SNAT in the SNAT Flow section.	

Table 278 Maintenance > Packet Flow Explore > SNAT Status (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT.
Source	This is the original source IP address(es).
Destination	This is the original destination IP address(es).
Outgoing	This is the outgoing interface that the SNAT rule uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click Loopback SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT and enables NAT loopback.
Source	This is the original source IP address(es). any means any IP address.
Destination	This is the original destination IP address(es). any means any IP address.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, Outgoing Interface IP means that the USG uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.
The following fields are available if you click Default SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Incoming	This indicates internal interface(s) on which the packets are received.
Outgoing	This indicates external interface(s) from which the packets are transmitted.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, Outgoing Interface IP means that the USG uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.

35

Shutdown

35.1 Overview

Use this to shutdown the device in preparation for disconnecting the power.

Always use the Maintenance > Shutdown > Shutdown screen or the "shutdown" command before you turn off the USG or remove the power. Not doing so can cause the firmware to become corrupt.

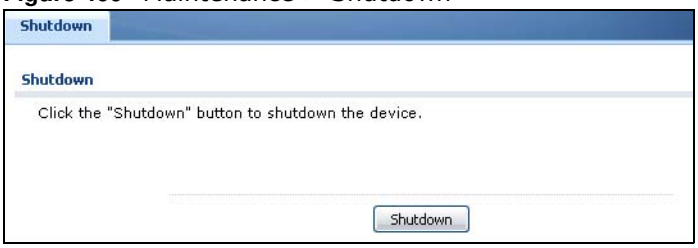
35.1.1 What You Need To Know

Shutdown writes all cached data to the local storage and stops the system processes.

35.2 The Shutdown Screen

To access this screen, click Maintenance > Shutdown.

Figure 460 Maintenance > Shutdown



Click the Shutdown button to shut down the USG. Wait for the device to shut down before you manually turn off or remove the power. It does not turn off the power.

You can also use the CLI command `shutdown` to shutdown the USG.

36

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

- You can also refer to the logs (see Chapter 6 on page 101).
- For the order in which the USG applies its features and checks, see Chapter 34 on page 628.

None of the LEDs turn on.

Make sure that you have the power cord connected to the USG and plugged in to an appropriate power source. Make sure you have the USG turned on. Check all cable connections.

If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.

Cannot access the USG from the LAN.

- Check the cable connection between the USG and your computer or switch.
- Ping the USG from a LAN computer. Make sure your computer's Ethernet card is installed and functioning properly. Also make sure that its IP address is in the same subnet as the USG's.
- In the computer, click Start, (All) Programs, Accessories and then Command Prompt. In the Command Prompt window, type "ping" followed by the USG's LAN IP address (192.168.1.1 is the default) and then press [ENTER]. The USG should reply.
- If you've forgotten the USG's password, use the RESET button. Press the button in for about 5 seconds (or until the PWR LED starts to blink), then release it. It returns the USG to the factory defaults (password is 1234, LAN IP address 192.168.1.1 etc.; see your User's Guide for details).
- If you've forgotten the USG's IP address, you can use the commands through the console port to check it. Connect your computer to the CONSOLE port using a console cable. Your computer should have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 115200 bps port speed.

I cannot access the Internet.

- Check the USG's connection to the Ethernet jack with Internet access. Make sure the Internet gateway device (such as a DSL modem) is working properly.
- Check the WAN interface's status in the Dashboard. Use the installation setup wizard again and make sure that you enter the correct settings. Use the same case as provided by your ISP.

The content filter category service is not working.

- Make sure your USG has the content filter category service registered and that the license is not expired. Purchase a new license if the license is expired.
- Make sure your USG is connected to the Internet.

I configured security settings but the USG is not applying them for certain interfaces.

Many security settings are usually applied to zones. Make sure you assign the interfaces to the appropriate zones. When you create an interface, there is no security applied on it until you assign it to a zone.

The USG is not applying the custom policy route I configured.

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

The USG is not applying the custom security policy I configured.

The USG checks the security policies in the order that they are listed. So make sure that your custom security policy comes before any other rules that the traffic would also match.

I cannot enter the interface name I want.

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

- The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the Web Configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

I cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface on an Ethernet interface.

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

My rules and settings that apply to a particular interface no longer work.

The interface's IP address may have changed. To avoid this create an IP address object based on the interface. This way the USG automatically updates every rule or setting that uses the object whenever the interface's IP address settings change. For example, if you change LAN1's IP address, the USG automatically updates the corresponding interface-based, LAN1 subnet address object.

I cannot set up a PPP interface.

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

The data rates through my cellular connection are no-where near the rates I expected.

The actual cellular data rate you obtain varies depending on the cellular device you use, the signal strength to the service provider's base station, and so on.

I created a cellular interface but cannot connect through it.

- Make sure you have a compatible mobile broadband device installed or connected. See www.zyxel.com for details.
- Make sure you have the cellular interface enabled.
- Make sure the cellular interface has the correct user name, password, and PIN code configured with the correct casing.
- If the USG has multiple WAN interfaces, make sure their IP addresses are on different subnets.

Hackers have accessed my WEP-encrypted wireless LAN.

WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. WPA2 or WPA2-PSK is recommended.

The wireless security is not following the re-authentication timer setting I specified.

If a RADIUS server authenticates wireless stations, the re-authentication timer on the RADIUS server has priority. Change the RADIUS server's configuration if you need to use a different re-authentication timer setting.

I cannot configure a particular VLAN interface on top of an Ethernet interface even though I have it configured it on top of another Ethernet interface.

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

The USG is not applying an interface's configured ingress bandwidth limit.

At the time of writing, the USG does not support ingress bandwidth management.

The USG routes and applies SNAT for traffic from some interfaces but not from others.

The USG automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic. You must manually configure a policy route to add routing and SNAT settings for an interface with the Interface Type set to General. You can also configure a policy route to override the default routing and SNAT behavior for an interface with the Interface Type set to Internal or External.

I cannot get Dynamic DNS to work.

- You must have a public WAN IP address to use Dynamic DNS.
- Make sure you recorded your DDNS account's user name, password, and domain name and have entered them properly in the USG.
- You may need to configure the DDNS entry's IP Address setting to Auto if the interface has a dynamic IP address or there are one or more NAT routers between the USG and the DDNS server.
- The USG may not determine the proper IP address if there is an HTTP proxy server between the USG and the DDNS server.

I cannot create a second HTTP redirect rule for an incoming interface.

You can configure up to one HTTP redirect rule for each (incoming) interface.

The USG keeps resetting the connection.

If an alternate gateway on the LAN has an IP address in the same subnet as the USG's LAN IP address, return traffic may not go through the USG. This is called an asymmetrical or "triangle" route. This causes the USG to reset the connection, as the connection has not been acknowledged.

You can set the USG's security policy to permit the use of asymmetrical route topology on the network (so it does not reset the connection) although this is not recommended since allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the USG. A better solution is to use virtual interfaces to put the USG and the backup gateway on separate subnets. See Asymmetrical Routes on page 321 and the chapter about interfaces for more information.

I cannot set up an IPSec VPN tunnel to another device.

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into both ZyXEL IPSec routers and check the settings in each field methodically and slowly. Make sure both the USG and remote IPSec router have the same security settings for the VPN tunnel. It may help to display the settings for both routers side-by-side.

Here are some general suggestions. See also Chapter 21 on page 333.

- The system log can often help to identify a configuration problem.
- If you enable NAT traversal, the remote IPSec device must also have NAT traversal enabled.
- The USG and remote IPSec router must use the same authentication method to establish the IKE SA.
- Both routers must use the same negotiation mode.
- Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.
- When using pre-shared keys, the USG and the remote IPSec router must use the same pre-shared key.
- The USG's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.
- The USG and remote IPSec router must use the same active protocol.
- The USG and remote IPSec router must use the same encapsulation.
- The USG and remote IPSec router must use the same SPI.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learnt by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other.
  Before doing so, ensure that both computers have Internet access (via the IPSec routers).
- It is also helpful to have a way to look at the packets that are being sent and received by the USG and remote IPSec router (for example, by using a packet sniffer).

Check the configuration for the following USG features.

- The USG does not put IPSec SAs in the routing table. You must create a policy route for each VPN tunnel. See Chapter 10 on page 227.
- Make sure the To-USG security policies allow IPSec VPN traffic to the USG. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- The USG supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the To-USG security policies allow UDP port 4500 too.
- Make sure regular security policies allow traffic between the VPN tunnel and the rest of the network. Regular security policies check packets the USG sends before the USG encrypts them and check packets the USG receives after the USG decrypts them. This depends on the zone to which you assign the VPN tunnel and the zone from which and to which traffic may be routed.
- If you set up a VPN tunnel across the Internet, make sure your ISP supports AH or ESP (whichever you are using).
- If you have the USG and remote IPSec router use certificates to authenticate each other, You must set up the certificates for the USG and remote IPSec router first and make sure they trust each other's certificates. If the USG's certificate is self-signed, import it into the remote IPsec router. If it is signed by a CA, make sure the remote IPsec router trusts that CA. The USG uses one of its Trusted Certificates to authenticate the remote IPSec router's certificate. The trusted certificate can be the remote IPSec router's self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.
- Multiple SAs connecting through a secure gateway must have the same negotiation mode.

