FGX

celestix

Integrated Security Software v4.2

Advanced User's Guide

Celestix Networks, Inc.
3125 Skyway Court P +1 510.668.0700
Fremont CA 94539 F +1 510.668.0710

Contents

About the User Guide 23
Document Conventions 24
Related Documentation 24

1 Quick Start 1
1.1 Hardware and system installation 1
1.2 Connect device to management PC 2
1.2.1 Connect Ethernet interface 2
1.2.2 Connect console port 2
1.3 Connect device to network (determine topology) 3
1.3.1 Transparent mode 3
1.3.2 Routing mode 3
1.4 Initialize configurations using Wizard 4
1.4.1 Login 4
1.4.2 Set system language / host name / system time 5
1.4.3 Configure transparent mode (Layer 2) 6
1.4.3.1 Network settings 6
1.4.3.2 Security settings 7
1.4.3.3 Review and save settings (overview) 7
1.4.3.4 Verify initialized configurations using WebUI 8
1.4.4 Configure routing mode (Layer 3) 11
1.4.4.1 Network settings 12
1.4.4.2 Network NAT settings 14
1.4.4.3 Security settings 15
1.4.4.4 Review and save settings (overview) 15
1.4.4.5 Verify initialized configurations using WebUI 16
1.4.5 Reset password 18
1.4.6 Import license 18
1.5 Initialize configurations using WebUI 19
1.5.1 Login 19
1.5.2 WebUI overview 20
1.5.3 Reset password 21
1.5.4 Set system language / host name /system time 22
1.5.5 Configure transparent mode 23
1.5.6 Configure routing mode 26
1.5.6.1 Ethernet connection 26

1.5.6.2 PPPoE connection 27
1.5.7 Import license 28
1.6 Initialize configurations using CLI 29
1.6.1 Logon using Console 29
1.6.2 CLI basics 31
1.6.3 Set system language / host name / system time 32
1.6.4 Reset password 32
1.6.5 Configure transparent mode 33
1.6.6 Routing Mode 35
1.6.6.1 Ethernet connection 35
1.6.6.2 PPPoE connection 37
1.6.7 Import license 39
1.6.8 Logon using SSH 39
1.6.9 Logon using Telnet 40
1.7 Verify initialized configurations 41
1.8 Common problems 43
1.9 Next steps 44

2 Functional overview 45

2.1. System configuration 46
2.2. Network configuration 47
2.3. Packet processing overview 48
2.4. Routing 50
2.4.1. Layer 3 Unicast 50
2.4.2 Layer 3 Multicast 52
2.4.3 Layer 2 Multicast 53
2.5. Network Address Translation (NAT) 54
2.6. Quality of service (QoS) 55
2.7. Firewall policies 56
2.8. Attack defense 59
2.9. Unified threat management (UTM) 60
2.9.1. Application control 61
2.9.1.1 Packet processing 61
2.9.1.2 Configuration steps 61
2.9.2. HTTP control 62
2.9.2.1 Packet processing 62
2.9.2.2 Configuration steps 62
2.9.3. DNS control 63
2.9.3.1 Packet processing 63
2.9.3.2 Configuration steps 63
2.9.4. Client protection 64
2.9.4.1 Packet processing 64
2.9.4.2 Configuration steps 65

2.9.5. Server protection 66
2.9.5.1 Packet processing 66
2.9.5.2 Configuration steps 67
2.10. Virtual private networks (VPN) 68
2.10.1. IPSec VPN 68
2.10.2. SSL VPN Web Portal 69
2.10.3. SSL VPN Tunnel 70
2.11. High availability (HA) 71
2.12. Virtual systems/networks (Vsys/Vnet) 72
2.13. Monitor/Logs 73
2.14. Reports 73

3 System Configuration 75

3.1 Home 76
3.2 System Overview 78
3.2.1 Basic Configuration Steps 78
3.2.2 Parameters 79
3.3 Banners 80
3.3.1 Overview 80
3.3.2 Basic Configuration Steps 80
3.4 Asset Summary 81
3.5 Copyright Information 82
3.6 System Time 83
3.6.1 Overview 83
3.6.2 Basic Configuration Steps 84
3.6.3 Parameters 86
3.7 Licenses 87
3.7.1 Overview 87
3.7.2 Basic Configuration Steps 88
3.7.3 Parameters 90
3.8 Update 91
3.8.1 Overview 91
3.8.2 Basic Configuration Steps 92
3.8.3 Parameters 93
3.9 Installation Package Management 94
3.10 Patch Package Management 95
3.11 Access Services 96
3.11.1 Basic Configuration Steps 96
3.11.2 Parameters 97
3.12 SNMP 98
3.12.1 Overview 98
3.12.2 Basic Configuration Steps 99

3.12.3 Parameters 101
3.13 Administrative Users 102
3.13.1 Overview 102
3.13.1.1 Administrative Users 102
3.13.1.2 Configuration Lock 103
3.13.2 Basic Configuration Steps 104
3.13.3 Parameters 105
3.14 Users 106
3.14.1 Overview 106
3.14.2 Basic Configuration Steps 107
3.14.3 Parameters 108
3.15 User Authentication 109
3.15.1 Overview 109
3.15.1.1 Local&External Authentications 109
3.15.1.2 External Authentication Servers 109
3.15.2 Basic Configuration Steps 110
3.15.3 Parameters 112
3.16 WebAuth Configuration 113
3.16.1 Overview 113
3.16.2 Basic Configuration Steps 114
3.16.3 Parameters 116
3.16.4 Example: User Authentication 117
3.16.4.1 Configure an LDAP Server 118
3.16.4.2 Set the LDAP Server on FGX 118
3.16.4.3 Specify User Authentication Server 119
3.16.4.4 Enable WebAuth for the Interface 119
3.16.4.5 Enable WebAuth for the User 120
3.16.4.6 Create a WebAuth (Automatic Redirection) Policy 120
3.16.4.7 User enters destination IP 121
3.16.4.8 User enters authentication IP 121
3.17 Backup and Restore 122
3.17.1 Overview 122
3.17.2 Basic Configuration Steps 122
3.18 Technical Support 124
3.18.1 Overview 124
3.18.2 Basic Configuration Steps 124
3.19 Centralized Management 125
3.19.1 Overview 125
3.19.2 Basic Configuration Steps 125
3.20 Diagnosis Tools 126
3.20.1 Ping 126
3.20.2 Traceroute 126
3.20.3 Debug 127

3.20.3.1 General Debug . . . 127
3.20.3.2 VPN Debug . . . 128
3.20.3.3 PPPoE Debug . . . 128
3.21 Alert Configuration . . . 129
3.21.1 Overview . . . 129
3.21.2 Basic Configuration Steps . . . 130
3.21.3 Parameters . . . 132
3.22 Log Maintenance . . . 134
3.22.1 Overview . . . 134
3.22.2 Basic Configuration Steps . . . 135
3.22.3 Parameters . . . 136
3.23 Certificates . . . 138
3.23.1 Overview . . . 138
3.23.2 Basic Configuration Steps . . . 139
3.23.3 Example: Generate Certificates . . . 141
3.23.3.1 Create a Certificate Request . . . 142
3.23.3.2 Enroll Certificate Automatically . . . 143
3.23.4 Parameters / Local certificates . . . 145
3.23.5 Parameters / CA certificates . . . 147
3.24 Objects . . . 148
3.24.1 IP Addresses . . . 148
3.24.1.1 Basic Configuration Steps . . . 148
3.24.1.2 IP Address Object Parameters . . . 149
3.24.1.3 IP Address Object Group Parameters . . . 149
3.24.2 Services . . . 150
3.24.2.1 Basic Configuration Steps . . . 150
3.24.2.2 Service Object Parameters . . . 151
3.24.2.3 Service Object Group Parameters . . . 151

4 Network Configuration . . . 153

4.1 Interfaces Overview . . . 154
4.1.1 Working Modes . . . 154
4.1.2 Interface Attributes . . . 154
4.1.2.1 Common Attributes . . . 155
4.1.2.2 Layer 2 Specific Attributes . . . 156
4.1.2.3 Layer 3 Specific Attributes . . . 157
4.2 Ethernet Interface . . . 158
4.2.1 Overview . . . 158
4.2.2 Basic configuration steps . . . 159
4.2.2.1 Layer 2 . . . 159
4.2.2.2 Layer 3 . . . 161
4.2.2.3 Shared Layer 3 . . . 164

4.2.3 Example: Ethernet Interface 165
4.3 Ethernet Channel 167
4.3.1 Overview 167
4.3.2 Basic configuration steps 167
4.3.2.1 Layer 2 167
4.3.2.2 Layer 3 169
4.3.2.3 Shared Layer 3 169
4.4 Redundant Interface 170
4.4.1 Overview 170
4.4.2 Basic configuration steps 170
4.4.2.1 Layer 2 170
4.4.2.2 Layer 3 172
4.4.2.3 Shared Layer 3 173
4.5 Virtual Interface 174
4.5.1 Overview 174
4.5.2 Basic configuration steps 174
4.5.2.1 Layer 2 174
4.5.2.2 Layer 3 175
4.6 VLAN Interface 176
4.6.1 Overview 176
4.6.2 Basic configuration steps 176
4.6.3 Example: VLAN Interface 178
1. Configure vlan201 179
2. Configure vlan202 180
4.7 Loopback Interface 181
4.7.1 Overview 181
4.7.2 Basic configuration steps 181
4.8 PPPoE Interface 183
4.8.1 Overview 183
4.8.2 Basic configuration steps 183
4.8.3 Parameter reference 186
4.9 Tunnel Interface 187
4.9.1 Overview 187
4.9.2 Basic configuration steps 187
4.9.3 Parameter reference 189
4.10 ARP 190
4.10.1 Overview 190
4.10.2 Basic configuration steps 190
4.10.3 Parameter reference 191
4.11 CAM 192
4.11.1 Overview 192
4.11.2 Basic configuration steps 192

4.11.3 Parameter reference 193
4.12 Zones 194
4.12.1 Overview 194
4.12.2 Basic configuration steps 194
4.12.3 Example: Zone Application 196
4.12.4 Parameter reference 198
4.13 DNS Host 199
4.13.1 Overview 199
4.13.2 Basic configuration steps 199
4.13.3 Parameter reference 199
4.14 DNS Proxy 200
4.14.1 Overview 200
4.14.2 Basic configuration steps 200
4.14.3 Parameter reference 201
4.15 DNS Cache 202
4.15.1 Overview 202
4.15.2 Basic configuration steps 202
4.15.3 Parameter reference 203
4.16 DHCP Servers 204
4.16.1 Overview 204
4.16.2 Basic configuration steps 204
4.16.3 DHCP Examples 206
Example 1: Configure DHCP Server 206
Example 2: Configure DHCP Relay Agent 208
4.16.4 Parameter reference 209
4.17 DHCP Server Subnets 210
4.17.1 Overview 210
4.17.2 Basic configuration steps 210
4.17.3 Parameter reference 212
4.18 DHCPv6 213
4.18.1 Overview 213
4.18.2 Basic configuration steps 213
4.18.3 DHCPv6 Examples 215
Example 1: Configure DHCPv6 Client 215
Example 2: Configure Stateless DHCPv6 Server 217
4.18.4 Parameter reference 219
4.19 STP 221
4.19.1 Overview 221
4.19.1.1 STP 221
4.19.1.2 RSTP 221
4.19.2 Basic configuration steps 222
4.19.3 Example: STP Application 224
1. Create Interfaces 225

2. Create Virtual Systems. 227
3. Create Virtual Networks 228
4. Configure STP 230
5. View Results. 231
4.19.4 Parameter reference 232
4.20 Neighbor Discovery. 233
4.20.1 Overview 233
4.20.2 Basic Configuration Steps. 234
4.20.3 ND Examples 235
Example 1: Duplicate Address Detection. 235
Example 2: Configure Router Advertisement. 238
4.20.4 Parameter reference 241

5 Network Address Translation 243

5.1. Overview 244
5.1.1. NAT Rule Creation and Selection 244
5.1.1.1. Rule List 244
5.1.1.2. Rule Policy 244
5.1.1.3. Rule Priority (number) 244
5.1.2. SNAT Rules 245
5.1.2.1. Policy and Priority. 245
5.1.2.2. NAPT 246
5.1.2.3. Hold Time. 246
5.1.2.4. One-to-One 246
5.1.2.5. Many-to-One 247
5.1.2.6. Many-to-Many 248
5.1.3. DNAT Rules 249
5.1.3.1. Policy and Priority. 249
5.1.3.2. NAPT 249
5.1.3.3. One-to-One 250
5.1.3.4. One-to-Many 251
5.1.3.5. Load Balancing. 252
5.1.3.6. Link Probes 252
5.1.3.7. Domain Name (DNS Rewrite) 252
5.1.4. MIP Rules. 253
5.1.4.1. Policy and Priority. 253
5.1.4.2. Domain Name (DNS Rewrite) 254
5.1.5. Import / Export 254
5.2. Basic Configuration Steps 255
5.2.1. Create SNAT Rule 255
5.2.1.1. Create Rule 255
5.2.1.2. Advanced Settings 256
5.2.1.3. One-to-One SNAT without NAPT. 256

5.2.1.4. Many-to-One SNAT with NAPT 257
5.2.1.5. Many-to-Many SNAT with NAPT 257
5.2.2. Create DNAT Rule 258
5.2.2.1. Create Rule 258
5.2.2.2. Advanced Settings 258
5.2.2.3. One-to-One DNAT without NAPT 258
5.2.2.4. One-to-One DNAT with NAPT 259
5.2.2.5. One-to-Many DNAT with NAPT 259
5.2.3. Create MIP Rule 260
5.2.3.1. Create Rule 260
5.2.3.2. Advanced Settings 260
5.2.3.3. One-to-One Mapping 260
5.3. Examples 262
Example 1: Create One-to-One SNAT Rule 262
Example 2: Create Many-to-One SNAT Rule with NAPT 264
Example 3: Create One-to-One DNAT Rule 266
Example 4: Create One-to-Many DNAT Rule with NAPT 268
Example 5: Create MIP Rule 270
Example 6: DNS Rewrite 272
5.4. Parameter Reference 274
5.4.1. SNAT Rule Parameters 274
5.4.2. DNAT Rule Parameters 275
5.4.3. MIP Rule Parameters 277

6 Routing 279

6.1. Overview 280
6.1.1 L3 Unicast 280
6.1.1.1 (Default policy) routes 280
6.1.1.2 Load balancing / link probe 281
6.1.1.3 Policy-based routing 282
6.1.2 L3 Multicast 283
6.1.2.1 L3 Multicast dynamic 283
6.1.2.2 L3 Multicast static 283
6.1.3 L2 Multicast 284
6.1.3.1 L2 Multicast dynamic (IGMP snooping) 284
6.1.3.2 L2 Multicast static 284
6.2. Basic Configuration Steps 285
6.2.1 L3 Unicast 285
6.2.2 L3 Multicast 289
6.2.2.1 L3 Multicast Dynamic 289
6.2.2.2 L3 Multicast Static 290
6.2.3 L2 Multicast 291
6.2.3.1 L2 multicast dynamic 291

6.2.3.2 L2 multicast static 292
6.3. Basic examples 293
6.3.1 Unicast 293
6.3.1.1 (Default policy) routes 293
6.3.1.2 Route load balancing. 295
6.3.1.3 Policy-based route. 296
6.3.2 L3 Multicast 297
6.3.2.1 L3 Multicast Dynamic 297
6.3.2.2 L3 Multicast Static 298
6.3.3 L2 multicast 299
6.3.3.1 L2 Multicast Dynamic 299
6.3.3.2 L2 Multicast Static 300
6.4. Advanced Examples 301
Example 1: L3 Unicast: (default policy) Route / Load Balancing 301
Example 2: L3 Unicast: Policy-based routes. 303
Example 3: L3 multicast dynamic (DVMRP) 306
Example 4: L3 multicast static. 308
Example 5: L2 multicast dynamic (IGMP Snooping). 310
Example 6: L2 multicast static. 311
6.5. Parameter Reference. 313
6.5.1 L3 Unicast Route Parameters 313
6.5.2 L3 Unicast Policy Parameters 314
6.5.3 L3 multicast dynamic (DVMRP) Parameters. 315
6.5.4 L3 multicast Static Parameters 315
6.5.5 L2 multicast dynamic (IGMP Snooping) Parameters 316
6.6. L2 multicast Static (CAM Entry) Parameters 316