The VPN connection is up but VPN traffic cannot be transmitted through the VPN tunnel.

If you have the Configuration > VPN > IPSec VPN > VPN Connection screen's Use Policy Route to control dynamic IPSec rules option enabled, check the routing policies to see if they are sending traffic elsewhere instead of through the VPN tunnels.

I uploaded a logo to show in the SSL VPN user screens but it does not display properly.

The logo graphic must be GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The USG automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.

I logged into the SSL VPN but cannot see some of the resource links.

Available resource links vary depending on the SSL application object's configuration.

I changed the LAN IP address and can no longer access the Internet.

The USG automatically updates address objects based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. However, you need to manually edit any address objects for your LAN that are not based on the interface.

I cannot get the RADIUS server to authenticate the USG's default admin account.

The default `admin` account is always authenticated locally, regardless of the authentication method setting.

The USG fails to authentication the ext-user user accounts I configured.

An external server such as AD, LDAP or RADIUS must authenticate the ext-user accounts. If the USG tries to use the local database to authenticate an `ext-user`, the authentication attempt will always fail. (This is related to AAA servers and authentication methods, which are discussed in other chapters in this guide.)

I cannot add the admin users to a user group with access users.

You cannot put access users and admin users in the same user group.

I cannot add the default admin account to a user group.

You cannot put the default `admin` account into any user group.

The schedule I configured is not being applied at the configured times.

Make sure the USG's current date and time are correct.

I cannot get a certificate to import into the USG.

1. For `My Certificates`, you can import a certificate that matches a corresponding certification request that was generated by the USG. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.
2. You must remove any spaces from the certificate's filename before you can import the certificate.
3. Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The USG currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the USG.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

I cannot access the USG from a computer connected to the Internet.

Check the service control rules and to-USG security policies.

I uploaded a logo to display on the upper left corner of the Web Configurator login screen and access page but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

I uploaded a logo to use as the screen or window background but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

The USG's traffic throughput rate decreased after I started collecting traffic statistics.

Data collection may decrease the USG's traffic throughput rate.

I can only see newer logs. Older logs are missing.

When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

The commands in my configuration file or shell script are not working properly.

- In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the USG treat the line as a comment.
- Your configuration files or shell scripts can use "exit" or a command line consisting of a single "!" to have the USG exit sub command mode.
- Include `write` commands in your scripts. Otherwise the changes will be lost when the USG restarts. You could use multiple `write` commands in a long script.

Note: "exit" or "!'" must follow sub commands if it is to make the USG exit sub command mode.

See Chapter 32 on page 605 for more on configuration files and shell scripts.

I cannot get the firmware uploaded using the commands.

The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

My packet capture captured less than I wanted or failed.

The packet capture screen's File Size sets a maximum size limit for the total combined size of all the capture files on the USG, including any existing capture files and any new capture files you generate. If you have existing capture files you may need to set this size larger or delete existing capture files.

The USG stops the capture and generates the capture file when either the capture files reach the File Size or the time period specified in the Duration field expires.

My earlier packet capture files are missing.

New capture files overwrite existing files of the same name. Change the File Suffix field's setting to avoid this.

36.1 Resetting the USG

If you cannot access the USG by any method, try restarting it by turning the power off and then on again. If you still cannot access the USG by any method or you forget the administrator

password(s), you can reset the USG to its factory-default settings. Any configuration files or shell scripts that you saved on the USG should still be available afterwards.

Use the following procedure to reset the USG to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

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

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

36.2 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See *http://www.zyxel.com/homepage.shtml* and also

http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

Please have the following information ready when you contact an office.

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Asia

China

- ZyXEL Communications (Shanghai) Corp.
  ZyXEL Communications (Beijing) Corp.
  ZyXEL Communications (Tianjin) Corp.
- http://www.zyxel.cn

India

- ZyXEL Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- ZyXEL Kazakhstan
- http://www.zyxel.kz

Korea

- ZyXEL Korea Corp.
- http://www.zyxel.kr

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- ZyXEL Philippines
- http://www.zyxel.com.ph

Singapore

- ZyXEL Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com/tw/zh/

Thailand

- ZyXEL Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

Europe

Austria

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Belarus

- ZyXEL BY
- http://www.zyxel.by

Belgium

- ZyXEL Communications B.V.
- http://www.zyxel.com/be/nl/
- http://www.zyxel.com/be/fr/

Bulgaria

- ZyXEL България
- http://www.zyxel.com/bg/bg/

Czech Republic

- ZyXEL Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- ZyXEL Communications A/S
- http://www.zyxel.dk

Estonia

- ZyXEL Estonia
- http://www.zyxel.com/ee/et/

Finland

- ZyXEL Communications
- http://www.zyxel.fi

France

- ZyXEL France
- http://www.zyxel.fr

Germany

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Hungary

- ZyXEL Hungary & SEE
- http://www.zyxel.hu

Italy

- ZyXEL Communications Italy
- http://www.zyxel.it/

Latvia

- ZyXEL Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- ZyXEL Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- ZyXEL Benelux
- http://www.zyxel.nl

Norway

- ZyXEL Communications
- http://www.zyxel.no

Poland

- ZyXEL Communications Poland
- http://www.zyxel.pl

Romania

- ZyXEL Romania
- http://www.zyxel.com/ro/ro

Russia

- ZyXEL Russia
- http://www.zyxel.ru

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- ZyXEL Communications ES Ltd
- http://www.zyxel.es

Sweden

- ZyXEL Communications
- http://www.zyxel.se

Switzerland

- Studerus AG
- http://www.zyxel.ch/

Turkey

- ZyXEL Turkey A.S.
- http://www.zyxel.com.tr

UK

- ZyXEL Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- ZyXEL Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Brazil

- ZyXEL Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Ecuador

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Israel

- ZyXEL Communication Corporation
- http://il.zyxel.com/homepage.shtml

Middle East

- ZyXEL Communication Corporation
- http://www.zyxel.com/me/en/

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- http://www.zyxel.com/us/en/

Oceania

Australia

- ZyXEL Communications Corporation
- http://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

B

Legal Information

Copyright

Copyright © 2016 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Regulatory Notice and Statement (Class B)

UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

FCC EMC Statement

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

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications 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 residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device 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 devices
  - •Connect the equipment to an outlet other than the receiver's
  - •Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.

This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

CANADA

The following information applies if you use the product within Canada area

Industry Canada ICES statement

ICAN ICES-3 (B)/NMB-3(B)

Industry Canada RSS-GEN & RSS-247 statement

- This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter (2468C-USG20WVPN) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna Information

TYPE	MANUFACTURER	GAIN	CONNECTOR
Omini-directional dipole	WHA YU	3dBi	Reverse SMA plug

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz , the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz , the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit
- Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio (2468C-USG20WVPN) de modèle s'il fait partie du matériel de catégorieI) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Informations Antenne

TYPE	FABRICANT	GAIN	CONNECTEUR
Omini-directional dipole	WHA YU	3dBi	Reverse SMA plug

Lorsque la fonction sans fil 5G fonctionnant en5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3) du CNR-247, doivent être clairement indiqués.

  Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

EUROPEAN UNION



The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 1999/5/EC (R&TTE)

Български (Bulgarian)	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/ЕС.
Español (Spanish)	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Čeština (Czech)	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
Dansk (Danish)	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch (German)	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
English	Hereby, ZyXEL declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Français (French)	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
Hrvatski (Croatian)	ZyXEL ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 1999/5/EC.
Íslenska (Icelandic)	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
Italiano (Italian)	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviešu valoda (Latvian)	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Nederlands (Dutch)	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
Polski (Polish)	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português (Portuguese)	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
Română (Romanian)	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.
Slovenčina (Slovak)	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
Slovenščina (Slovene)	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
Suomi (Finnish)	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
Norsk (Norwegian)	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.

This device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

National Restrictions

This product may be used in all EU countries (and other countries following the EU Directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttiva 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der Richtlinie 1999/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2.4GHz and 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2.4GHz and 5GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do not obstruct the device ventilation slots, as insufficient airflow may harm your device.

The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

- For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
- For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment Statement

ErP (Energy-related Products)

ZyXEL products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called

as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

Network standby power consumption < 12W, and/or

Off mode power consumption < 0.5W, and/or

Standby mode power consumption < 0.5W.

Wireless setting, please refer to "Wireless" chapter for more detail.

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

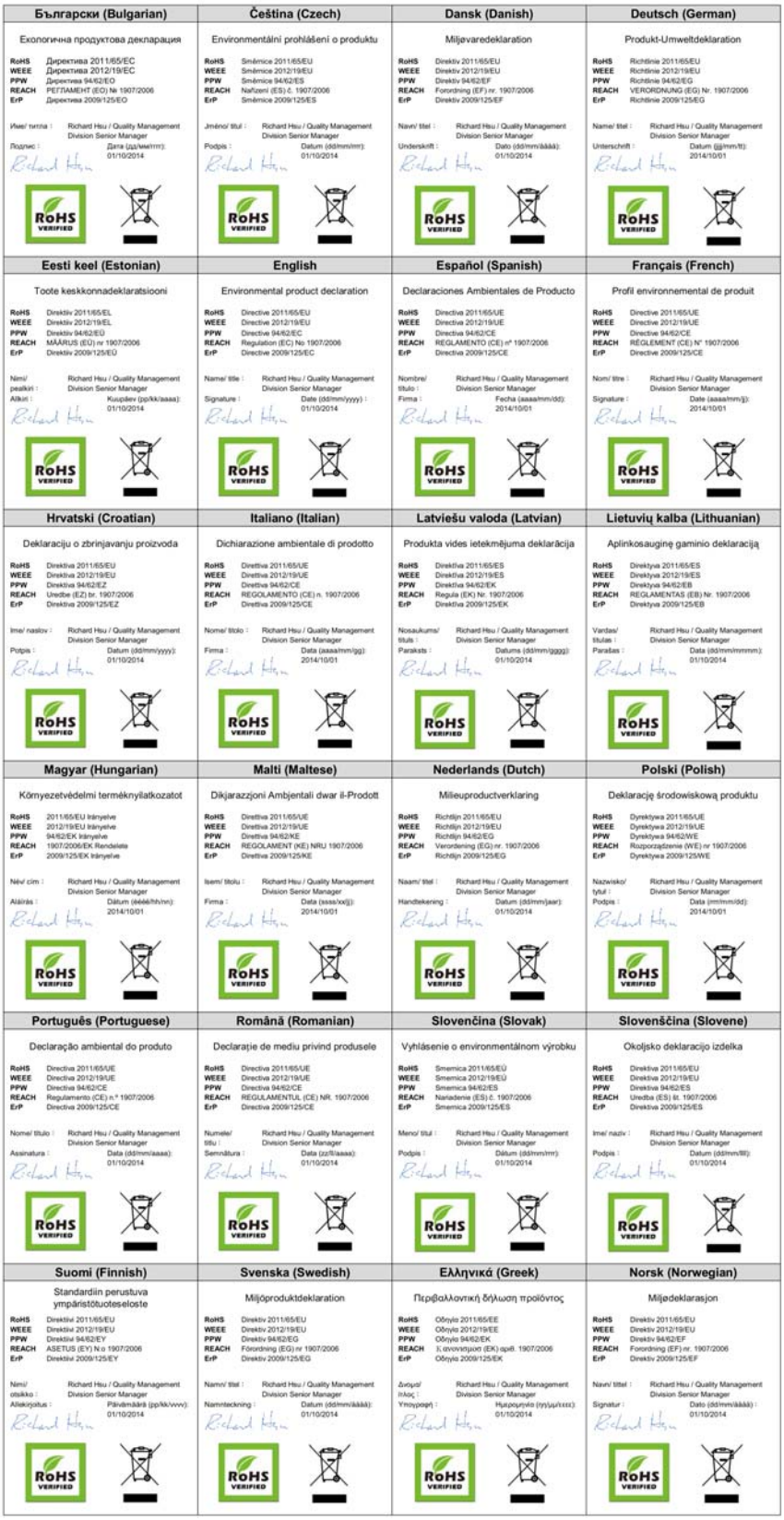
Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



Environmental Product Declaration



Български (Bulgarian)

Екологична продуктова декларация

RoHS Директива 2011/65/EC
WEEE Директива 2012/19/EC
PPW Директива 94/62/EO
REACH РЕГЛАМЕНТ (ЕО) № 1907/2006
ErP Директива 2009/125/EO

Име/ титла : Richard Hsu / Quality Management Division Senior Manager
Подпис : Дата (дд/мм/гггг): 01/10/2014

Čeština (Czech)

Environmentální prohlášení o produktu

RoHS Směrnice 2011/65/EU
WEEE Směrnice 2012/19/EU
PPW Směrnice 94/62/ES
REACH Nařízení (ES) č. 1907/2006
ErP Směrnice 2009/125/ES

Jméno/ titul : Richard Hsu / Quality Management Division Senior Manager
Podpis : Datum (dd/mm/rrrr): 01/10/2014

Dansk (Danish)

Miljøvaredeklaration

RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EF
REACH Forordning (EF) nr. 1907/2006
ErP Direktiv 2009/125/EF

Navn/ titel : Richard Hsu / Quality Management Division Senior Manager
Underskrift : Dato (dd/mm/åååå): 01/10/2014

Deutsch (German)

Produkt-Umweltdeklaration

RoHS Richtlinie 2011/65/EU
WEEE Richtlinie 2012/19/EU
PPW Richtlinie 94/62/EG
REACH VERORDNUNG (EG) Nr. 1907/2006
ErP Richtlinie 2009/125/EG

Name/ titel : Richard Hsu / Quality Management Division Senior Manager
Unterschrift : Datum (tt/mm/jj): 2014/10/01

Eesti keel (Estonian)

Toote keskkonnadeklaratsiooni

RoHS Direktiiv 2011/65/EL
WEEE Direktiiv 2012/19/EL
PPW Direktiiv 94/62/EÜ
REACH MÄÄRUS (EÜ) nr 1907/2006
ErP Direktiiv 2009/125/EÜ

Nimi/ positsioon : Richard Hsu / Quality Management Division Senior Manager
Allkiri : Kuupäev (pp/kk/aaaa): 01/10/2014

English

Environmental product declaration

RoHS Directive 2011/65/EU
WEEE Directive 2012/19/EU
PPW Directive 94/62/EC
REACH Regulation (EC) No 1907/2006
ErP Directive 2009/125/EC

Name/ title : Richard Hsu / Quality Management Division Senior Manager
Signature : Date (dd/mm/yyyy) : 01/10/2014

Español (Spanish)

Declaraciones Ambientales de Producto

RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH REGLAMENTO (CE) nº 1907/2006
ErP Directiva 2009/125/CE

Nombre/ título : Richard Hsu / Quality Management Division Senior Manager
Firma : Fecha (aaaa/mm/dd): 2014/10/01

Français (French)

Profil environnemental de produit

RoHS Directive 2011/65/UE
WEEE Directive 2012/19/UE
PPW Directive 94/62/CE
REACH RÈGLEMENT (CE) N° 1907/2006
ErP Directive 2009/125/CE

Nom/ titre : Richard Hsu / Quality Management Division Senior Manager
Signature : Date (aaaa/mm/jj): 2014/10/01

Hrvatski (Croatian)

Deklaraciju o zbrinjavanju proizvoda

RoHS Direktiva 2011/65/EU
WEEE Direktiva 2012/19/EU
PPW Direktiva 94/62/EZ
REACH Uredbe (EZ) br. 1907/2006
ErP Direktiva 2009/125/EZ

Ime/ naslov : Richard Hsu / Quality Management Division Senior Manager
Potpis : Datum (dd/mm/yyyy): 01/10/2014

Italiano (Italian)

Dichiarazione ambientale di prodotto

RoHS Direttiva 2011/65/UE
WEEE Direttiva 2012/19/UE
PPW Direttiva 94/62/CE
REACH REGOLAMENTO (CE) n. 1907/2006
ErP Direttiva 2009/125/CE

Nome/ titolo : Richard Hsu / Quality Management Division Senior Manager
Firma : Data (aaaa/mm/gg): 2014/10/01

Latviešu valoda (Latvian)

Produkta vides ietekmējuma deklarācija

RoHS Direktīva 2011/65/ES
WEEE Direktīva 2012/19/ES
PPW Direktīva 94/62/EK
REACH Regula (EK) Nr. 1907/2006
ErP Direktīva 2009/125/EK

Nosaukums/ tituls : Richard Hsu / Quality Management Division Senior Manager
Paraksts : Datums (dd/mm/gggg): 01/10/2014

Lietuvių kalba (Lithuanian)

Aplinkosauginę gaminio deklaraciją

RoHS Direktyva 2011/65/ES
WEEE Direktyva 2012/19/ES
PPW Direktyva 94/62/EB
REACH REGLAMENTAS (EB) Nr. 1907/2006
ErP Direktyva 2009/125/EB

Vardas/ titulas : Richard Hsu / Quality Management Division Senior Manager
Parašas : Data (dd/mm/mmmm): 01/10/2014

Magyar (Hungarian)