7 Quality of Service 317

7.1. Basic Concepts 318
7.2. Basic configuration steps 319
7.2.1 Create general QoS profiles 320
7.2.2 Create per IP/user QoS profiles 320
7.2.3 Create QoS policies 321
7.3. Example 325
7.3.1. Create general QoS profiles (max/min bandwidth) 326
7.3.2. Create per-IP QoS profile (max bandwidth) 326
7.3.3. Edit QoS levels 326
7.3.4. Create multi-level QoS policies 327
7.4. Parameter reference 328
7.4.1. QoS Policies. 328
7.4.2. QoS Profiles 329

7.4.3. Per IP/User QoS Profiles 329

8 Policies 331

8.1. Overview 332
8.1.1 IP-MAC Binding 332
8.1.1.1 IP-MAC Binding Policies 332
8.1.1.2 Policy Matching Order 332
8.1.2 Access Policies 332
8.1.2.1 Policy Content 332
8.1.2.2 How a Policy Is Enforced 333
8.1.3 Default Access Policies 333
8.1.4 Multicast Policies 333
8.1.5 Session Policies 333
8.1.5.1 Source IP Based Session Limit 334
8.1.5.2 Destination IP Based Session Limit 334
8.1.5.3 Policy-Based Session Limit 335
8.2. Basic Configuration Steps 336
8.2.1 Configure IP-MAC Binding 336
8.2.1.1 Create IP-MAC Binding Policy 336
8.2.1.2 Set Default Action 337
8.2.2 Create Access Policy 338
8.2.3 Configure Default Access Policies 340
8.2.4 Create Multicast Policy 341
8.2.5 Create Session Policy 342
8.3. Examples 344
Example 1. Create IP-MAC Binding Policy 345
Example 2. Create Access Policy 347
Example 3. Apply Multicast Policy Among Zones 350
3.1 Enable DVMRP 351
3.2 Create Static Multicast Route 352
3.3 Create Multicast Policy 353
Example 4. Create Destination IP-Based Session Policy 354
8.4. Parameter Reference 356
8.4.1 IP-MAC Binding Policy Parameters 356
8.4.2 Access Policy Parameters 357
8.4.3 Multicast Policy Parameters 360
8.4.4 Session Policy Parameters 361

9 Attack Defense 363

9.1. Basic Concepts 364
9.1.1. Attack Goals 364
9.1.2. Attack Types 364

9.1.3. Countermeasures 364
9.2. Attack Types / Tactics / Countermeasures 365
9.3. Basic Configuration Steps 374
9.3.1. Create a Zone 374
9.3.2. Apply Attack Defense 375
9.3.2.1. DoS Defense 376
9.3.2.2. Reconnaissance Defense 376
9.3.2.3. TCP Evasion Control 377
9.3.2.4. IP Option Check 378
9.3.2.5. ICMP Attack Defense 379
9.4. Parameter Reference 380
9.4.1. DoS Defense Parameters 380
9.4.2. ICMP Attack Defense Parameters 381
9.4.3. IP Option Check Parameters 382
9.4.4. Reconnaissance Defense 382
9.4.5. TCP Evasion Control Parameters 383

10 Unified Threat Management 385
10.1. Overview 386
10.1.1. Export control 387
10.1.1.1. Application packet processing 387
10.1.1.2. HTTP packet processing 387
10.1.1.3. DNS packet processing 387
10.1.2. Client protection 388
10.1.2.1. Basic steps 388
10.1.2.2. IPS 389
10.1.2.3. Anti-Virus 390
10.1.2.4. Anti-Spam 391
10.1.3. Server protection 392
10.1.3.1. Basic steps 392
10.1.3.2. IPS, AV, AS 392
10.2. Basic Configuration 393
10.2.1. Export control 394
10.2.1.1. Create zones, access policies, default route, NAT rules 395
10.2.1.2. Configure application control 396
10.2.1.3. Configure (HTTP request) URL filtering 400
10.2.1.4. Configure (HTTP response) page filtering 404
10.2.1.5. Configure DNS domain blacklist 405
10.2.2. Client protection 406
10.2.2.1. Create zones, access policies, default route, NAT rules 407
10.2.2.2. Update AV, AS, IPS rules 407
10.2.2.3. Configure global AV actions (trusted list, action when virus detected, heuristic, scan limits) 410

10.2.2.4. Configure global AS actions (allow/block list, spam word list, scan) . 412
10.2.2.5. Configure IPS client SMTP, POP3, IMAP, DNS protocol restriction . 416
10.2.2.6. Configure DNS CPD global actions 416
10.2.2.7. Create AV, AS, IPS action profiles 417
10.2.2.8. Create client protection policies 425
10.2.2.9. Create trusted server / email list 428
10.2.3. Server protection 429
10.2.3.1. Create zones, access policies, default route, NAT rules 430
10.2.3.2. Update AV, AS, IPS rules 430
10.2.3.3. Configure global AV actions (trusted list, action when virus detected, heuristic, scan limits) 430
10.2.3.4. Configure global AS actions (allow/block list, spam word list, scan failures) 430
10.2.3.5. Configure IPS server HTTP, SMTP, POP3, IMAP, DNS protocol restriction 430
10.2.3.6. Configure web/mail protection global actions 431
10.2.3.7. Create AV, AS, IPS action profiles 433
10.2.3.8. Create server protection policies 434
10.2.3.9. Create trusted client / mail address list 439
10.2.4. Notification messages 440
10.2.5. Overview page 441
10.3. Scenarios 442
Scenario 1: Export Control 442
Scenario 2: Client Protection 442
Scenario 3: Server Protection 442
10.4. UTM Examples 443
Example 1: Typical Application of UTM Export Control 443
1. Create interfaces, zones, default route, access policies, and NAT rules . . 444
5. 2. Configure Application Control 445
3. Configure URL Filtering 448
4. Configure DNS Domain Blacklist 453
5. Configure Page Filtering 454
Example 2: Typical Application of UTM Client Protection 456
1. Modify Access Policies 457
2. Configure Anti-Virus 457
3. Configure Anti-Spam 458
4. Configure DNS Cache Poisoning Defense 459
5. Create Client Protection Policy 459
10. 6. Monitor Client Protection 462
3. Example 3: Typical Application of UTM Server Protection 469
1. Modify Access Policies 469
2. Configure Anti-Virus 470
3. Configure Anti-Spam 470

4. Create Server Protection Policies 471
5. Configure Web Protection 475
6. Configure Mail Protection 475
4. 7. Monitor Server Protection 476
10.5. Parameter reference 480
10.5.1. Overview 480
10.5.2. Export Control 481
10.5.2.1. (Export Control) Policies 481
10.5.2.2. Application Control 484
10.5.2.3. URL Filtering 487
10.5.2.4. DNS Domain Blacklist 490
10.5.2.5. Page Filtering 490
10.5.3. Client Protection 491
10.5.3.1. (Client Protection) Policies 491
10.5.3.2. (Client Protection) Trusted Server List 493
10.5.3.3. (Client Protection) Trusted Mail Address List 493
10.5.3.4. DNS Cache Poisoning Defense 494
10.5.4. Server protection 495
10.5.4.1. (Server Protection) Policies 495
10.5.4.2. (Server Protection) Trusted Client List 497
10.5.4.3. (Server Protection) Trusted Mail Address List 497
10.5.4.4. Web Protection 498
10.5.4.5. Mail Protection 500
10.5.5. Anti-Virus 501
10.5.5.1. (AV) General Settings 502
10.5.5.2. Trusted URLs 503
10.5.5.3. Trusted Web Servers 503
10.5.5.4. Trusted Clients 503
10.5.5.5. (Anti-Virus) Profiles 504
10.5.5.6. (Anti-Virus Rule) Update 505
10.5.6. Anti-Spam 506
10.5.6.1. (Anti-Spam) General Settings 506
10.5.6.2. Allow List 509
10.5.6.3. Block List 510
10.5.6.4. Spam Word List 511
10.5.6.5. (Anti-Spam) Profiles 512
10.5.6.6. (Anti-Spam Rule) Update 513
10.5.7. IPS 514
10.5.7.1. (IPS) Profiles 514
10.5.7.2. Protocol restriction 516
10.5.7.3. (Attack Signature Rule) Update 523

10.5.8. Notification Messages 524

11 Virtual Private Network 2 527

11.1. Concepts 528
11.1.1. Site-to-Site IPSec Manual Tunnel 529
11.1.1.1. Requirements 529
11.1.1.2. Implementation (packet modifications) 529
11.1.1.3 IPSec SA Security Protocols and Working Modes 530
11.1.2. Site to Site IPSec Auto IKE 533
11.1.2.1. Requirements 533
11.1.2.2. Implementation 534
11.1.3. Site to Remote Peer IPSec Auto IKE 537
11.1.3.1. Requirements 537
11.1.3.2. Solution 537
11.1.4. Browser to Site Portal SSL/TLS 538
11.1.4.1. Requirements 538
11.1.4.2. Solution 538
11.1.4.3. Implementation 539
11.1.5. Client to Site SSL/TLS. 540
11.1.5.1. Requirements 540
11.1.5.2. Solution 540
11.1.6. Site to Site IPSec VPN (tunnel mode) + NAT 541
11.1.6.1. SNAT. 541
11.1.6.2. DNAT. 541
11.1.6.3. MIP 542
11.1.7. VPN with Virtual Routers (HA) 543
11.2. Configuration Basics 544
11.2.1. Site to Site IPSec Manual SA (example 1) 544
11.2.1.1. Pre-Planning 544
11.2.1.2. Configuration Steps. 544
11.2.2. Site to Site IPSec Auto IKE (example 2) 545
11.2.2.1. Pre-Planning 545
11.2.2.2. Configuration Steps. 545
11.2.3. Site to remote peer IPSec AutoIKE (example 3). 546
11.2.3.1. Pre-Planning 546
11.2.3.2. Configuration Steps. 546
11.2.4. SSL VPN Web Portal (example 4) 547
11.2.4.1. Pre-Planning 547
11.2.4.2. Configuration Steps. 547
11.2.5. SSL VPN Tunnel (example 5) 548
11.2.5.1. Pre-Planning 548
11.2.5.2. Configuration Steps. 548
11.3. Basic Examples. 549

Example 1. Site to Site Manual Tunnel 550
1.1. Configure I/F IP Addresses/Default Route/Default Policy. 551
1.2. Create Manual Tunnel (Authentication/Encryption) 553
1.3. Route Tunnel 555
1.4. Monitor Tunnel 557
Example 2. Site to Site Auto IKE Tunnel 558
2.1. Configure I/F IP Addresses, Default Route / Access Policy 559
2.2. Create Auto IKE tunnel 561
2.3. Route Tunnel. 565
2.4. Monitor Tunnel 566
Example 3. Site to Remote Peer IPSec Auto IKE 567
3.1. Configure I/F IP Addresses, Default Policy 568
3.2. Configure Remote PC client 569
3.3. Create IPSec VPN User 578
3.4. Create Auto IKE Tunnel 579
3.5. Dialin 580
3.6. Monitor Tunnel 581
Example 4. SSL VPN Portal. 582
4.1. Configure IP Addresses for Interfaces 583
4.2. Create an IP Address Pool, VPN User, Group. 584
4.3. Create SSL VPN Applications, Template 585
4.4. Import CA/Local Certificates. 587
4.5. Create SSL VPN Services 588
4.6. Access Applications with SSL VPN 589
Example 5. SSL VPN Tunnel 591
5.1. Configure IP Addresses for Interfaces 591
5.2. Remote PC: Install Client Software / Add Client Connection 591
5.3. Create IP Address Pool, VPN User, Group 591
5.4. Create an SSL VPN Tunnel 592
5.5. Connect to SSL VPN Server 592
5.6. Monitor 592
Example 6. SNAT Traversal (IPSec VPN) 593
6.1. Configure IP Addresses for Interfaces/Default Route 594
6.2. Establish Auto IKE Tunnel (static peer, pre-shared key) 596
6.3. Create Access Policy 599
6.4. Operation 600
VPN Gateway A / B: 601
Example 7. HA Synchronization（SSL VPN client) 602
7.1. Configure IP Addresses for Interfaces 603
7.2. Configure Virtual Router Detection Group. 605
7.3. Configure Virtual Routers 607
7.4. Configure Cluster 609
7.5. Create IP Address Pool. 611

7.6. Create SSL VPN User 612
7.7. Create SSL VPN User Group 613
7.8. Create SSL VPN Tunnel 614
7.9. Install SSL VPN Client 615
7.10. Create Client Connection 615
7.11. Connect to SSL VPN Server 616
Example 8. IPSec VPN Tunnel Group (for auto IKE tunnel only) 617
8.1. Configure Interface IP Addresses, Default Policy 617
8.2. Create Auto IKE Tunnels 618
8.3. Create Auto IKE Tunnel Group 619
8.4. Create Static Route 619
8.5. Monitor 620
11.4. Parameter Reference 621
11.4.1. IPSec VPN Parameters 621
11.4.1.1. Parameters of IPSec VPN User Groups 621
11.4.1.2. Parameters of Auto IKE tunnels 622
11.4.1.3. Parameters of Manual Tunnels 624
11.4.1.4. Parameters of IPSec VPN Tunnel Groups 625
11.4.1.5. General Settings 625
11.4.2. SSL VPN Parameters 626
11.4.2.1. SSL VPN User Group Parameters 626
11.4.2.2. SSL VPN Web Portal Application Parameters 626
11.4.2.3. SSL VPN Web Portal Template Parameters 627
11.4.2.4. SSL VPN Web Portal Services Parameters 628
11.4.2.5. Parameters of SSL VPN Tunnels 630
11.4.3. IP Address Pool Parameters 630

12 High Availability 631
12.1. Overview 631
12.1.1. Standard and enhanced VRRP 632
12.1.1. Standard 632
12.1.1. Enhanced 632
12.1.2. Standard VRRP Configuration 633
12.1.2.1 VR 633
12.1.2.2 VR election 633
12.1.2.3 VR IP tracking 633
12.1.3. Enhanced VRRP (VRDG/Cluster) Configuration 634
12.1.3.1 VR 634
12.1.3.2 VRDG 634
12.1.3.3 VRDG election 635
12.1.3.4 VRDG IP tracking 635
12.1.3.5 Cluster 635
12.1.4. Standard VRRP operation 637

12.1.4.1. States . . . 637
12.1.4.2. Election . . . 637
12.1.4.3. IP tracking . . . 637
12.1.5. Enhanced (VRDG/cluster) operation . . . 638
12.1.5.1. VRDG/cluster operation . . . 638
12.1.5.2. Cluster sync info . . . 638
12.2. Basic configuration steps . . . 640
12.2.1. Basic VRRP . . . 640
12.2.1.1. Device1: Configure VR . . . 640
12.2.1.2. Device2 . . . 641
12.2.2. Enhanced (VRDG/Cluster) . . . 642
12.2.2.1. Device1: Configure VR . . . 642
12.2.2.2. Device1: Configure VRDG . . . 642
12.2.2.3. Device1: Configure cluster . . . 644
12.2.2.4. Device2 . . . 644
12.3. Examples . . . 646
Example 1: Basic enhanced (VRDG/cluster) configuration . . . 646
1.1 Configure default policy, interfaces . . . 647
1.2 Configure VR . . . 648
1.3 Configure VRDG . . . 650
1.4 Configure cluster . . . 651
Example 2: Master/backup election . . . 654
2.1 Configure default policy, interfaces . . . 655
2.2 Configure VR . . . 656
2.3 View election results . . . 657
2.4 Failover . . . 659
2.5 Failure restore . . . 660
Example 3: Load sharing (master/master mode) . . . 661
3.1 Configure default policy, interfaces . . . 662
3.2 Configure VR . . . 663
3.3 Configure VRDG . . . 665
3.4 Configure cluster . . . 666
Example 4: IP tracking . . . 667
4.1 Configure default policy, interfaces . . . 668
4.2 Configure VR and IP tracking . . . 669
4.3 View tracking status . . . 670
4.4 Tracking failure on Device1 . . . 671
4.5 Failure restore . . . 672
Example 5: Cluster synchronization . . . 673
5.1 Configure cluster . . . 674
5.2 Check differences between local and remote . . . 675
5.3 Synchronize configuration manually . . . 677
5.4 Synchronize configuration automatically . . . 679