Környezetvédelmi terméknyilatkozatot

RoHS 2011/65/EU irányelve
WEEE 2012/19/EU irányelve
PPW 94/62/EK irányelve
REACH 1907/2006/EK Rendelete
ErP 2009/125/EK irányelve

Név/ cím : Richard Hsu / Quality Management Division Senior Manager
Aláírás : Dátum (éééé/hh/nn): 2014/10/01

Malti (Maltese)

Dikjarazzjoni Ambjentali dwar il-Prodott

RoHS Direttiva 2011/65/UE
WEEE Direttiva 2012/19/UE
PPW Direttiva 94/62/KE
REACH REGOLAMENT (KE) NRU 1907/2006
ErP Direttiva 2009/125/KE

Isem/ titolu : Richard Hsu / Quality Management Division Senior Manager
Firma : Data (ssss/xx/jj): 2014/10/01

Nederlands (Dutch)

Milieuproductverklaring

RoHS Richtlijn 2011/65/EU
WEEE Richtlijn 2012/19/EU
PPW Richtlijn 94/62/EG
REACH Verordening (EG) nr. 1907/2006
ErP Richtlijn 2009/125/EG

Naam/ titel : Richard Hsu / Quality Management Division Senior Manager
Handtekening : Datum (dd/mm/jaar): 01/10/2014

Polski (Polish)

Deklarację środowiskową produktu

RoHS Dyrektywa 2011/65/UE
WEEE Dyrektywa 2012/19/UE
PPW Dyrektywa 94/62/WE
REACH Rozporządzenie (WE) nr 1907/2006
ErP Dyrektywa 2009/125/WE

Nazwisko/ tytuł : Richard Hsu / Quality Management Division Senior Manager
Podpis : Data (rrrr/mm/dd): 2014/10/01

Português (Portuguese)

Declaração ambiental do produto

RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH Regulamento (CE) n.º 1907/2006
ErP Directiva 2009/125/CE

Nome/ título : Richard Hsu / Quality Management Division Senior Manager
Assinatura : Data (dd/mm/aaaa): 01/10/2014

Română (Romanian)

Declarație de mediu privind produsele

RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH REGLAMENTUL (CE) NR. 1907/2006
ErP Directiva 2009/125/CE

Numele/ titlu : Richard Hsu / Quality Management Division Senior Manager
Semnătura : Data (zz/ll/aaaa): 01/10/2014

Slovenčina (Slovak)

Vyhlásenie o environmentálnom výrobku

RoHS Smernica 2011/65/EÚ
WEEE Smernica 2012/19/EÚ
PPW Smernica 94/62/ES
REACH Nariadenie (ES) č. 1907/2006
ErP Smernica 2009/125/ES

Meno/ titul : Richard Hsu / Quality Management Division Senior Manager
Podpis : Dátum (dd/mm/rrrr): 01/10/2014

Slovenščina (Slovene)

Okoljsko deklaracijo izdelka

RoHS Direktiva 2011/65/EU
WEEE Direktiva 2012/19/EU
PPW Direktiva 94/62/ES
REACH Uredba (ES) št. 1907/2006
ErP Direktiva 2009/125/ES

Ime/ naziv : Richard Hsu / Quality Management Division Senior Manager
Podpis : Datum (dd/mm/ll): 01/10/2014

Suomi (Finnish)

Standardiin perustuva ympäristötuoteseloste

RoHS Direktiivi 2011/65/EU
WEEE Direktiivi 2012/19/EU
PPW Direktiivi 94/62/EY
REACH ASETUS (EY) N:o 1907/2006
ErP Direktiivi 2009/125/EY

Nimi/ otsikko : Richard Hsu / Quality Management Division Senior Manager
Allekirjoitus : Päivämäärä (pp/kk/vvvv): 01/10/2014

Svenska (Swedish)

Miljöproduktdeklaration

RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EG
REACH Förordning (EG) nr 1907/2006
ErP Direktiv 2009/125/EG

Namn/ titel : Richard Hsu / Quality Management Division Senior Manager
Namnteckning : Datum (dd/mm/åååå): 01/10/2014

Ελληνικά (Greek)

Περιβαλλοντική δήλωση προϊόντος

RoHS Οδηγία 2011/65/ΕΕ
WEEE Οδηγία 2012/19/ΕΕ
PPW Οδηγία 94/62/ΕΚ
REACH Κ ανανησμοσ (ΕΚ) αρθ. 1907/2006
ErP Οδηγία 2009/125/ΕΚ

Δνομα/ τίτλος : Richard Hsu / Quality Management Division Senior Manager
Υπογραφή : Ημερομηνία (ηη/μμ/εεεε): 01/10/2014

Norsk (Norwegian)

Miljødeklarasjon

RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EF
REACH Forordning (EF) nr. 1907/2006
ErP Direktiv 2009/125/EF

Navn/ tittel : Richard Hsu / Quality Management Division Senior Manager
Signatur : Dato (dd/mm/åååå) : 01/10/2014

台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

用 20cm 計算 MPE 能符合 1 mW/cm2

電磁波曝露量 MPE 標準值 1mW/cm2，送測產品實測值為： 0.918 mW/ cm2

無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用， 俟無干擾之虞，始得繼續使用。

無線資訊傳設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作， 發射的信號應維持於操作頻帶中

以下訊息僅適用於產品操作於 5.25-5.35 秭赫頻帶內並銷售至台灣地區

- 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得 設置使用，且不得直接販售給一般消費者

安全警告

為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
- 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

Specifications

- Product Rating: Refer to the USG label.
- Power Adapter: 12V DC, 2.0A, LPS, 40°C (degrees Centigrade).
- Device Operating / Storage Environment: Refer to the USG package.

This product is intended to be supplied by a Listed Direct Plug-In Power Unit marked "Class 2", Listed Power Adapter or DC power source marked "L.P.S." (or "Limited Power Source"), rated 12Vdc, 2A minimum, Tma = 40 degree C, and the altitude of operation = 2000m. If need further assistance with purchasing the power source, please contact ZyXEL for further information.

ZyXEL Limited Warranty

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

Note

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

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

C

Product Features

Please refer to the product datasheet for the latest product features.

Table 279 Product Features

MODEL NAME	USG20-VPN	USG20W-VPN
Version	4.16	4.16
# of MAC	6	7
Interface		
VLAN	8	8
Virtual (alias)	4	4
PPP (system default)	2	2
PPP (user create)	2	2
Bridge	2	2
Tunnel (GRE/IPv6 Transition)	4	4
Routing		
Static route	64	64
Policy route	100	100
Sessions (Forwarding, NAT/firewall)	20000	20000
Reserved Sessions For Managed Devices	500	500
ARP Table Size	16384	16384
NAT		
Max. Virtual Server Number	128	128
Firewall (Security policy)		
Max Firewall ACL Rule Number = Secure Policy Number (Marketing spec, Lab test * 10%)	500	500
Max Session Limit per Host Rules	1000	1000
User Profile		
Max. Local User	64	64
Max. Admin User	5	5
Max. User Group.	16	16
Max User In One User Group	64	64
Max Concurrent User	64	64
Objects		
Address Object (Marketing spec, Lab amount = VPN rule #)	100	100

Table 279 Product Features

MODEL NAME	USG20-VPN	USG20W-VPN
Address Group	25	25
Max. Address Object In One Group	64	64
Service Object	200	200
Service Group	50	50
Max. Service Object In One Group	64	64
Schedule Object	32	32
Schedule Group	16	16
Max. Schedule Object In One Group	24	24
ISP Account	16(PPP+3G)	16(PPP+3G)
Max. LDAP Server Object #	2	2
Max. LDAP Server for Each LDAP Group	2	2
Max. RADIUS Server Object #	2	2
Max. RADIUS Server for Each RADIUS Group	2	2
Max. AD Server Object #	4	4
Max. AD Server for Each AD Group	2	2
Max. Zone Number (System Default)	8	8
Max. Zone Number (User Define)	8	8
Max. Trunk Number (System Default)	1	1
Max. Trunk Number (User Define)	4	4
Max Radio Profile	16	16
Max SSID Profile	32	32
Max Security Profile	32	32
Max Macfilter Profile	32	32
Max MAC Entry Per Macfilter Profile	512	512
VPN		
Max. VPN Tunnels Number	10	10
Max. VPN Concentrator Number	2	2
Max. VPN Configuration Provision Rule Number	10	10
Certificate		
Certificate Buffer Size	128k	128k
Built-in service		
A record	32	32
NS record (DNS Domain Zone Forward)	8	8
MX record	4	4
Max Service Control Entries	16 per service	16 per service
Max. DHCP Network Pool	vlan+brg+ethernet	vlan+brg+ethernet

Table 279 Product Features

MODEL NAME	USG20-VPN	USG20W-VPN
Max. DHCP Host Pool(Static DHCP)	64	64
Max. DHCP Extended Options	10	10
Max DDNS Profiles	5	5
DHCP Relay	2 per interface	2 per interface
USB Storage		
Device Number	1	1
Centralized Log		
Log Entries	512	512
Debug Log Entries	1024	1024
Admin E-mail Address	2	2
Syslog Server	4	4
Content Filtering		
Max. Number of Content Filter Policy	16	16
Max. Number of Filtering Profiles	16	16
Forbidden Domain Entry Number	256 per profile	256 per profile
Trusted Domain Entry Number	256 per profile	256 per profile
Keyword Blocking Number	128 per profile	128 per profile
Common Forbidden Domain Entry Number	1024	1024
Common Trusted Domain Entry Number	1024	1024
Anti-Spam (Available in ZLD 2.10 and later versions)		
Maximum AS Rule Number (Profile)	16	16
Maximum White List Rule Support	128	128
Maximum Black List Rule Support	128	128
Maximum DNSBL Domain Support	5	5
Max. Statistics Number	500	500
Max. Statistics Ranking	10	10
MyZyXEL.com		
SKU update interval (day)	2 ~ 6 hrs	2 ~ 6 hrs
SSL VPN (Available in ZLD 2.00 and later versions)		
Default SSL VPN Connections	5	5
Maximum SSL VPN Connections	15	15
Max. SSL VPN Network List	8	8
SSL VPN Max Policy	16	16
AP controller		
Default # of Control AP	NA	NA
Max. # of Control AP	NA	NA

Table 279 Product Features

MODEL NAME	USG20-VPN	USG20W-VPN
Others		
Device HA VRRP Group	n/a	n/a
Max OSPF Areas	32	32

Index

Symbols

Numbers

3322 Dynamic DNS 250
3DES 359
6in4 tunneling 184
6to4 tunneling 184

A

AAA
  Base DN 505
  Bind DN 505, 508
  directory structure 504
  Distinguished Name, see DN
  DN 505, 506, 508
  password 508
  port 508, 510
  search time limit 508
  SSL 508
AAA server 502
  AD 504
  and users 456
  directory service 503
  LDAP 503, 504
  local user database 504
  RADIUS 503, 504, 509
  RADIUS group 510
  see also RADIUS
access 23
Access Point Name, see APN
access users 456, 457
  custom page 560
  forcing login 299
  idle timeout 464
  logging in 299
  multiple logins 464
  see also users 456
  Web Configurator 466
access users, see also force user authentication policies
account
  user 455
accounting server 502
Active Directory, see AD
active protocol 364
  AH 364
  and encapsulation 364
  ESP 364
active sessions 91, 109
ActiveX 430
AD 503, 505, 506, 508
  directory structure 504
  Distinguished Name, see DN
  password 508
  port 508, 510
  search time limit 508
  SSL 508
address groups 488
  and content filtering 416, 417
  and FTP 577
  and security policy 303
  and SNMP 581
  and SSH 573
  and Telnet 575
  and WWW 559
address objects 488
  and content filtering 416, 417
  and FTP 577
  and NAT 235, 259
  and policy routes 234
  and security policy 303
  and SNMP 581
  and SSH 573
  and Telnet 575
  and VPN connections 338
  and WWW 559
  HOST 488
  RANGE 488

SUBNET 488
types of 488
address record 548
admin user
troubleshooting 643
admin users 456
multiple logins 464
see also users 456
Advanced Encryption Standard, see AES
AES 359
AF 238
AH 342, 364
and transport mode 365
alerts 596, 597, 599, 601, 602, 603
anti-spam 439
ALG 267, 272
and NAT 267, 269
and policy routes 269, 272
and security policy 267, 269
and trunks 272
FTP 267
H.323 267, 268, 273
peer-to-peer calls 269
RTP 273
see also VoIP pass through 267
SIP 267, 268
anti-spam 435, 439, 442
action for spam mails 440
alerts 439
and registration 438
black list 435, 439, 442
concurrent e-mail sessions 129, 437
DNSBL 436, 440, 447
e-mail header buffer 436
e-mail headers 436
excess e-mail sessions 437
general settings 437
identifying legitimate e-mail 435
identifying spam 435
log options 439
mail scan 440
mail sessions threshold 437
POP2 436
POP3 436
registration status 438
regular expressions 445
SMTP 436
status 130
white list 435, 439, 444, 445
APN 179
Application Layer Gateway, see ALG
application patrol
and HTTP redirect 264
ASAS (Authenex Strong Authentication System) 503
asymmetrical routes 321
allowing through the security policy 324
vs virtual interfaces 321
attacks
Denial of Service (DoS) 341
Authenex Strong Authentication System (ASAS) 503
authentication
in IPSec 343
LDAP/AD 504
server 502
authentication algorithms 248, 359, 360
and active protocol 359
and routing protocols 248
MD5 248, 360
SHA1 360
text 248
Authentication Header, see AH
authentication method objects 511
and users 456
and WWW 559
create 513
example 511
authentication policy
exceptional services 301
Authentication server
RADIUS client 582
authentication server 581
authentication type 54, 531
Authentication, Authorization, Accounting servers, see AAA server
authorization server 502
auxiliary interfaces 142

B

backing up configuration files 607
bandwidth

egress 180, 189
ingress 180, 189
bandwidth limit
troubleshooting 640
bandwidth management
maximize bandwidth usage 238, 405
Base DN 505
Batch import 584
Bind DN 505, 508
black list 439, 442
anti-spam 435
bookmarks 384
bridge interfaces 142, 203
and virtual interfaces of members 204
basic characteristics 143
effect on routing table 203
member interfaces 203
virtual 214
bridges 202

C

CA
and certificates 515
CA (Certificate Authority), see certificates
Calling Station ID 481
capturing packets 618
card SIM 180
CEF (Common Event Format) 594, 601
cellular 174
APN 179
interfaces 142
signal quality 115
SIM card 180
status 116
system 115
troubleshooting 639
certificate
troubleshooting 643
Certificate Authority (CA)
see certificates
Certificate Revocation List (CRL) 515
vs OCSP 529
certificates 514
advantages of 515
and CA 515
and FTP 576
and HTTPS 555
and IKE SA 363
and SSH 572
and VPN gateways 338
and WWW 558
certification path 515, 522, 527
expired 515
factory-default 515
file formats 516
fingerprints 523, 528
importing 518
in IPSec 350
not used for encryption 515
revoked 515
self-signed 515, 520
serial number 522, 527
storage space 518, 525
thumbprint algorithms 516
thumbprints 516
used for authentication 515
verifying fingerprints 516
certification requests 520
certifications 657
viewing 660
Challenge Handshake Authentication Protocol (CHAP) 531
CHAP (Challenge Handshake Authentication Protocol) 531
CHAP/PAP 531
CLI 22, 28
button 28
messages 28
popup window 28
Reference Guide 2
client 392
cloud-based network management system 583
commands 22
sent by Web Configurator 28
Common Event Format (CEF) 594, 601
compression (stac) 531
computer names 162, 200, 212, 218, 399
concurrent e-mail sessions 129, 437
configuration
information 616, 621
web-based SSL application example 533
configuration file

troubleshooting 645
configuration files 605
at restart 608
backing up 607
downloading 609, 626
downloading with FTP 576
editing 605
how applied 606
lastgood.conf 608, 611
managing 607
startup-config.conf 611
startup-config-bad.conf 608
syntax 606
system-default.conf 611
uploading 611
uploading with FTP 576
use without restart 605
connection
troubleshooting 641
connection monitor (in SSL) 124
connectivity check 161, 173, 180, 189, 199, 213, 343
console port
speed 544
contact information 647, 662
content filter
troubleshooting 638
content filtering 416, 417
and address groups 416, 417
and address objects 416, 417
and registration 419, 422
and schedules 416, 417
and user groups 416
and users 416
by category 416, 417, 423
by keyword (in URL) 417, 431
by URL 417, 430, 432, 433
by web feature 417, 430
cache 434
categories 423
category service 422
default policy 417
external web filtering service 422, 434
filter list 417
managed web pages 423
policies 416, 417
registration status 135, 419, 422
statistics 126
testing 424
uncategorized pages 423
unsafe web pages 422
URL for blocked access 419
cookies 23, 430
copyright 653
CPU usage 91
current date/time 86, 540
and schedules 497
daylight savings 542
setting manually 543
time server 544
current user list 124
custom
access user page 560
login page 560
customer support 647, 662