5.5 Synchronize system time 680
12.4. Parameter reference 681
12.4.1. Virtual Routers 681
12.4.2. Virtual Router Detection Groups 683
12.4.3. Clusters 684

13 Virtual Systems 685
13.1. Overview 685
13.1.1. Vsys 686
13.1.2. Vnet 687
13.2. Basic configuration steps 688
13.2.1. Create Layer 3 Interfaces 689
13.2.2. Create Vsys (resources, interfaces, management IP, UTM) 690
13.2.3. Create Vsys administrators 692
13.2.4. Logon to /switch Vsys 693
13.2.5. Manage Vsys 695
13.2.6. Create Vnet 696
13.3. Scenarios 697
1. Transparent Mode 697
2. Routing Mode 698
3. Hybrid Mode 699
13.4. Examples 700
Example 1: Multi-Vsys Based on Shared Layer 3 Interface 700
1. Create Layer 3 Interfaces 701
2. Create Vsys and assign interfaces 702
3. Assign Vsys 1-3 to admin 703
4. Configure Vsys 704
5. Create Virtual Network 706
6. Create Vsys Administrators 710
7. Set Vsys Management IP Addresses 711
Example 2: Multi-Vsys Based on Trunk Interface 713
1. Create Layer 3 Interfaces 714
2. Create Vsys 716
3. Assign Vsys to admin 717
4. Set Interface IP and Access Policy for Vsys 718
13.5. Parameter reference 720
13.5.1. Virtual Systems 720
13.5.2. Virtual Networks 721
13.5.3. Functions Configurable in Vsys 721

14 Monitoring 723
14.1 Topology 724
14.2 Traffic Statistics 724

14.2.1 Interface Traffic 725
14.2.2 Top Applications 725
14.2.3 Top URLs 725
14.2.4 Top Users 725
14.2.5 Top IP Addresses 725
14.3 Virtual Systems 726
14.4 Route 727
14.5 NAT 728
14.6 ARP 729
14.6.1 ARP Table 729
14.6.2 ARP Proxy Table 729
14.7 CAM 730
14.8 DHCP IP Address Binding Status 731
14.9 DHCPv6 Client 731
14.10 DNS Cache 732
14.11 High Availability 732
14.11.1 Virtual Routers 733
14.11.2 Virtual Router Detection Groups 734
14.11.3 Clusters 735
14.12 System Utilization 736
14.12.1 CPU and Memory Live Utilization 736
14.12.2 Disk Utilization 736
14.12.3 Processes 737
14.13 Online Users 738
14.13.1 WebAuth Users 738
14.13.2 SSL VPN Users 738
14.14 IPSec VPN Tunnels 739
14.14.1 Auto IKE Tunnels 739
14.14.2 Manual Tunnels 740
14.14.3 Accelerator Card Statistics 741
14.14.4 Soft Encryption Statistics 741
14.14.5 Tunnel Groups 742
14.15 Multicast 743
14.15.1 DVMRP Neighbors 743
14.15.2 IGMP Snooping State 743
14.16 Alerts/Logs 744
14.16.1 System Logs 744
14.16.2 Anti-Virus Alerts 745
14.16.3 Anti-Spam Alerts 745
14.16.4 URL Filtering Alerts 746
14.16.5 IPS Alerts 747

14.16.6 Application Control Alerts 748

15 Reporting 749
15.1 Overview 750
15.1.1 Recorded Content 750
15.1.2 Report Content / Format. 750
15.1.3 Scheduled Report Generation 750
15.1.4 View / Download / Email Reports 751
15.1.5 Retaining Old Reports 751
15.2 Basic Configuration Steps 752
15.2.1 Configure General Settings 752
15.2.2 Create a Report Schedule 753
15.2.3 Manage Report Results 756
15.3 Parameter Reference 757
15.3.1 SMTP Server Parameters 757
15.3.2 Schedule Parameters 758
15.3.3 Report Result Parameters 758
15.3.4 Global Content Parameters 759
15.3.4.1 System 760
15.3.4.2 Traffic 761
15.3.4.3 Web Security 764
15.3.4.4 Mail Security 766
15.3.4.5 Anti-Virus 767
15.3.4.6 Attack 770
15.3.4.7 Application 773
15.3.4.8 User Statistics 775
15.3.5 Per-User Content Parameters 776
15.3.5.1 Application 776
15.3.5.2 Web Security 777

A MIBs 779

About the User Guide

This Celestix FGX user guide consists of the following chapters:

- Chapter 1, “Quick Start” describes initial configuration through web-based Wizard, WebUI, and CLI as well as the verification of initial configurations.
- Chapter 2, “Functional overview” . An overview of the FGX functionality described in detail in chapters 3 to 15.
- Chapter 3, “System Configuration” describes system-related configurations.
- Chapter 4, “Network Configuration” introduces interfaces, zones, STP, DHCP, DNS and IPv6.
- Chapter 6, “Routing” describes routing and multicasting features.
- Chapter 5, “Network Address Translation” introduces SNAT, DNAT, and MIP.
- Chapter 7, “Quality of Service” describes QoS features, configurations, and examples.
- Chapter 8, “Policies” introduces access policies, session policies, multicast policies, IP-MAC binding policies, and default policies.
- Chapter 9, “Attack Defense” describes attack detection and defense.
- Chapter 10, “Unified Threat Management” describes export control and client/server protection.
- Chapter 11, “Virtual Private Network 2” describes IPSec VPN and SSL VPN (includes SSL VPN Web Portal and SSL VPN Tunnel).
- Chapter 12, “High Availability” describes standard VRRP and enhanced functionalities.
- Chapter 13, “Virtual Systems” describes virtual systems and virtual networks.
- Chapter 14, “Monitoring” describes information monitoring.
- Chapter 15, “Reporting” explains report generation.
- Appendix A, “MIBs” lists supported MIB objects.

Document Conventions

Table 1 Illustration Icons

 Router	 Server	 User
 Switch	 Database	 User
 FGX	 PC	 Laptop

Related Documentation

CELESTIX FGX Integrated Security Software v4.2 CLI Reference Guide

1 Quick Start

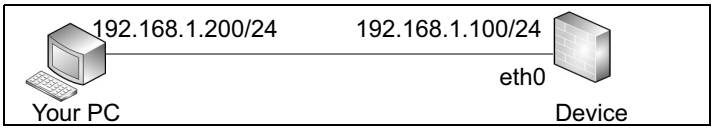
This chapter describes:

- 1.1 Hardware and system installation
- 1.2 Connect device to management PC
- 1.3 Connect device to network (determine topology)
- 1.4 Initialize configurations using Wizard
- 1.5 Initialize configurations using WebUI
- 1.6 Initialize configurations using CLI
- 1.7 Verify initialized configurations
- 1.8 Common problems
- 1.9 Next steps

1.1 Hardware and system installation

For details, see *CELESTIX FGX Getting Started Guide*.

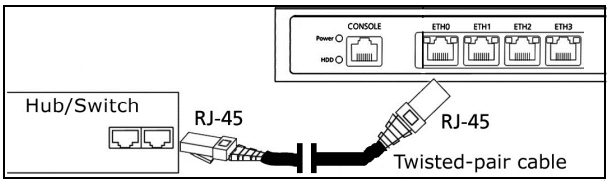
1.2 Connect device to management PC



- 1.2.1 Connect Ethernet interface
- 1.2.2 Connect console port

1.2.1 Connect Ethernet interface

1. Use an RJ45 network cable to connect your computer to eth0 of the FGX device or just connect FGX eth0 to LAN.
   Use a CAT 5, CAT 5E, or CAT 6 UTP cable or STP cable with RJ-45 connectors at both ends—one connected to the FGX ETH0, and the other to Ethernet interface of a HUB or switch within the LAN as shown in the following figure.



2. Set your computer's IP address to 192.168.1.200 and the subnet mask to 255.255.255.0.

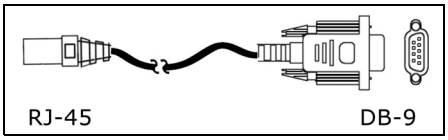
At least one of the following browsers should be installed on the terminal used to manage FGX:

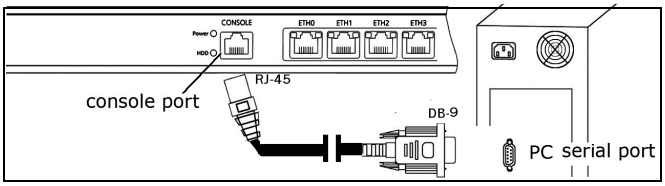
- Microsoft Internet Explorer (version 7.0 or higher)
- Mozilla Firefox (version 10.0 or higher)
- Google Chrome (version 9.0 or higher)
- Opera (version 11.x or higher)
- Safari (version 5.0 or higher)

1.2.2 Connect console port

The console access is allowed by default. You can manage FGX through the console port.

Connect the RJ-45 connector end of the console cable to the console port, and the DB-9 connector end to your computer's serial port.





Choose a VT100-compatible terminal or terminal emulator with an RS-232 port (standard DTE port), and configure as follows:

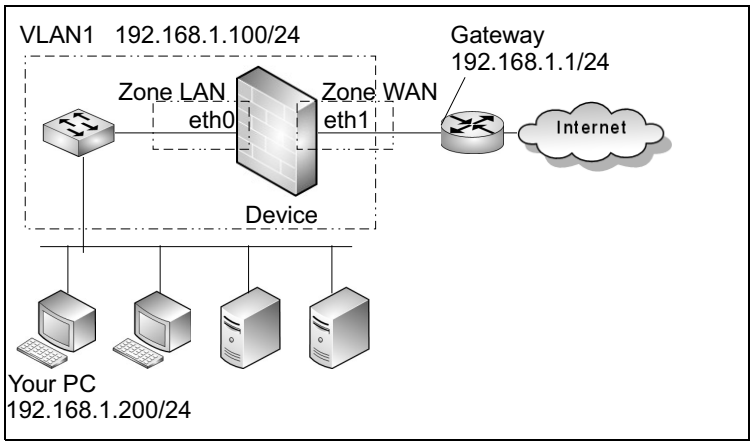
- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1

1.3 Connect device to network (determine topology)

- 1.3.1 Transparent mode
- 1.3.2 Routing mode

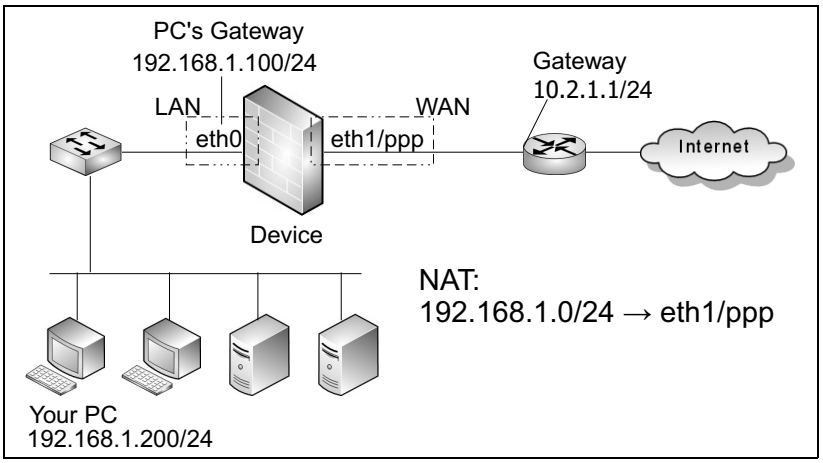
1.3.1 Transparent mode

FGX can be deployed on a private network behind an existing gateway. FGX works in transparent mode for Layer 2 data forwarding. When you want security protection without changing the network topology, you can use this working mode.



1.3.2 Routing mode

FGX can be deployed as a gateway between private and public networks. FGX works in routing mode for Layer 3 routing.



1.4 Initialize configurations using Wizard

FGX provides a WebUI wizard to finish initialization. With the wizard, you can finish:

- 1.4.1 Login
- 1.4.2 Set system language / host name / system time
- 1.4.3 Configure transparent mode (Layer 2)
- 1.4.4 Configure routing mode (Layer 3)

After that, you need to finish the following using the WebUI:

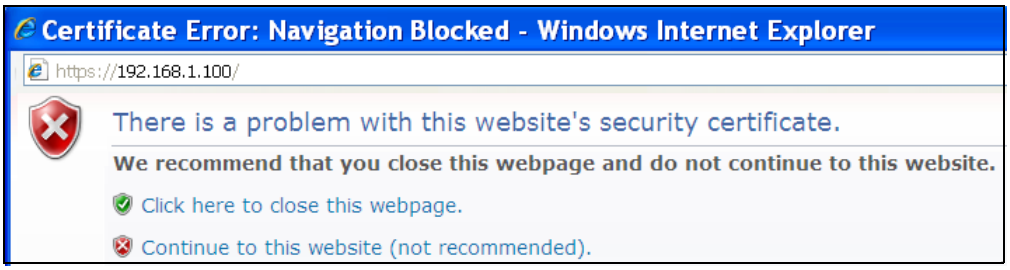
- 1.4.5 Reset password
- 1.4.6 Import license

1.4.1 Login

The wizard appears only:

- During first login.
- After system reset.

1. Turn on the FGX device.
2. Enter **https://192.168.1.100** in a browser. A certificate error page appears. Click "Continue to this website (not recommended)" to trust FGX certificate.

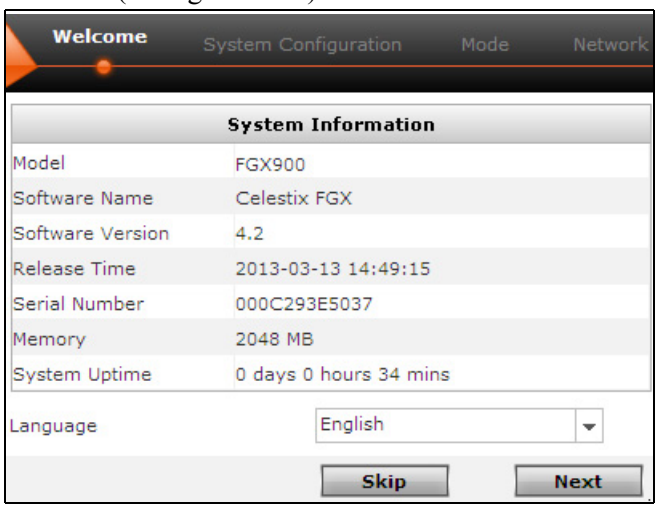


3. Login page appears (language can be changed in the next dialog). Enter **admin** and **[Celest1x]** in the text fields and click the login button.

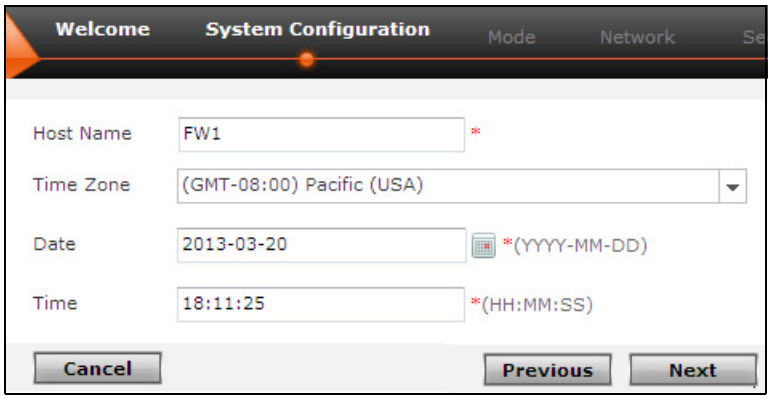
Note: After entering the wrong password 5 times in a row, the account is locked for 20 minutes.

1.4.2 Set system language / host name / system time

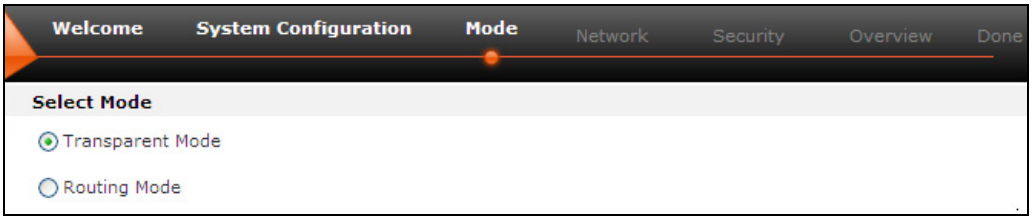
4. The **Welcome** page is shown. If required, select the language in the drop-down list and click **Next** (the right button).



5. Set the host name and system time and click **Next**.



6. The mode dialog appears. Select a deployment mode.

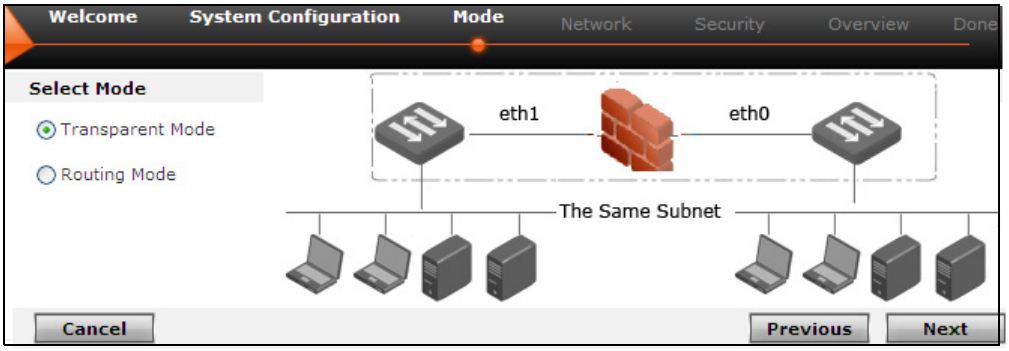


- 1.4.3 Configure transparent mode (Layer 2)
- 1.4.4 Configure routing mode (Layer 3)

1.4.3 Configure transparent mode (Layer 2)

- 1.4.3.1 Network settings
- 1.4.3.2 Security settings
- 1.4.3.3 Review and save settings (overview)
- 1.4.3.4 Verify initialized configurations using WebUI

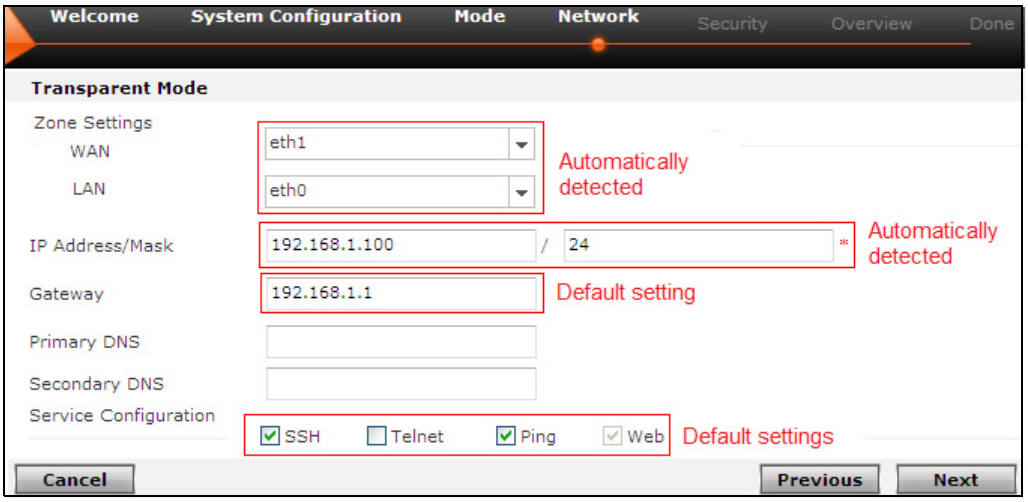
1. Choose **Transparent Mode** and click **Next**.



1.4.3.1 Network settings

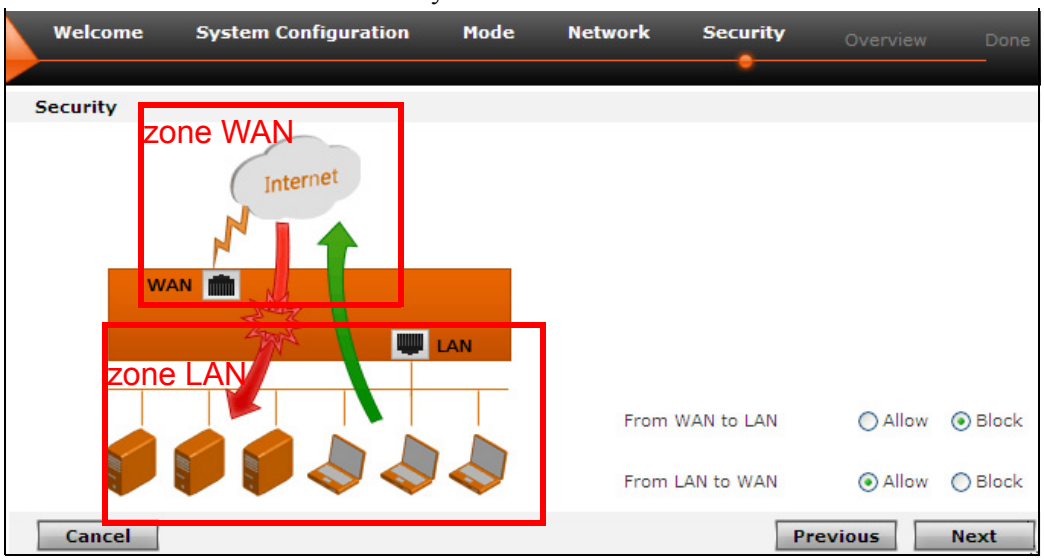
2. Configure the network settings:

- Zone Settings. Default zones include:
  - LAN—Layer 2 mode, includes the first detected Layer 2 Ethernet interface (the Ethernet interface with the smallest ID on the device) by default.
  - WAN—Layer 2 mode, includes second detected Layer 2 Ethernet interface by default.
- IP Address/Mask. IP address / subnet mask of the default VLAN interface vlan1. By default,
  - vlan1's IP is 192.168.1.100/24.
  - vlan1 includes all Ethernet interfaces.
  - IPv6 is enabled on vlan1
- Gateway address of FGX. It is 192.168.1.1 by default.
- DNS server addresses. Used to resolve domain names for FGX to access the Internet.
- Service configuration. Enable or disable services used to manage FGX. You can only set services for LAN in initialization wizard.



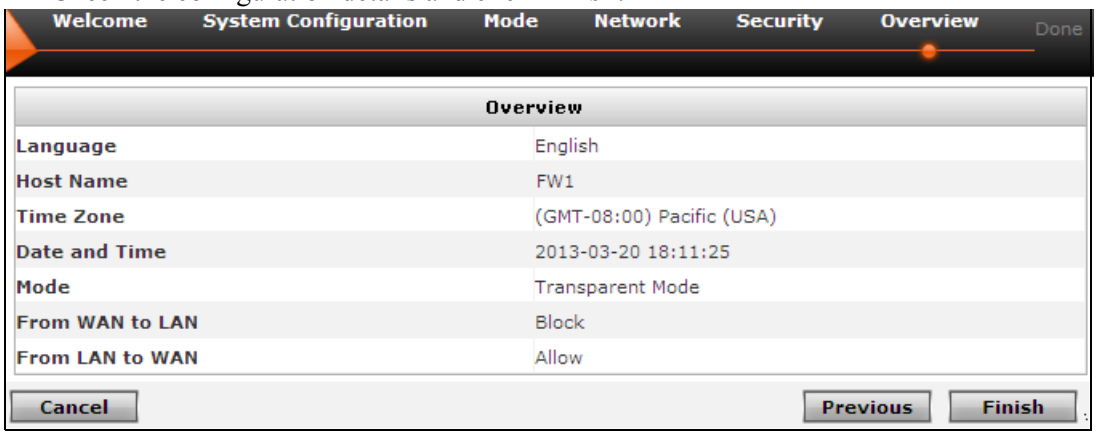
1.4.3.2 Security settings

3. Set the actions for access security control and click **Next**.

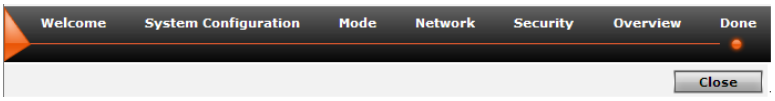


1.4.3.3 Review and save settings (overview)

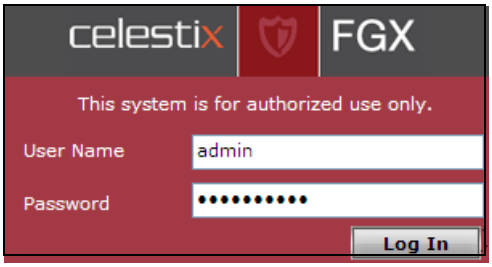
4. Check the configuration details and click **Finish**.



5. Click **Close** to exit the wizard.



6. Login page appears with the new management IP address in the address bar.

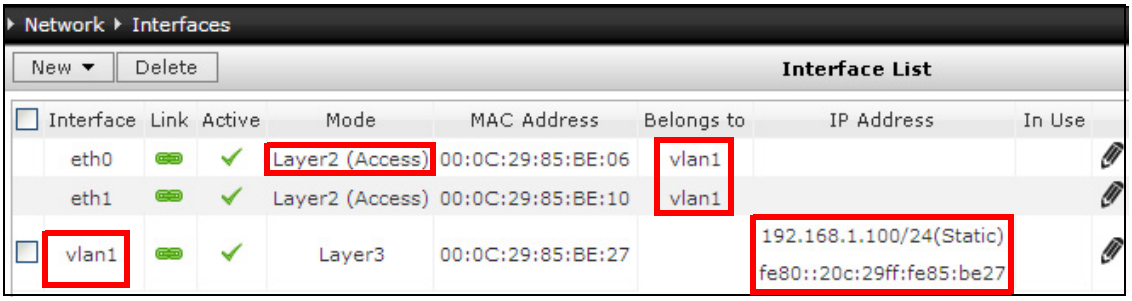


1.4.3.4 Verify initialized configurations using WebUI

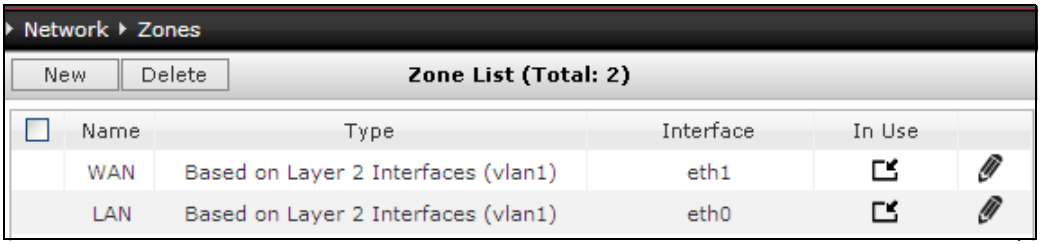
To verify whether the initialized configurations take effect:

1. Enter the default user name and password to login.
2. View the new host name and system time on the top of the home page.

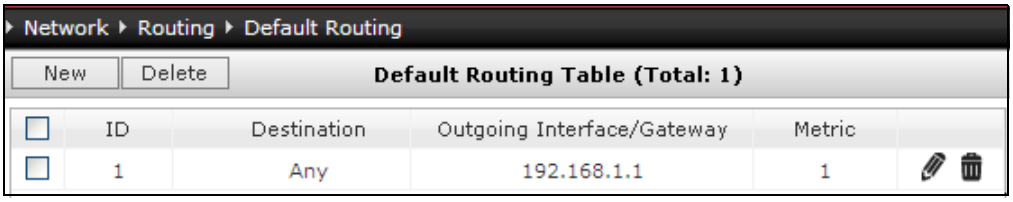
3. Choose **Network > Interfaces** and view the created vlan1 which holds eth0 and eth1. eth0 already changes to a Layer 2 Ethernet interface.



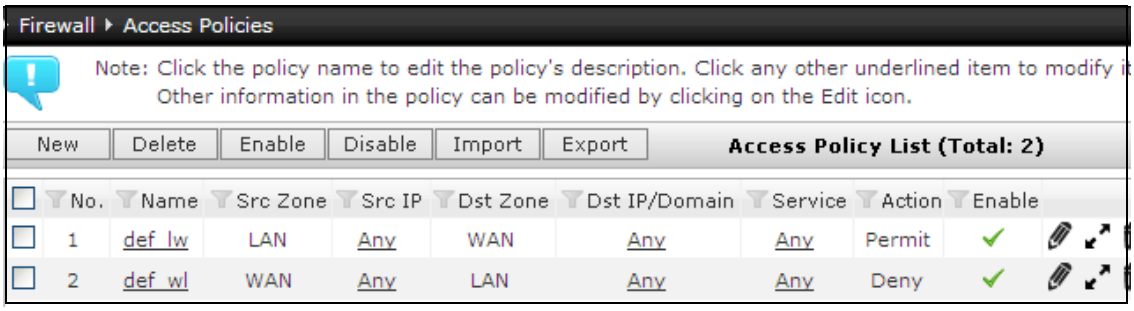
4. Choose **Network > Zones** and view the created Layer 2 zones LAN and WAN. LAN includes eth0 and WAN includes eth1. Two zones are used by default access policies.



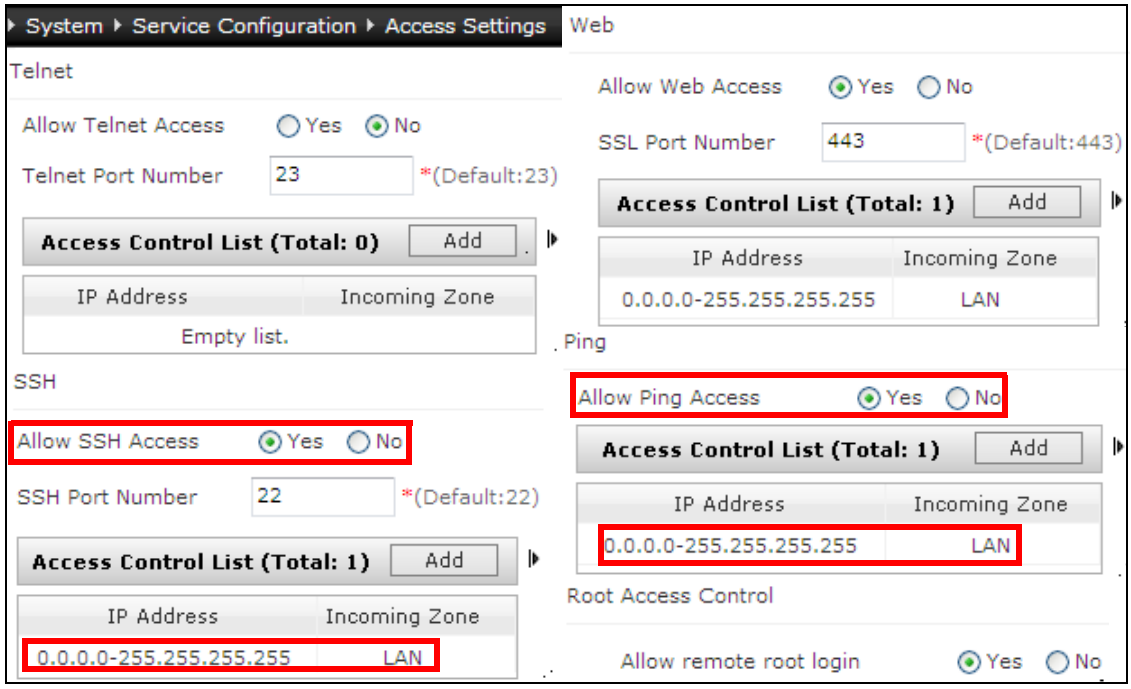
5. Choose **Network > Routing > Default Routing** and check whether the default gateway is already changed. The following is the default setting.