D

Data Encryption Standard, see DES
date 540
daylight savings 542
DCS 137
DDNS 250
backup mail exchanger 255
mail exchanger 255
service providers 250
troubleshooting 640
Dead Peer Detection, see DPD
default
security policy behavior 320
Default_L2TP_VPN_GW 397
Denial of Service (Dos) attacks 341
DES 359
device access
troubleshooting 637
DHCP 217, 539
and DNS servers 218
and domain name 539
and interfaces 217
pool 218
static DHCP 218
DHCP Unique IDentifier 146
DHCPv6 537
DHCP Unique IDentifier 146

diagnostics 616, 621
Diffie-Hellman key group 360
DiffServ 238
Digital Signature Algorithm public-key algorithm, see DSA
direct routes 230
directory 503
directory service 503
  file structure 504
disclaimer 653
Distinguished Name (DN) 505, 506, 508
DN 505, 506, 508
DNS 545
  address records 548
  domain name forwarders 550
  domain name to IP address 548
  IP address to domain name 549
  L2TP VPN 399
  Mail eXchange (MX) records 551
  pointer (PTR) records 549
DNS Blacklist see DNSBL 436
DNS inbound LB 292
DNS servers 55, 545, 550
  and interfaces 218
DNSBL 436, 440, 447
  see also anti-spam 436
documentation
  related 2
domain name 539
Domain Name System, see DNS
DPD 352
DSA 520
DSCP 231, 234, 407, 632
DUID 146
Dynamic Channel Selection 137
Dynamic Domain Name System, see DDNS
Dynamic Host Configuration Protocol, see DHCP.
dynamic peers in IPSec 341
DynDNS 250
DynDNS see also DDNS 250
Dynu 250

E

egress bandwidth 180, 189
e-mail 435
  daily statistics report 590
  header buffer 436
  headers 436
Encapsulating Security Payload, see ESP
encapsulation
  and active protocol 364
  IPSec 342
  transport mode 364
  tunnel mode 364
  VPN 364
encryption
  IPSec 343
  RSA 522
encryption algorithms 359
  3DES 359
  AES 359
  and active protocol 359
  DES 359
encryption method 531
enforcing policies in IPSec 342
ESP 342, 364
  and transport mode 365
Ethernet interfaces 142
  and OSPF 149
  and RIP 149
  and routing protocols 148
  basic characteristics 143
  virtual 214
exceptional services 301
extended authentication
  and VPN gateways 338
  IKE SA 363
Extended Service Set IDentification 470
ext-user
  troubleshooting 643

F

file extensions
  configuration files 605
  shell scripts 605

file manager 605
file sharing SSL application
create 534
Firefox 23
firmware
and restart 611
current version 86, 612
getting updated 611
uploading 611, 613
uploading with FTP 576
firmware upload
troubleshooting 645
flash usage 91
forcing login 299
FQDN 548
FTP 576
additional signaling port 272
ALG 267
and address groups 577
and address objects 577
and certificates 576
and zones 577
signaling port 272
with Transport Layer Security (TLS) 576
full tunnel mode 368, 372
Fully-Qualified Domain Name, see FQDN

G

Generic Routing Encapsulation, see GRE.
global SSL setting 373
user portal logo 374
GRE 219
GSM 180
Guide
CLI Reference 2
Quick Start 2

H

H.323 273
additional signaling port 271
ALG 267, 273
and RTP 273
and security policy 268
signaling port 271
HSDPA 180
HTTP
over SSL, see HTTPS
redirect to HTTPS 558
vs HTTPS 555
HTTP redirect 263
and application patrol 264
and interfaces 266
and policy routes 264
and security policy 264
packet flow 264
troubleshooting 640
HTTPS 555
and certificates 555
authenticating clients 555
avoiding warning messages 564
example 563
vs HTTP 555
with Internet Explorer 563
with Netscape Navigator 563
hub-and-spoke VPN, see VPN concentrator
HyperText Transfer Protocol over Secure Socket Layer, see HTTPS

I

ICMP 493
identifying
legitimate e-mail 435
spam 435
IEEE 802.1q VLAN
IEEE 802.1q. See VLAN.
IEEE 802.1x 470
IKE SA
aggressive mode 358, 362
and certificates 363
and RADIUS 363
and to-ZyWALL security policy 642
authentication algorithms 359, 360
content 361
Dead Peer Detection (DPD) 352
Diffie-Hellman key group 360
encryption algorithms 359
extended authentication 363

ID type 361
IP address, remote IPSec router 359
IP address, ZyXEL device 359
local identity 361
main mode 358, 362
NAT traversal 363
negotiation mode 358
password 363
peer identity 361
pre-shared key 361
proposal 359
see also VPN
user name 363
IMAP 436
inbound LB algorithm
least connection 294
least load 294
weighted round robin 294
inbound load balancing 292
time to live 295
incoming bandwidth 180, 189
ingress bandwidth 180, 189
interface
status 105
troubleshooting 638
interfaces 141
and DNS servers 218
and HTTP redirect 266
and layer-3 virtualization 142
and NAT 259
and physical ports 142
and policy routes 234
and static routes 237
and VPN gateways 338
and zones 142
as DHCP relays 217
as DHCP servers 217, 539
auxiliary, see also auxiliary interfaces.
backup, see trunks
bandwidth management 217, 225, 226
bridge, see also bridge interfaces.
cellular 142
DHCP clients 216
Ethernet, see also Ethernet interfaces.
gateway 217
general characteristics 142
IP address 216
metric 217
MTU 217
overlapping IP address and subnet mask 216
port groups, see also port groups.
PPPoE/PPTP, see also PPPoE/PPTP interfaces.
prerequisites 143
relationships between 143
static DHCP 218
subnet mask 216
trunks, see also trunks.
Tunnel, see also Tunnel interfaces.
types 142
virtual, see also virtual interfaces.
VLAN, see also VLAN interfaces.
WLAN, see also WLAN interfaces.
Internet access
troubleshooting 637, 642
Internet Control Message Protocol, see ICMP
Internet Explorer 23
Internet Message Access Protocol, see IMAP 436
Internet Protocol Security, see IPSec
Internet Protocol version 6, see IPv6
IP policy routing, see policy routes
IP pool 372
IP protocols 493
and service objects 493
ICMP, see ICMP
TCP, see TCP
UDP, see UDP
IP static routes, see static routes
IP/MAC binding 283
exempt list 286
monitor 112
static DHCP 285
IPSec 319, 333
active protocol 342
AH 342
and certificates 338
authentication 343
basic troubleshooting 641
certificates 350
connections 338
connectivity check 343
Default_L2TP_VPN_GW 397
encapsulation 342
encryption 343
ESP 342
established in two phases 336
L2TP VPN 396
local network 333

local policy 342
NetBIOS 341
peer 333
Perfect Forward Secrecy 343
PFS 343
phase 2 settings 342
policy enforcement 342
remote access 341
remote IPSec router 333
remote network 333
remote policy 342
replay detection 341
SA life time 342
SA monitor 123
SA see also IPSec SA 364
see also VPN
site-to-site with dynamic peer 341
static site-to-site 341
transport encapsulation 342
tunnel encapsulation 342
VPN gateway 338
IPSec SA
active protocol 364
and security policy 642
and to-ZyWALL security policy 642
authentication algorithms 359, 360
destination NAT for inbound traffic 367
encapsulation 364
encryption algorithms 359
local policy 364
NAT for inbound traffic 365
NAT for outbound traffic 365
Perfect Forward Secrecy (PFS) 365
proposal 365
remote policy 364
search by name 123
search by policy 123
Security Parameter Index (SPI) (manual keys) 365
see also IPSec
see also VPN
source NAT for inbound traffic 366
source NAT for outbound traffic 366
status 123
transport mode 364
tunnel mode 364
when IKE SA is disconnected 364
IPSec VPN
troubleshooting 641
IPv6 144
link-local address 145
prefix 144
prefix delegation 145
prefix length 144
stateless autoconfiguration 145
IPv6 tunnelings
6in4 tunneling 184
6to4 tunneling 184
IPv6-in-IPv4 tunneling 184
ISP account
CHAP 531
CHAP/PAP 531
MPPE 531
MSCHAP 531
MSCHAP-V2 531
PAP 531
ISP accounts 529
and PPPoE/PPTP interfaces 168, 529
authentication type 531
encryption method 531
stac compression 531

J

Java 430
permissions 23
JavaScripts 23

K

key pairs 514

L

L2TP VPN 396
Default_L2TP_VPN_GW 397
DNS 399
IPSec configuration 396
policy routes 397
session monitor 125
WINS 399
lastgood.conf 608, 611

Layer 2 Tunneling Protocol Virtual Private Network, see L2TP VPN 396
layer-2 isolation 288
example 288
IP 289
LDAP 503
and users 456
Base DN 505
Bind DN 505, 508
directory 503
directory structure 504
Distinguished Name, see DN
DN 505, 506, 508
password 508
port 508, 510
search time limit 508
SSL 508
user attributes 469
least connection algorithm 294
least load algorithm 294
least load first load balancing 220
LED troubleshooting 637
legitimate e-mail 435
licensing 134
Lightweight Directory Access Protocol, see LDAP
Link Layer Discovery Protocol (LLDP) 117
LLDP (Link Layer Discovery Protocol) 117
load balancing 219
algorithms 220, 224, 226
DNS inbound 292
least load first 220
round robin 221
see also trunks 219
session-oriented 220
spillover 221
weighted round robin 221
local user database 504
log
troubleshooting 644
log messages
categories 597, 599, 601, 602, 603
debugging 131
regular 131
types of 131
log options 439
login
custom page 560
SSL user 380
logo
troubleshooting 644
logo in SSL 374
logout
SSL user 385
Web Configurator 26
logs
and security policy 327
e-mail profiles 592
e-mailing log messages 596
formats 594
log consolidation 597
settings 592
syslog servers 592
system 592
types of 592