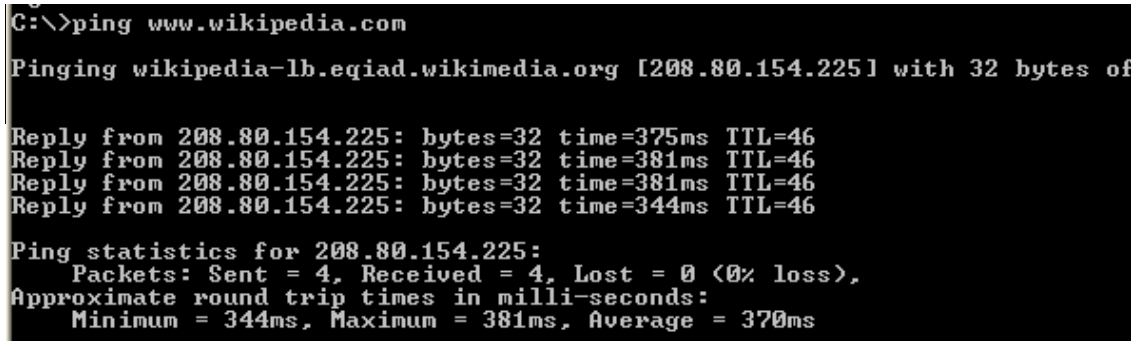
6. Choose **Firewall > Access Policies** and check whether two default access policies are added to allow access from LAN to WAN and deny access from WAN to LAN.



7. Choose **System > Service Configuration > Access Settings** to view whether services are enabled or disabled.



8. Verify the initialized configurations by testing the network connectivity.
   - On your management PC ping a website on the Internet, and the ping should be successful because access from LAN to WAN is allowed.



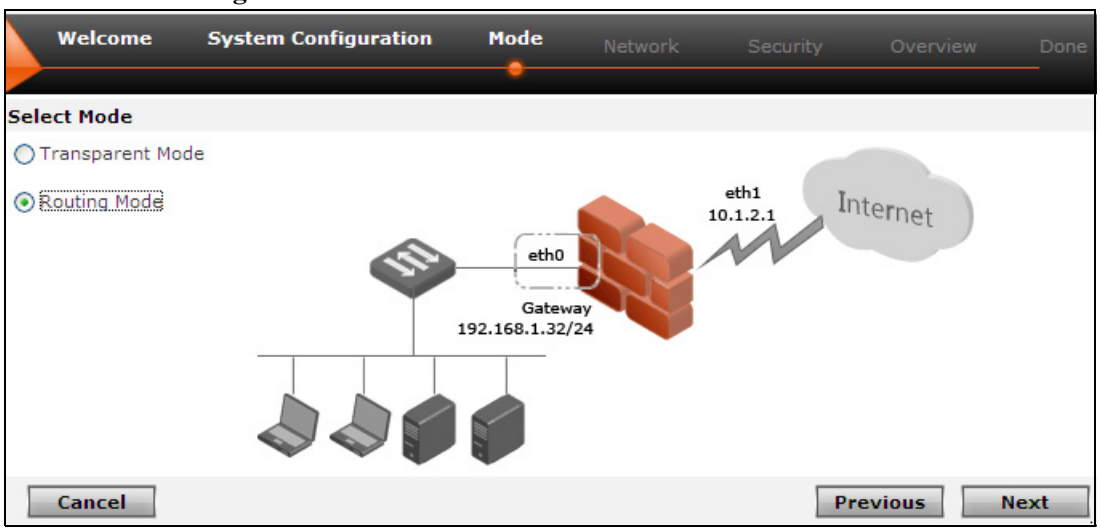
- On a client in WAN ping your management PC, and the ping should fail because access from WAN to LAN is denied.

```
C:\>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

1.4.4 Configure routing mode (Layer 3)

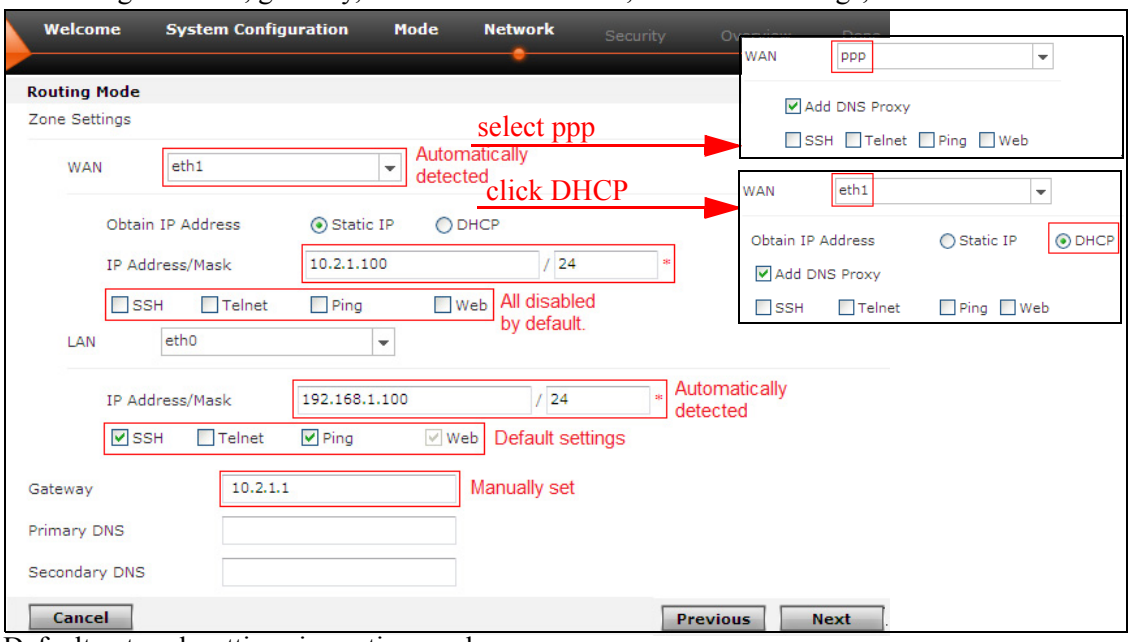
- 1.4.4.1 Network settings
  - 1.4.4.1.1 Network Ethernet settings
  - 1.4.4.1.2 Network PPPoE settings
- 1.4.4.2 Network NAT settings
- 1.4.4.3 Security settings
- 1.4.4.4 Review and save settings (overview)
- 1.4.4.5 Verify initialized configurations using WebUI

1. Choose **Routing Mode** and click **Next**.



1.4.4.1 Network settings

2. Configure zones, gateway, DNS server addresses, and access settings, and click **Next**.



Default network settings in routing mode:

LAN	Default zone at Layer 3 mode. Includes the first detected Layer 3 Ethernet interface (the Ethernet interface with the smallest ID on the device), and the Ethernet interface uses a static IP address.
WAN	Default zone at Layer 3 mode. Includes the second detected Layer 3 Ethernet interface, and the Ethernet interface uses a static IP address.

3. Choose to access the Internet using an Ethernet or PPPoE interface:
   - 1.4.4.1.1 Network Ethernet settings
   - 1.4.4.1.2 Network PPPoE settings (only for small networks using PPPoE)

1.4.4.1.1 Network Ethernet settings

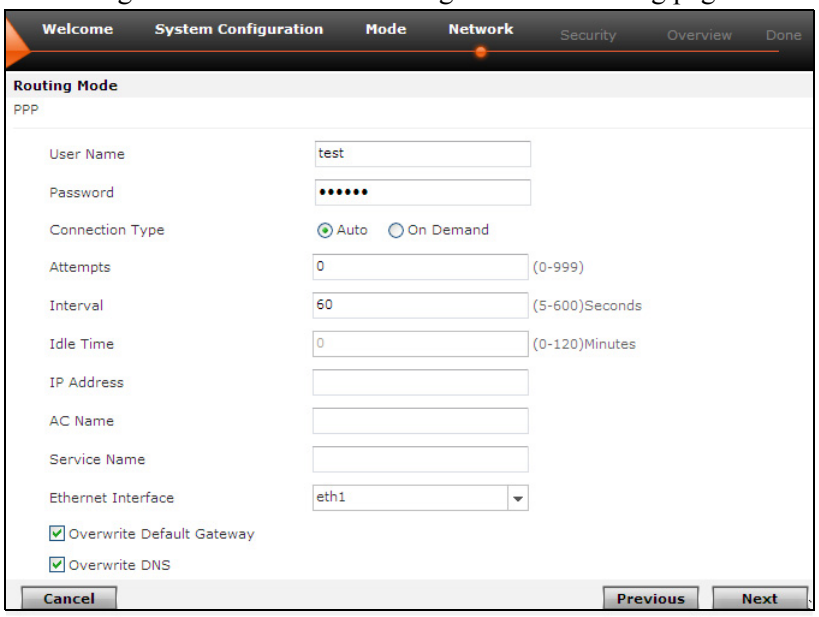
To access the Internet through an Ethernet interface:

1. Select **eth1** from the **WAN** drop-down box.
   a. Click **Static IP** or **DHCP** to obtain an IP address for eth1.
      If you choose **Static IP**, you need to enter an IP address and the mask length for eth1.
   b. Enable or disable **SSH**, **Telnet**, **Ping**, and **Web** access to WAN.
2. Select **eth0** from the **LAN** drop-down box.
   a. Set the IP address and the mask length for eth0.
   b. Enable or disable **SSH**, **Telnet**, and **Ping** access to LAN. **Web** access is enabled by default.
   c. Set the gateway address and DNS server addresses for FGX.
3. Click **Next** and go to NAT configuration page.

1.4.4.1.2 Network PPPoE settings

To access the ISP network through a PPPoE interface:

1. Select **ppp** from the **WAN** drop-down box.
2. Enable or disable DNS proxy and configure services as described above. Click **Next**.
3. Configure PPPoE interface settings on the following page.



d. Configure the user name and password for PPPoE connection.

- **User Name**—the name of a PPPoE dial-up user, 0-127 characters. Can be digits, letters, and the following special characters: `~!@#$%^&*()_+-=[]{}\|;:”<>,./?. It must begin with a digit or letter.
- **Password**—0-127 UTF-8 characters except spaces.

Setting no user name and password means PPPoE connection requires no authentication.

e. Select a connection type:

- **Auto** (default)—automatically connects to the ISP. When the connection is disconnected, FGX requires an auto re-connection.
- **On demand**—connects to the ISP only upon access request.

f. Set the retry attempts, retry interval, and idle period for PPPoE connection.

- **Attempts**—0-999. Default value is 0. 0 indicates no limit.
- **Interval**—5-600 seconds. Default value is 60.
- **Idle Time**—the length of idle time (no data transmission) that will cause a disconnect. 0-120 minutes. 0 indicates permanent connection (default). Can be configured only when the connection type is **On Demand**.

g. Set an IP address for the PPPoE interface on FGX.

Only for IPv4 mode. The format is [1-223].[0-225].[0-225].[0-225]. You cannot enter 127.0.0.0-127.255.255.255 or 192.168.255.254. If no IP address is set, FGX will use an IP address obtained from the ISP to dial up.

h. Set the AC name and the service name.

- **AC Name**—the brand, model, or serial number of the ADSL modem.
- **Service Name**—the name of the ISP or that of the service provided by the ISP.

AC name and service name are provided by the ISP. 0-127 UTF-8 characters except spaces and question marks. Usually not configured.

i. Select **eth1** from the **Ethernet Interface** drop-down box.

It must be a Layer 2 Ethernet interface or redundant interface. By default, the PPPoE interface is bound to the Ethernet interface with the smallest ID on the device, except for the one already assigned to LAN.

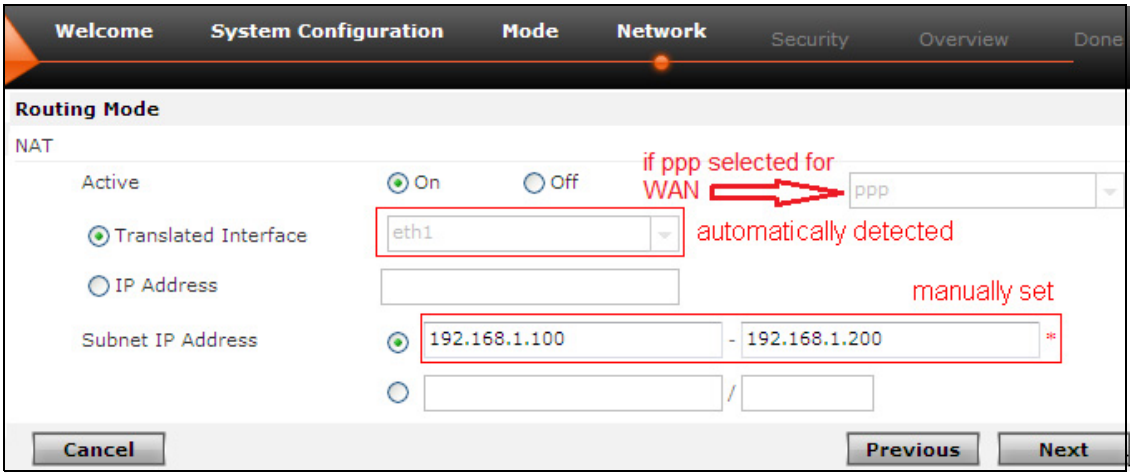
j. Check the last two check boxes to use the default gateway and DNS server addresses obtained from the ISP.

- **Overwrite Default Gateway**—send packets that should be sent to the default gateway to the PPPoE interface after PPPoE dial-up. Disabled by default.