M

MAC address 467
and VLAN 190
Ethernet interface 157
range 86
MAC authentication 481
Calling Station ID 481
case 481
delimiter 481
mac role 467
mail sessions threshold 437
managed web pages 423
management access
troubleshooting 644
Management Information Base (MIB) 578
managing the device
using SNMP. See SNMP.
MD5 360
memory usage 91
Message Digest 5, see MD5
messages
CLI 28
metrics, see reports
Microsoft
Challenge-Handshake Authentication Protocol (MSCHAP) 531

Challenge-Handshake Authentication Protocol Version 2 (MSCHAP-V2) 531
Point-to-Point Encryption (MPPE) 531
mobile broadband see also cellular 174
model name 86
Monitor 584
monitor 124
SA 123
mounting
rack 21, 47
wall 47
MPPE (Microsoft Point-to-Point Encryption) 531
MSCHAP (Microsoft Challenge-Handshake Authentication Protocol) 531
MSCHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol Version 2) 531
MTU 180, 189
multicast 475
multicast rate 475
My Certificates, see also certificates 517
myZyXEL.com 134
accounts, creating 134

N

NAT 238, 256
ALG, see ALG
and address objects 235
and address objects (HOST) 259
and ALG 267, 269
and interfaces 259
and policy routes 228, 235
and security policy 322
and to-ZyWALL security policy 260
and VoIP pass through 269
and VPN 362
loopback 261
port forwarding, see NAT
port translation, see NAT
traversal 363
NAT Port Mapping Protocol 274
NAT Traversal 274
NAT-PMP 274
NBNS 162, 200, 212, 218, 372
NetBIOS
Broadcast over IPSec 341
Name Server, see NBNS.
NetBIOS Name Server, see NBNS
NetMeeting 273
see also H.323
Netscape Navigator 23
network access mode 20
full tunnel 368
Network Address Translation, see NAT
network list, see SSL 373
Network Time Protocol (NTP) 543
No-IP 250
NSSA 241

O

objects 369
AAA server 502
addresses and address groups 488
authentication method 511
certificates 514
schedules 497
services and service groups 492
SSL application 532
users, user groups 455
One-Time Password (OTP) 503
Online Certificate Status Protocol (OCSP) 529
vs CRL 529
Open Shortest Path First, see OSPF
OSPF 241
and Ethernet interfaces 149
and RIP 242
and static routes 242
and to-ZyWALL security policy 241
area 0 242
areas, see OSPF areas
authentication method 149
autonomous system (AS) 241
backbone 242
configuration steps 244
direction 149
link cost 149
priority 150
redistribute 242
redistribute type (cost) 245
routers, see OSPF routers
virtual links 243

vs RIP 239, 241
OSPF areas 241
and Ethernet interfaces 149
backbone 241
Not So Stubby Area (NSSA) 241
stub areas 241
types of 241
OSPF routers 242
area border (ABR) 242
autonomous system boundary (ASBR) 242
backbone (BR) 242
backup designated (BDR) 243
designated (DR) 243
internal (IR) 242
link state advertisements
priority 243
types of 242
other documentation 2
OTP (One-Time Password) 503
outgoing bandwidth 180, 189

P

packet
statistics 102, 103
packet capture 618
files 617, 621, 622, 623
troubleshooting 645
packet captures
downloading files 618, 621, 622, 623
PAP (Password Authentication Protocol) 531
Password Authentication Protocol (PAP) 531
Peanut Hull 250
Peer-to-peer (P2P)
calls 269
Perfect Forward Secrecy (PFS) 343
Diffie-Hellman key group 365
Personal Identification Number code, see PIN code
PFS (Perfect Forward Secrecy) 343, 365
physical ports
packet statistics 102, 103
PIN code 180
PIN generator 503
pointer record 549
Point-to-Point Protocol over Ethernet, see PPPoE.
Point-to-Point Tunneling Protocol, see PPTP
policy enforcement in IPSec 342
policy route
troubleshooting 638
policy routes 228
actions 229
and address objects 234
and ALG 269, 272
and HTTP redirect 264
and interfaces 234
and NAT 228
and schedules 234, 406, 410
and service objects 493
and trunks 220, 234
and user groups 233, 406, 410
and users 233, 406, 410
and VoIP pass through 269
and VPN connections 234, 642
benefits 228
BWM 230
criteria 229
L2TP VPN 397
overriding direct routes 230
POP
POP2 436
POP3 436
pop-up windows 23
port forwarding, see NAT
port groups 142, 147
port roles 146
and Ethernet interfaces 146
and physical ports 146
port translation, see NAT
Post Office Protocol, see POP 436
power off 636
PPP 218
troubleshooting 639
PPP interfaces
subnet mask 216
PPPoE 218
and RADIUS 218
TCP port 1723 219
PPPoE/PPTP interfaces 142, 167
and ISP accounts 168, 529
basic characteristics 143
gateway 168
subnet mask 168

PPTP 218
and GRE 219
as VPN 219
prefix delegation 145
problems 637
proxy servers 263
web, see web proxy servers
PTR record 549
Public-Key Infrastructure (PKI) 515
public-private key pairs 514

Q

QoS 228, 402
Quick Start Guide 2

R

rack-mounting 21, 47
RADIUS 503, 504
advantages 503
and IKE SA 363
and PPPoE 218
and users 456
user attributes 469
RADIUS server 581
troubleshooting 643
RDP 532
Real-time Transport Protocol, see RTP
RealVNC 532
Reference Guide, CLI 2
registration 134
and anti-spam 438
and content filtering 419, 422
related documentation 2
Relative Distinguished Name (RDN) 505, 506, 508
remote access IPSec 341
Remote Authentication Dial-In User Service, see RADIUS
remote desktop connections 532
Remote Desktop Protocol
see RDP
remote management
FTP, see FTP
see also service control 554
Telnet 574
to-Device security policy 320
WWW, see WWW
remote network 333
remote user screen links 532
replay detection 341
reports
collecting data 107
content filtering 126
daily 590
daily e-mail 590
specifications 108
traffic statistics 106
reset 645
RESET button 645
RFC
1058 (RIP) 239
1389 (RIP) 239
1587 (OSPF areas) 241
1631 (NAT) 238
1889 (RTP) 273
2131 (DHCP) 217
2132 (DHCP) 217
2328 (OSPF) 241
2402 (AH) 342, 364
2406 (ESP) 342, 364
2516 (PPPoE) 218
2637 (PPTP) 218
2890 (GRE) 219
3261 (SIP) 273
RIP 239
and Ethernet interfaces 149
and OSPF 239
and static routes 239
and to-ZyWALL security policyl 239
authentication 239
direction 149
redistribute 239
RIP-2 broadcasting methods 149
versions 149
vs OSPF 239
Rivest, Shamir and Adleman public-key algorithm (RSA) 520
round robin 221
routing
troubleshooting 640

Routing Information Protocol, see RIP
routing protocols 239
and authentication algorithms 248
and Ethernet interfaces 148
RSA 520, 522, 528
RSSI threshold 475
RTP 273
see also ALG 273

S

schedule
troubleshooting 643
schedules 497
and content filtering 416, 417
and current date/time 497
and policy routes 234, 406, 410
and security policy 303, 326, 406, 410
one-time 497
recurring 497
types of 497
screen resolution 23
SecuExtender 392
Secure Hash Algorithm, see SHA1
Secure Socket Layer, see SSL
security associations, see IPSec
security policy 319
actions 327
and address groups 303
and address objects 303
and ALG 267, 269
and H.323 (ALG) 268
and HTTP redirect 264
and IPSec VPN 642
and logs 327
and NAT 322
and schedules 303, 326, 406, 410
and service groups 326
and service objects 493
and services 326
and SIP (ALG) 268
and user groups 326, 330
and users 326, 330
and VoIP pass through 269
and zones 319, 325
asymmetrical routes 321, 324
global rules 320
priority 324
rule criteria 320
see also to-Device security policy 319
session limits 321, 327
triangle routes 321, 324
troubleshooting 638
security settings
troubleshooting 638
serial number 86
service control 554
and to-ZyWALL security policy 554
and users 555
limitations 554
timeouts 555
service groups 493
and security policy 326
service objects 492
and IP protocols 493
and policy routes 493
and security policy 493
Service Set 470
service subscription status 135
services 492
and security policy 326
Session Initiation Protocol, see SIP
session limits 321, 327
session monitor (L2TP VPN) 125
sessions 109
sessions usage 91
SHA1 360
shell script
troubleshooting 645
shell scripts 605
and users 469
downloading 614
editing 613
how applied 606
managing 613
syntax 606
uploading 615
shutdown 636
signal quality 115
SIM card 180
Simple Mail Transfer Protocol, see SMTP 436
Simple Network Management Protocol, see SNMP