- **Overwrite DNS**—overwrite the DNS server information configured on FGX (DNS Host) with that obtained from the ISP. Only for IPv4 mode. Disabled by default.

Note: For more information about PPPoE interfaces, see 4.8 PPPoE Interface.

1.4.4.2 Network NAT settings

4. Configure NAT, and click **Next**.



a. Enable NAT for internal network security. NAT here only translates the source IP addresses of requests to the Internet into a public IP address.

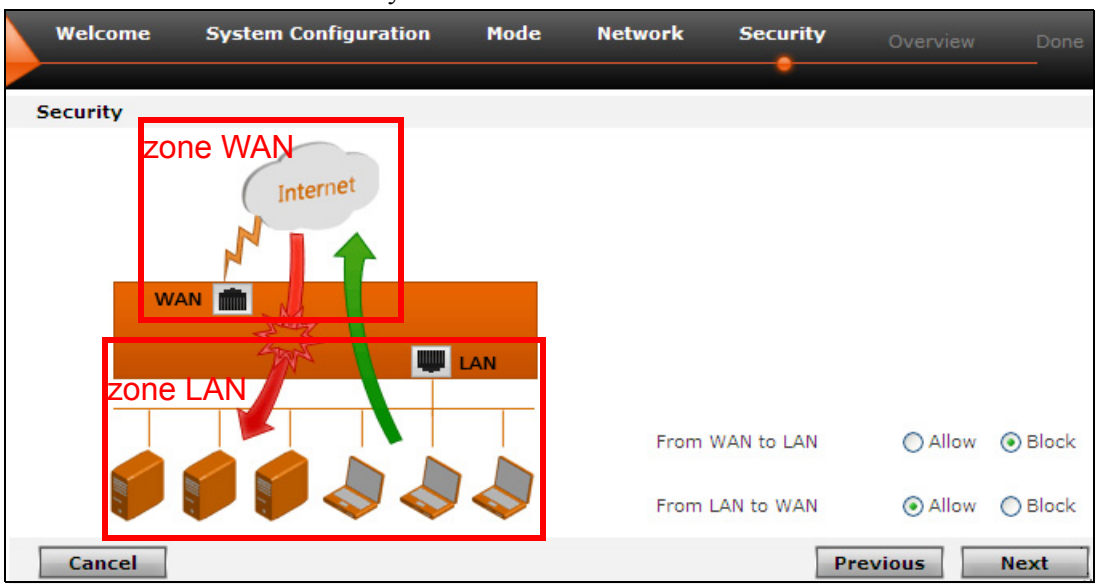
b. Select a translation type:

- Click **Translated Interface** and the interface (eth or ppp) you have assigned to WAN will be automatically selected. FGXwill translate the source IP addresses into the IP address of the selected interface.
- Click **IP Address** and specify an IP address. FGX will translate the source IP addresses into the specified IP address.

c. Configure internal subnet IP addresses to be translated. You can choose to set an IP address range or a subnet address for translation.

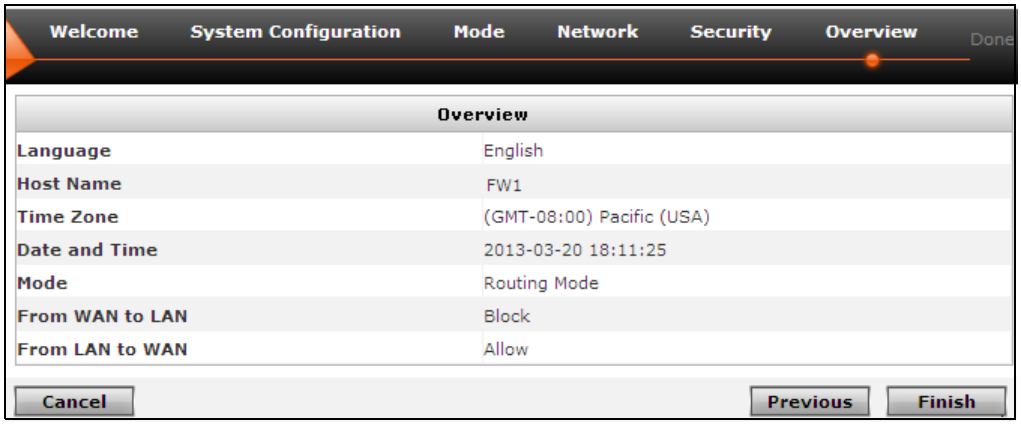
1.4.4.3 Security settings

5. Set actions for access security control and click **Next**.

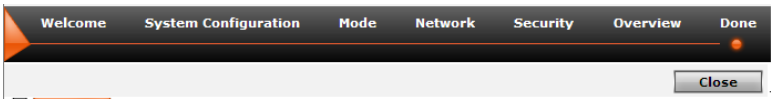


1.4.4.4 Review and save settings (overview)

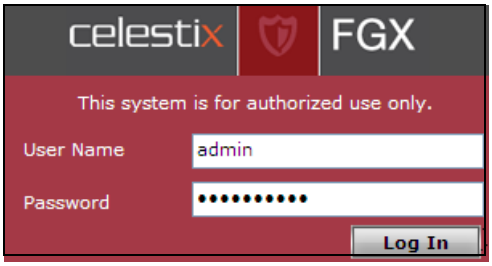
6. Check the configuration details and click **Finish**.



7. Click **Close** to exit the wizard.



8. Login page appears with the new management IP address in the address bar.

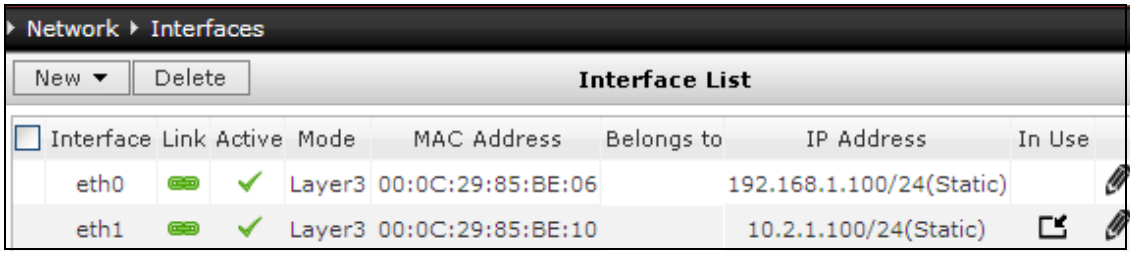


1.4.4.5 Verify initialized configurations using WebUI

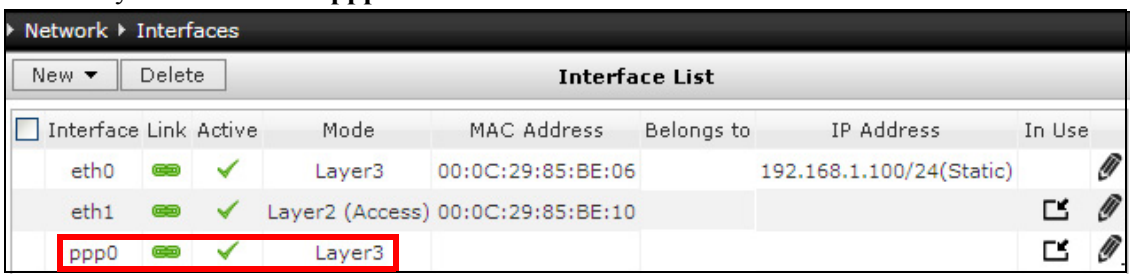
To verify whether the initialized configurations take effect:

1. Enter the default user name and password to login.
2. View the new hostname and system time on the top of the home page.

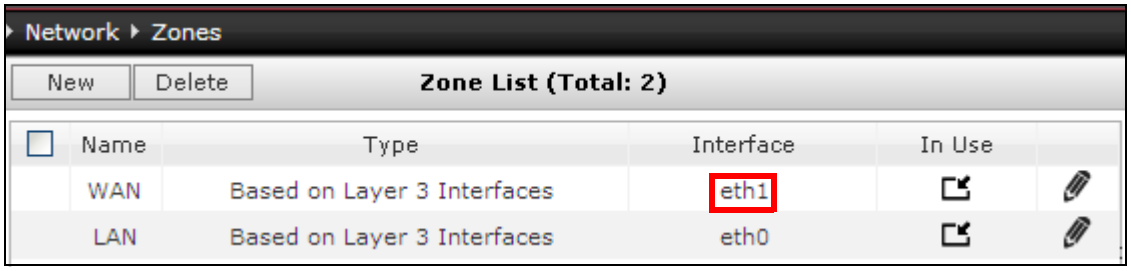
3. Choose **Network > Interfaces** and view the interface settings.
   - If you have selected **eth1** for WAN:



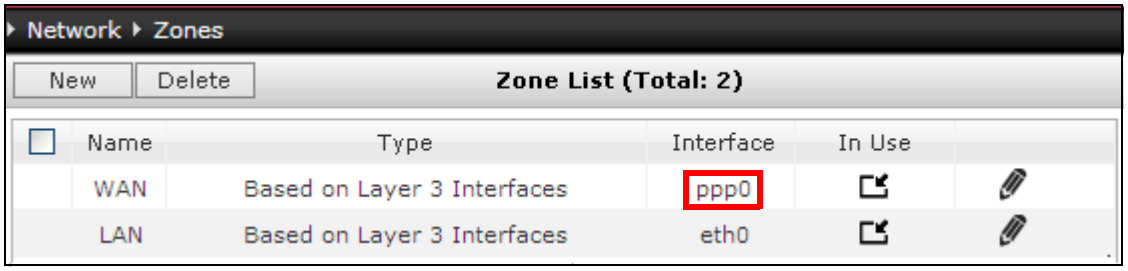
   - If you have selected **ppp** for WAN:



4. Choose **Network > Zones** and view the created Layer 3 zones LAN and WAN.
   - If you have selected **eth1** for WAN:

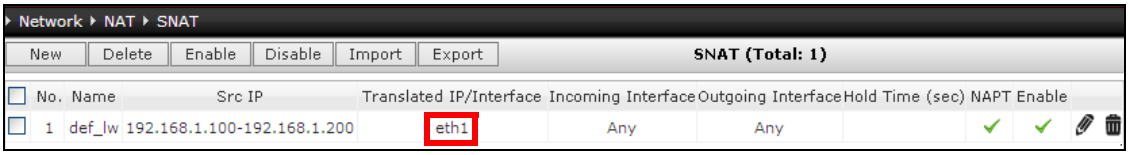


   - If you have selected **ppp** for WAN:

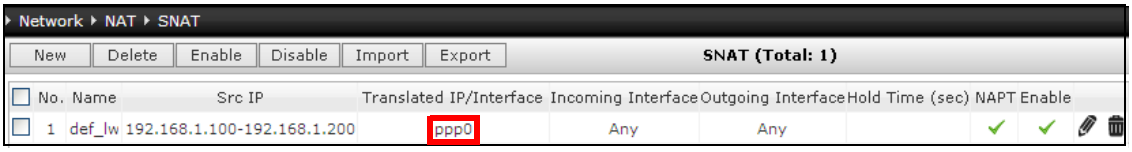


5. Choose **Network > NAT > SNAT** and check whether the SNAT rule is already created according to your initial configuration.

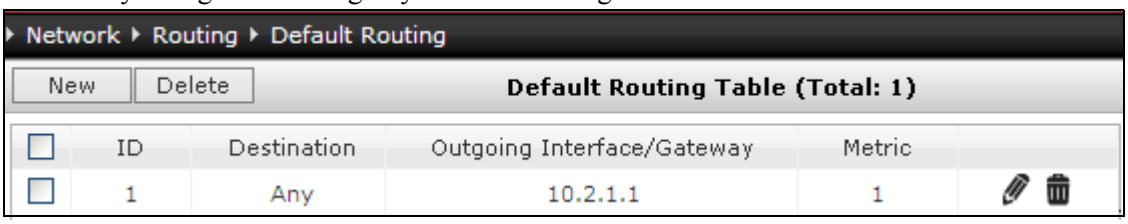
   - If you have selected **eth1** for WAN:



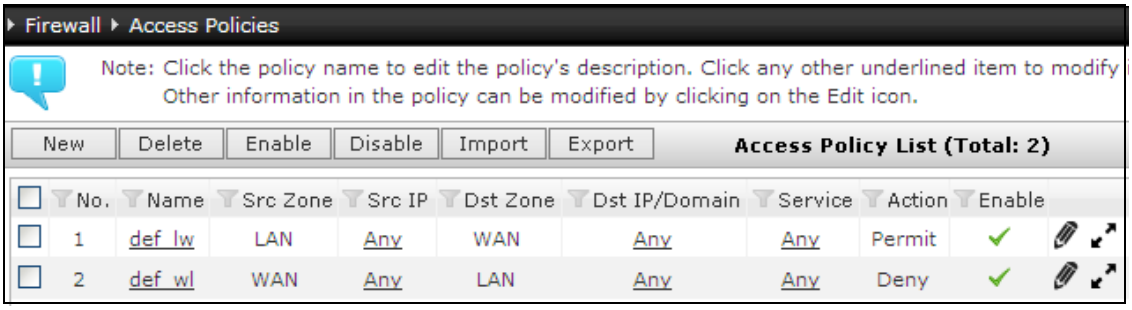
   - If you have selected **ppp** for WAN:



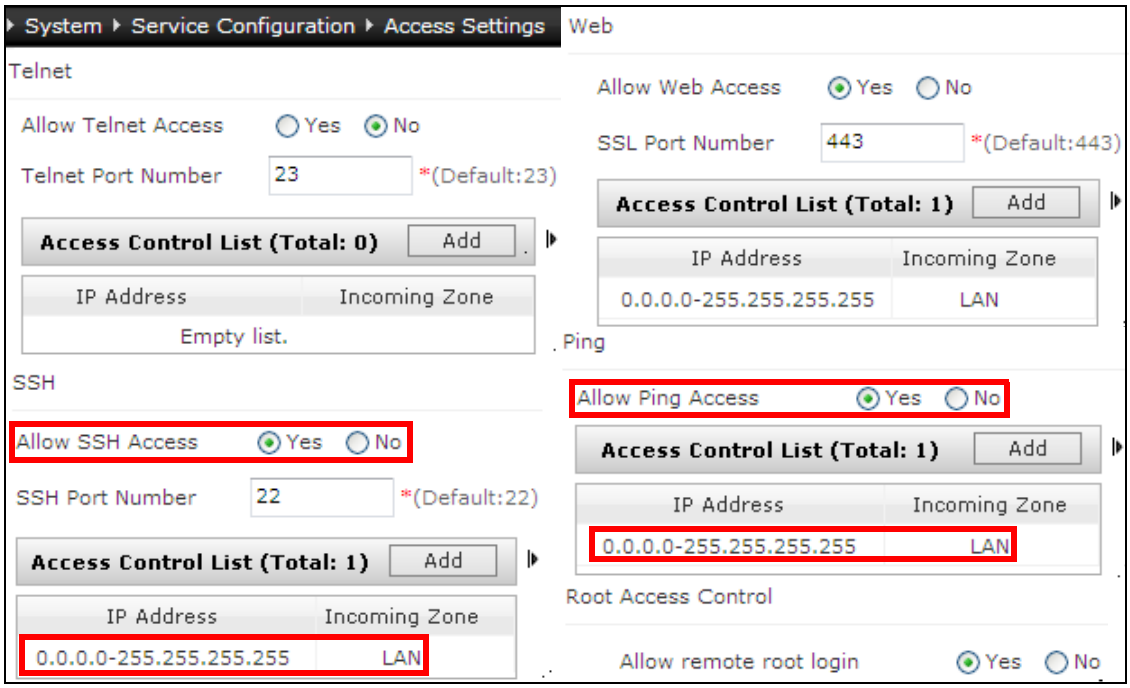
6. Choose **Network > Routing > Default Routing** and check whether the default gateway is already changed according to your initial configuration.



7. Choose **Firewall > Access Policies** and check whether two default access policies are added to allow access from LAN to WAN and deny access from WAN to LAN.



8. Choose **System > Service Configuration > Access Settings** to view whether services are enabled or disabled.



9. Verify the initialized configurations as for transparent mode.

1.4.5 Reset password

The same as steps using WebUI. See 1.5.3 Reset password.

1.4.6 Import license

The same as steps using WebUI. See 1.5.7 Import license.

1.5 Initialize configurations using WebUI

- 1.5.1 Login
- 1.5.2 WebUI overview
- 1.5.4 Set system language / host name /system time
- 1.5.3 Reset password

Choose to configure one of the following two working modes:

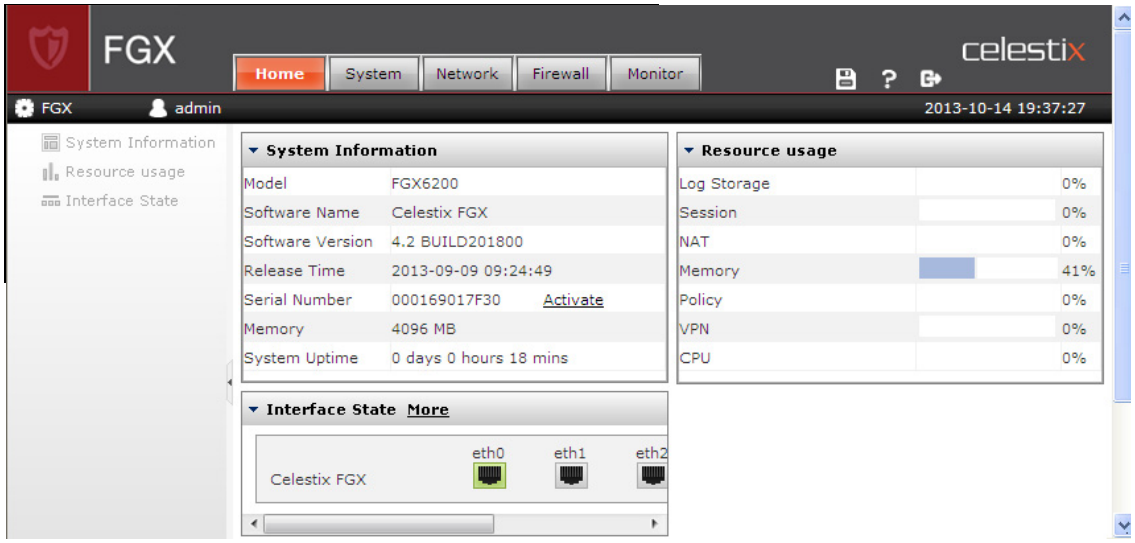
- 1.5.5 Configure transparent mode
- 1.5.6 Configure routing mode

To configure functions, import a valid license:

- 1.5.7 Import license

1.5.1 Login

1. Login using the wizard as described in 1.4 Initialize configurations using Wizard.
2. In the **Welcome** dialog click **Skip**. The following WebUI dialog appears.



1.5.2 WebUI overview

The following table lists WebUI operation buttons.

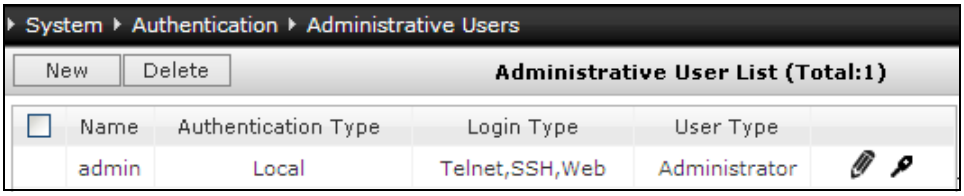
Table 1 WebUI Operation Buttons

Button	Description	Button	Description
	Configuration lock (Only one admin can have the configuration lock at a time.)		Switch to virtual systems
	Save		Edit the date and time of the system.
	Online help		In Use (view policies or profiles using an entry)
	Logoff		Move a policy to change its priority.
	Refresh		Clone
	Close (or delete)		Enabled (entry)
	Edit		Disabled (entry)
	Delete		Filter enabled (filters set parameters to display)
	Restore (the system settings)		Filter disabled
	View		Add an entry to a list box.
	Download		Delete an entry from a list box.
	Export		Move up an entry in a list.
	Change password		Move down an entry in a list.