Simple Traversal of UDP through NAT, see STUN
SIP 268, 273
ALG 267
and RTP 273
and security policy 268
media inactivity timeout 271
signaling inactivity timeout 271
signaling port 271
SMTP 436
SNAT 238
troubleshooting 640
SNMP 22, 577, 578
agents 578
and address groups 581
and address objects 581
and zones 581
Get 578
GetNext 578
Manager 578
managers 578
MIB 578
network components 578
Set 578
Trap 578
traps 578
version 3 and security 578
versions 577
Source Network Address Translation, see SNAT
spam 318, 435
spillover (for load balancing) 221
SSH 570
and address groups 573
and address objects 573
and certificates 572
and zones 573
client requirements 572
encryption methods 572
for secure Telnet 573
how connection is established 571
versions 572
with Linux 574
with Microsoft Windows 573
SSL 368, 372, 555
access policy 368
and AAA 508
and AD 508
and LDAP 508
certificates 380
client 392
client virtual desktop logo 374
computer names 372
connection monitor 124
full tunnel mode 372
global setting 373
IP pool 372
network list 373
remote user login 380
remote user logout 385
SecuExtender 392
see also SSL VPN 368
troubleshooting 642
user application screens 385
user file sharing 386
user screen bookmarks 384
user screens 379, 383
user screens access methods 379
user screens certificates 380
user screens login 380
user screens logout 385
user screens required information 380
user screens system requirements 379
WINS 372
SSL application object 532
file sharing application 534
remote user screen links 532
summary 534
types 532
web-based 532, 534
web-based example 533
SSL policy
add 370
edit 370
objects used 369
SSL VPN 368
access policy 368
full tunnel mode 368
network access mode 20
remote desktop connections 532
see also SSL 368
troubleshooting 642
weblink 533
stac compression 531
startup-config.conf 611
if errors 608
missing at restart 608
present at restart 608
startup-config-bad.conf 608

static DHCP 285
static routes 228
  and interfaces 237
  and OSPF 242
  and RIP 239
  metric 237
station 137
statistics
  content filtering 126
  daily e-mail report 590
  traffic 106
status 83
stub area 241
STUN 268
  and ALG 268
subscription services
  SSL VPN 134
  SSL VPN, see also SSL VPN
  status 135
supported browsers 23
SWM 230
syslog 594, 601
syslog servers, see also logs
system log, see logs
system name 86, 539
system reports, see reports
system uptime 86
system-default.conf 611

T

TCP 493
  connections 493
  port numbers 493
Telnet 574
  and address groups 575
  and address objects 575
  and zones 575
  with SSH 573
throughput rate
  troubleshooting 644
TightVNC 532
time 540
time servers (default) 543
to-Device security policy
  and remote management 320
  global rules 320
  see also security policy 319
token 503
to-ZyWALL security policy
  and NAT 260
  and NAT traversal (VPN) 642
  and OSPF 241
  and RIP 239
  and service control 554
  and VPN 642
TR-069 protocol 583
traffic statistics 106
Transmission Control Protocol, see TCP
transport encapsulation 342
Transport Layer Security (TLS) 576
triangle routes 321
  allowing through the security policy 324
  vs virtual interfaces 321
Triple Data Encryption Standard, see 3DES
troubleshooting 616, 621, 637
  admin user 643
  bandwidth limit 640
  cellular 639
  certificate 643
  configuration file 645
  connection resets 641
  content filter 638
  DDNS 640
  device access 637
  ext-user 643
  firmware upload 645
  HTTP redirect 640
  interface 638
  Internet access 637, 642
  IPSec VPN 641
  LEDs 637
  logo 644
  logs 644
  management access 644
  packet capture 645
  policy route 638
  PPP 639
  RADIUS server 643
  routing 640
  schedules 643
  security policy 638

security settings 638
shell scripts 645
SNAT 640
SSL 642
SSL VPN 642
throughput rate 644
VLAN 640
VPN 642
WLAN 639
trunks 142, 219
and ALG 272
and policy routes 220, 234
member interface mode 224, 226
member interfaces 224, 226
see also load balancing 219
Trusted Certificates, see also certificates 524
tunnel encapsulation 342
Tunnel interfaces 142

U

UDP 493
messages 493
port numbers 493
UltraVNC 532
Universal Plug and Play 274
Application 274
security issues 275
unsafe web pages 422
unsolicited commercial e-mail 318, 435
upgrading
firmware 611
uploading
configuration files 611
firmware 611
shell scripts 613
UPnP 274
usage
CPU 91
flash 91
memory 91
onboard flash 91
sessions 91
user accounts
for WLAN 457
user authentication 456
external 456
local user database 504
user awareness 457
User Datagram Protocol, see UDP
user group objects 455
user groups 455, 457
and content filtering 416
and policy routes 233, 406, 410
and security policy 326, 330
user name
rules 458
user objects 455
user portal
links 532
logo 374
see SSL user screens 379, 383
user sessions, see sessions
user SSL screens 379, 383
access methods 379
bookmarks 384
certificates 380
login 380
logout 385
required information 380
system requirements 379
users 455, 456
access, see also access users
admin (type) 456
admin, see also admin users
and AAA servers 456
and authentication method objects 456
and content filtering 416
and LDAP 456
and policy routes 233, 406, 410
and RADIUS 456
and security policy 326, 330
and service control 555
and shell scripts 469
attributes for Ext-User 457
attributes for LDAP 469
attributes for RADIUS 469
attributes in AAA servers 469
currently logged in 87
default lease time 464, 466
default reauthentication time 464, 466
default type for Ext-User 457
ext-group-user (type) 456
Ext-User (type) 456

ext-user (type) 456
groups, see user groups
Guest (type) 456
lease time 460
limited-admin (type) 456
lockout 465
reauthentication time 460
types of 456
user (type) 456
user names 458

V

Vantage Report (VRPT) 594, 601
virtual interfaces 142, 214
basic characteristics 143
not DHCP clients 216
types of 214
vs asymmetrical routes 321
vs triangle routes 321
Virtual Local Area Network, see VLAN.
Virtual Local Area Network. See VLAN.
Virtual Network Computing
see VNC
Virtual Private Network, see VPN
VLAN 183, 189
advantages 190
and MAC address 190
ID 190
troubleshooting 640
VLAN interfaces 142, 191
and Ethernet interfaces 191, 640
basic characteristics 143
virtual 214
VoIP pass through 273
and NAT 269
and policy routes 269
and security policy 269
see also ALG 267
VPN 333
active protocol 364
and NAT 362
basic troubleshooting 641
hub-and-spoke, see VPN concentrator
IKE SA, see IKE SA
IPSec 319, 333
IPSec SA
proposal 359
security associations (SA) 336
see also IKE SA
see also IPSec 319, 333
see also IPSec SA
status 87
troubleshooting 642
VPN concentrator 354
advantages 354
and IPSec SA policy enforcement 356
disadvantages 354
VPN connections
and address objects 338
and policy routes 234, 642
VPN gateways
and certificates 338
and extended authentication 338
and interfaces 338
and to-ZyWALL security policy 642
VRPT (Vantage Report) 594, 601

W

wall-mounting 47
warranty 660
note 661
Web Configurator 22
access 23
access users 466
requirements 23
supported browsers 23
web features
ActiveX 430
cookies 430
Java 430
web proxy servers 430
web proxy servers 264, 430
see also HTTP redirect
web-based SSL application 532
configuration example 533
create 534
weblink 533
weighted round robin (for load balancing) 221
weighted round robin algorithm 294
WEP (Wired Equivalent Privacy) 470

white list (anti-spam) 435, 439, 444, 445
Wi-Fi Protected Access 470
Windows Internet Naming Service, see WINS
Windows Internet Naming Service, see WINS.
Windows Remote Desktop 532
WINS 162, 200, 212, 218, 372
  in L2TP VPN 399
WINS server 162, 399
wireless client 137
Wizard Setup 37, 50
WLAN
  troubleshooting 639
  user accounts 457
WLAN interfaces 142
WPA 470
WPA2 470
WWW 556
  and address groups 559
  and address objects 559
  and authentication method objects 559
  and certificates 558
  and zones 560
  see also HTTP, HTTPS 556

Z

ZON Utility 587
zones 453
  and FTP 577
  and interfaces 453
  and security policy 319, 325
  and SNMP 581
  and SSH 573
  and Telnet 575
  and VPN 453
  and WWW 560
  extra-zone traffic 454
  inter-zone traffic 454
  intra-zone traffic 453
  types of traffic 453