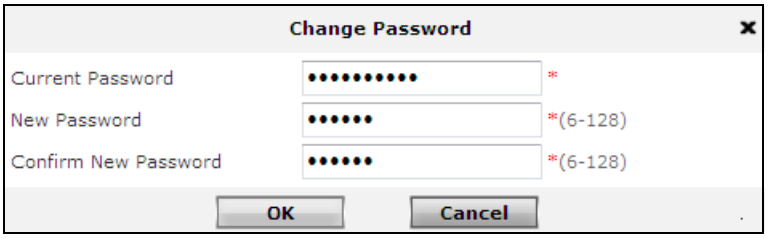
1.5.3 Reset password

To change the default login password:

1. Choose **System > Authentication**.



2. Click to change the password.

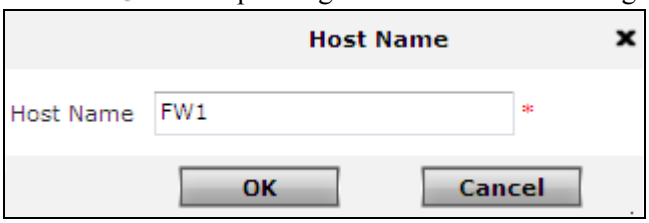


3. Click **OK**. The new password will take effect at next login.

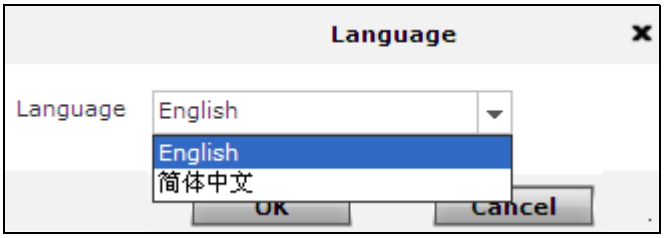
1.5.4 Set system language / host name /system time

1. Choose **System > Overview**.

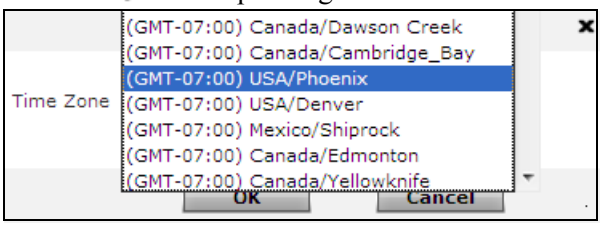
2. Click corresponding to **Host Name** and change the host name.

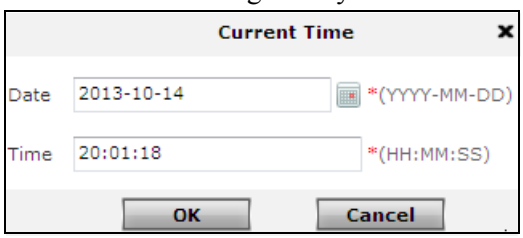


3. Click **OK**.
4. Click corresponding to **Language** and select a system language.



5. Click **OK**.
6. Click corresponding to **Time Zone** and **Current Time** and change the system time.

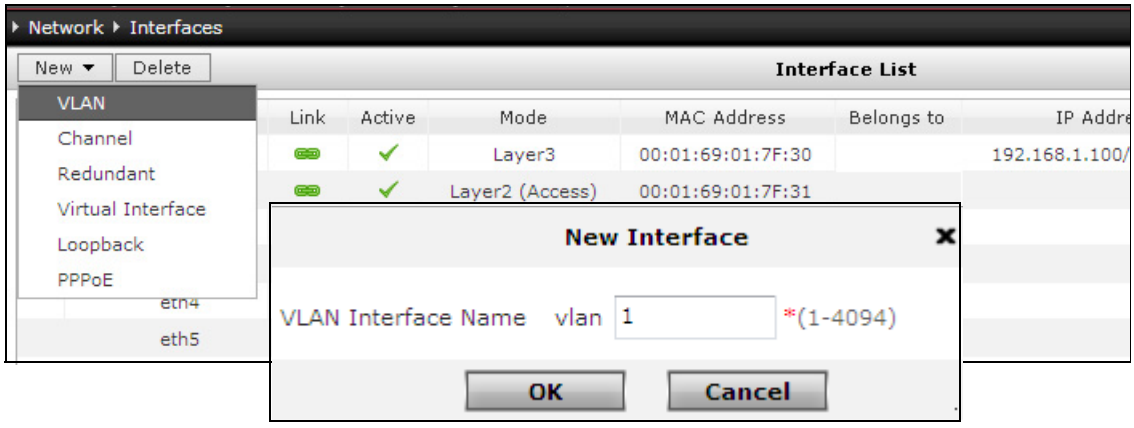




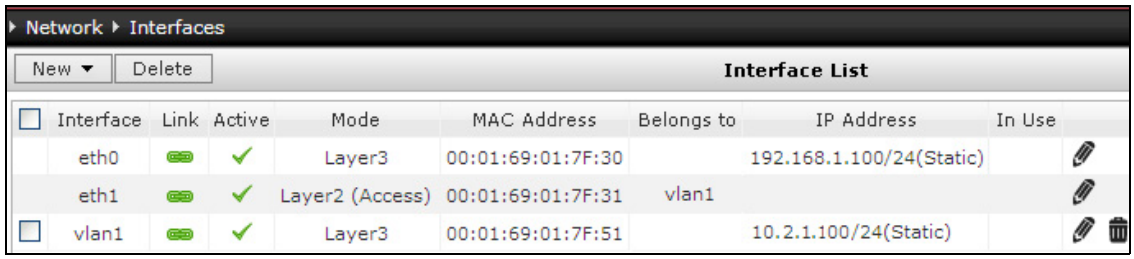
7. Click **OK**. Click .

1.5.5 Configure transparent mode

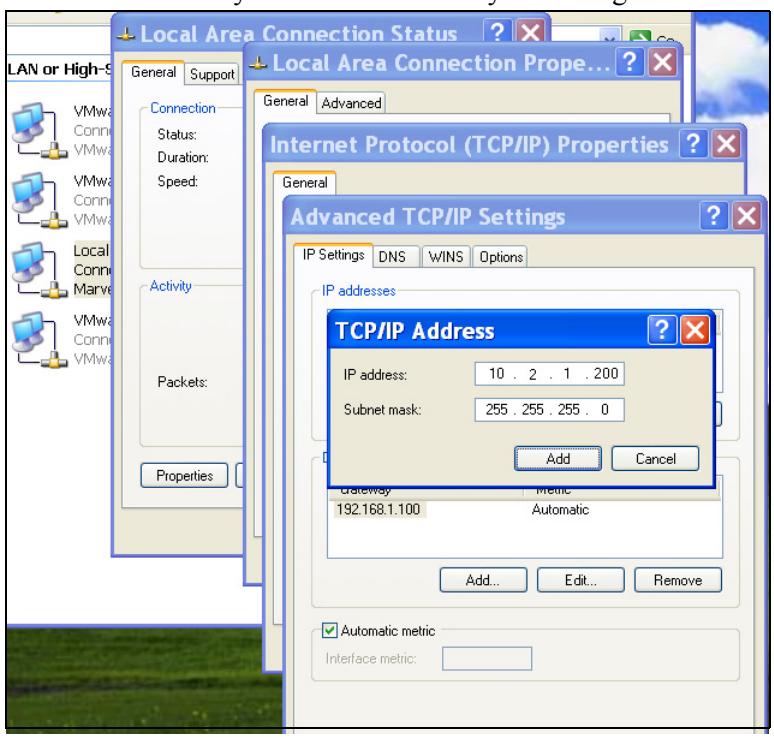
1. Choose **Network > Interfaces**. Click **New > VLAN** and create a new VLAN interface vlan1.



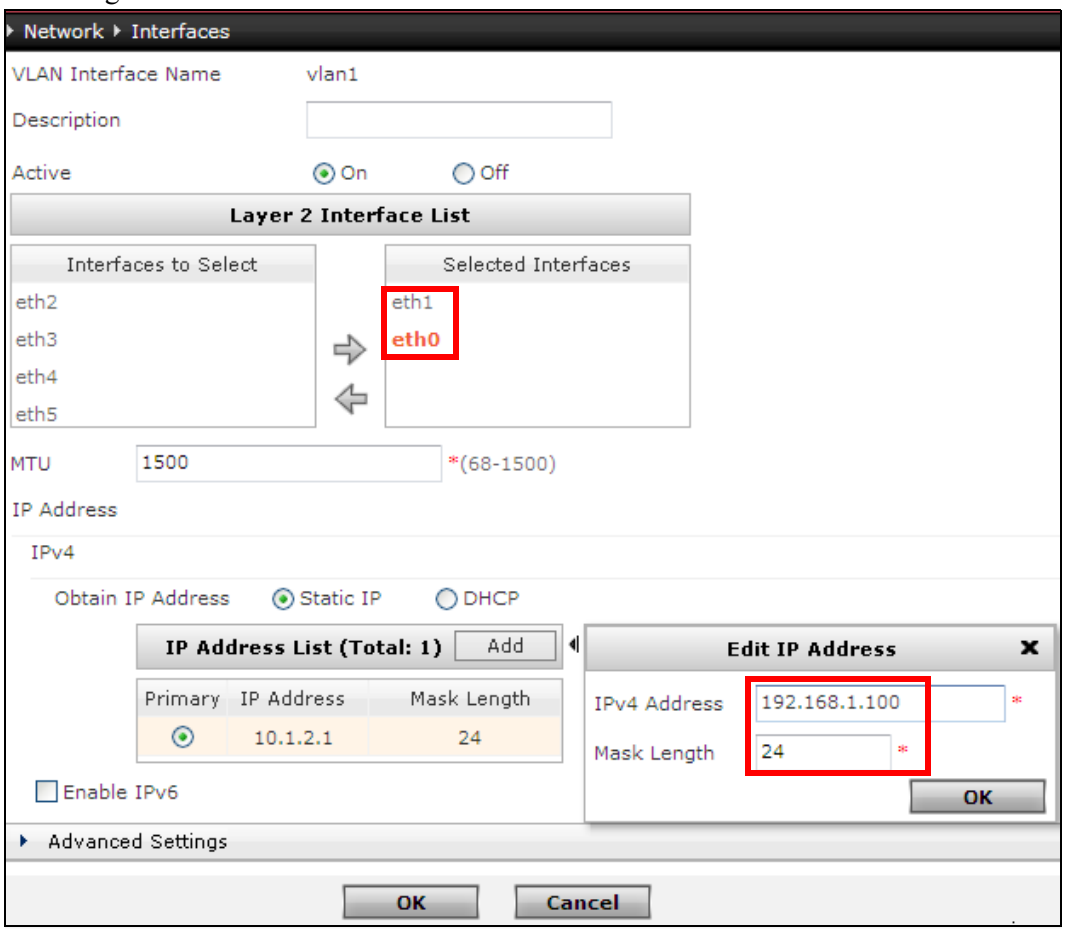
2. Add eth1 to vlan1 and set vlan1's IP address to 10.2.1.100/24.



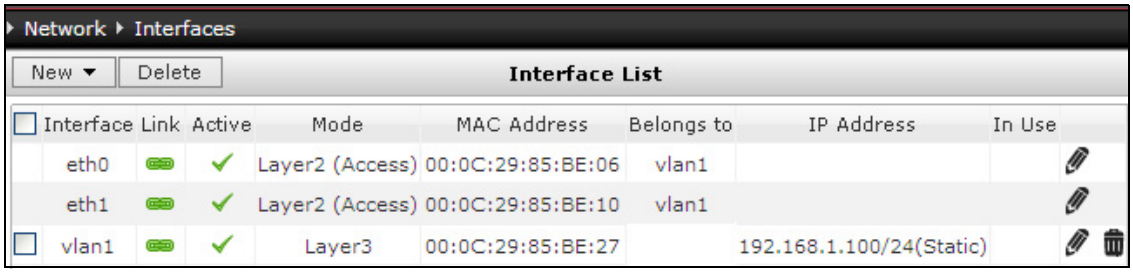
3. Add a secondary IP 10.2.1.200/24 to your management PC.



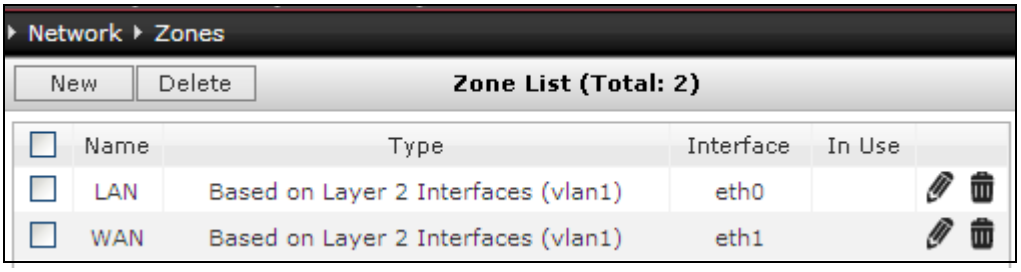
4. Unplug the network cable from eth0 and plug it into eth1, and enter https://10.2.1.100 in the browser to login through vlan1 (eth1).
5. Choose **Network > Interfaces**, set eth0 to Layer 2 working mode. Add eth0 to vlan1 and change vlan1's IP address to 192.168.1.100/24. Click **OK**.



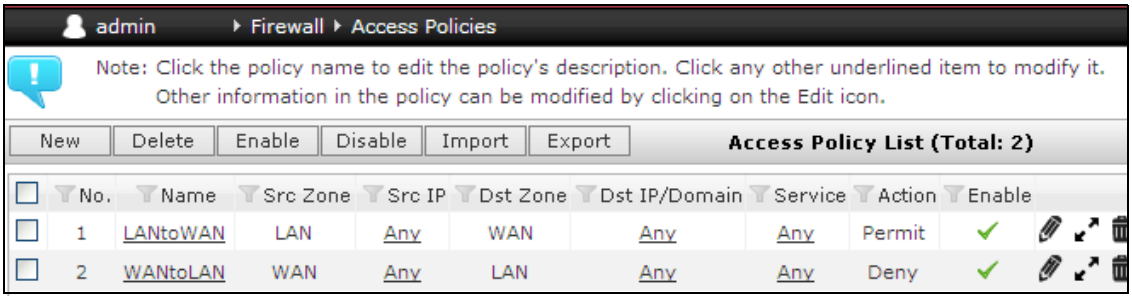
6. Unplug the network cable from eth1 and plug into eth0, and enter https://192.168.1.100 in the browser to login through vlan1 (eth0).
7. Choose **Network > Interfaces** and view interface settings.



8. Choose **Network > Zones** and create Layer2 zones LAN and WAN. Add eth0 to LAN and eth1 to WAN.



9. Choose **Firewall > Access Policies** and create access policies as follows:



10. Click  .

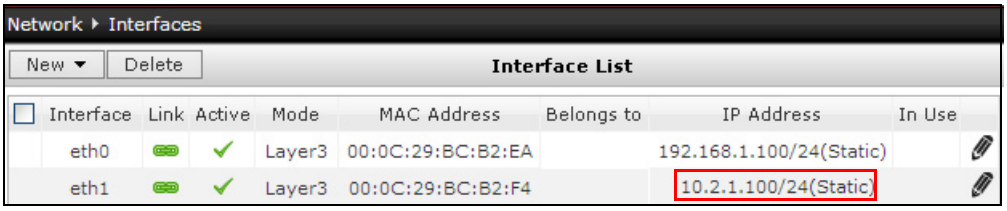
11. Verify the initialized configurations as 1.4.3.4 Verify initialized configurations using WebUI.

1.5.6 Configure routing mode

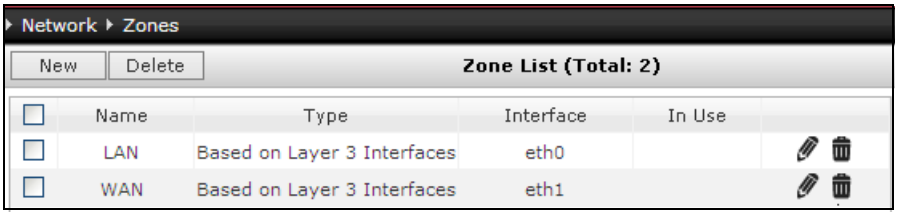
- 1.5.6.1 Ethernet connection
- 1.5.6.2 PPPoE connection

1.5.6.1 Ethernet connection

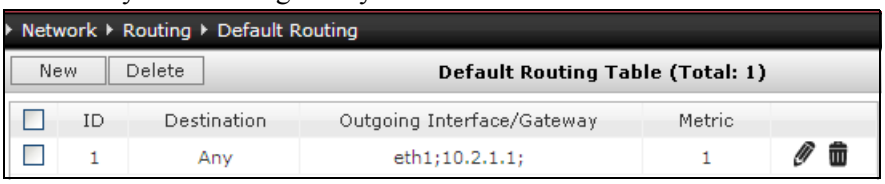
1. Choose **Network > Interfaces**. Set eth1 to Layer 3 working mode and set its IP address to 10.2.1.100/24.



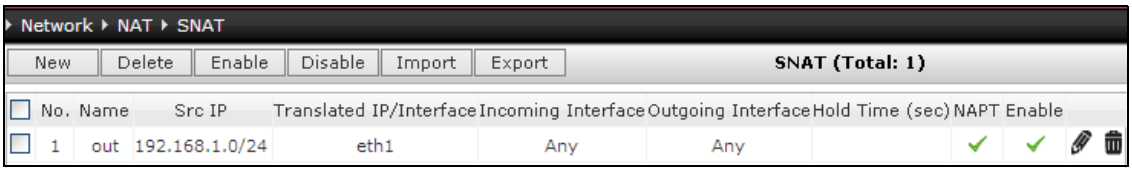
2. Create Layer 3 zone LAN and WAN. Add eth0 to LAN and eth1 to WAN.



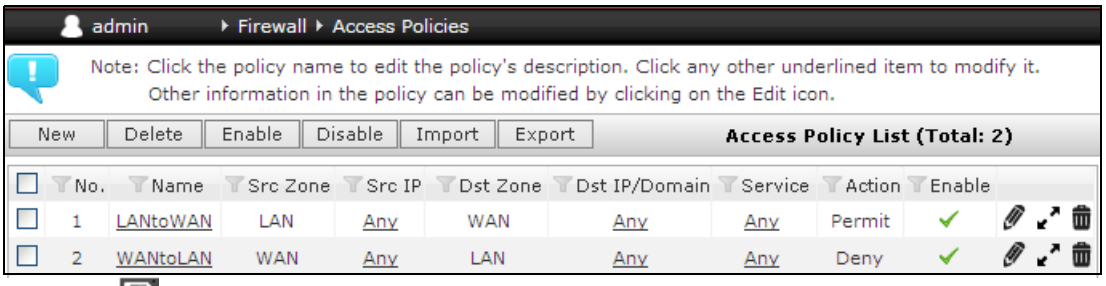
3. Modify the default gateway to 10.2.1.1:



4. Create a SNAT rule to translate 192.168.1.0/24 to the IP address of eth1:



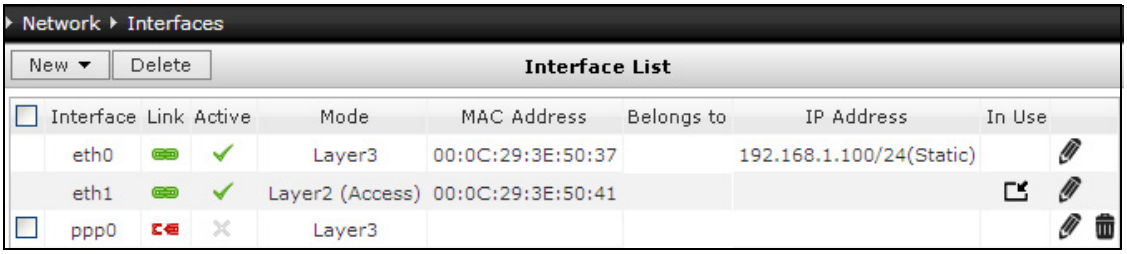
5. Create access policies to allow access from LAN to WAN and deny access from WAN to LAN.



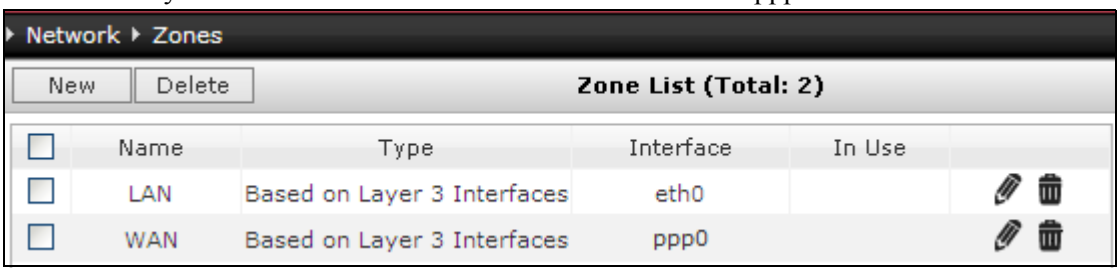
6. Click  .
7. Verify the initialized configurations as 1.4.4.5 Verify initialized configurations using WebUI.

1.5.6.2 PPPoE connection

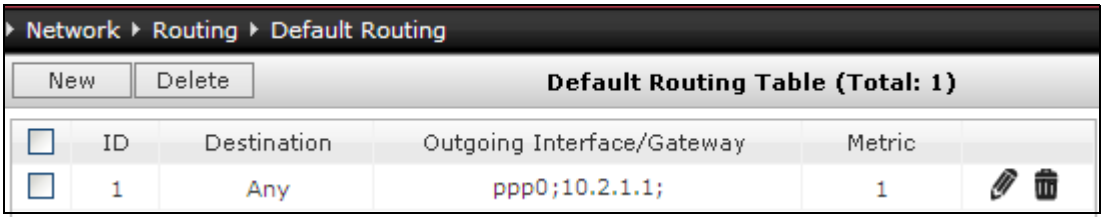
1. Choose **Network > Interfaces**. Create a PPPoE interface ppp0 holding eth1.



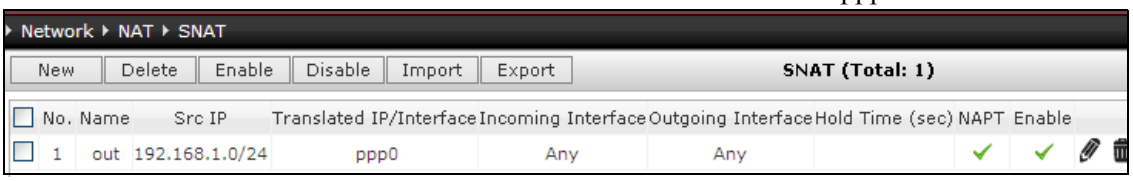
2. Create Layer 3 zone LAN and WAN. Add eth0 to LAN and ppp0 to WAN.



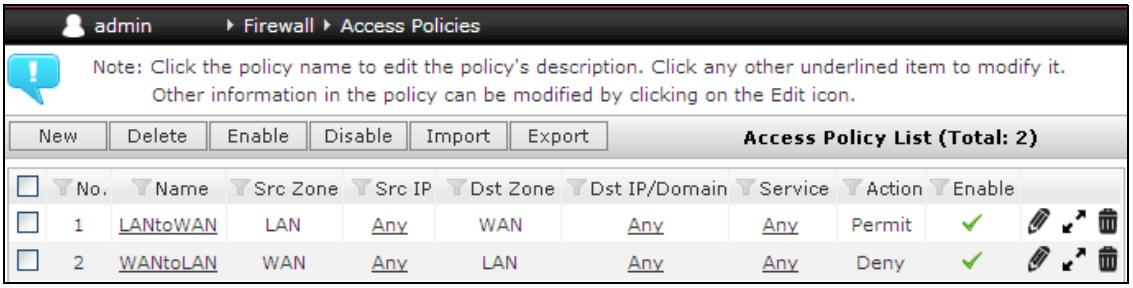
3. Modify the default gateway to 10.2.1.1:



4. Create a SNAT rule to translate 192.168.1.0/24 to the IP address of ppp0:



5. Create access policies to allow access from LAN to WAN and deny access from WAN to LAN.



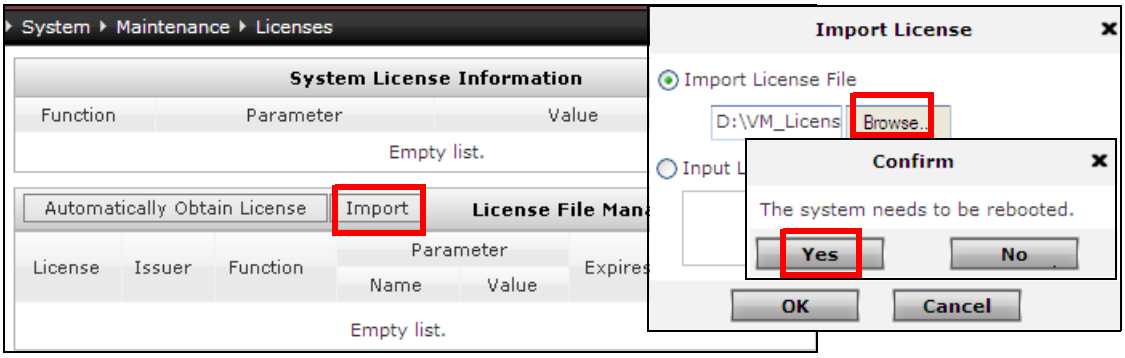
6. Click  .

7. Verify the initialized configurations as 1.4.4.5 Verify initialized configurations using WebUI.

1.5.7 Import license

Before you start the following steps, make sure the license file is already stored on your local computer.

1. Choose **System > Maintenance > Licenses**. Click **Import** to import the license. Click **Yes** at the popup prompt to reboot the system.



Note: You can also click **Automatically Obtain License** to obtain a license online, but you need to first make sure the network connectivity between your FGX device and the license server.

2. The login page appears after the system is rebooted. Login and continue configuring FGX using WebUI.

1.6 Initialize configurations using CLI

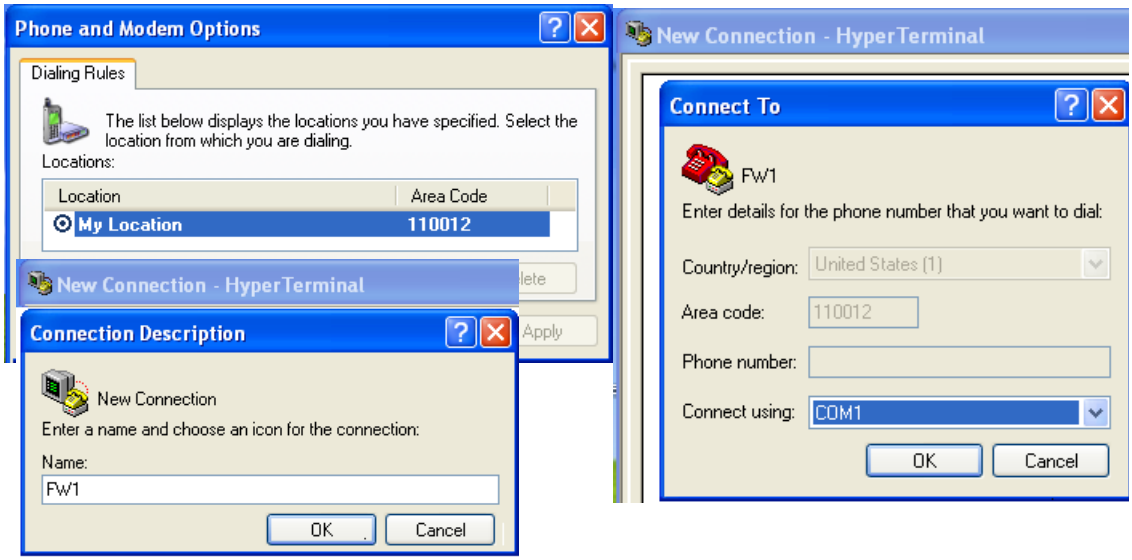
- 1.6.1 Logon using Console
- 1.6.2 CLI basics
- 1.6.3 Set system language / host name / system time
- 1.6.4 Reset password
- 1.6.5 Configure transparent mode
- 1.6.6 Routing Mode
- 1.6.7 Import license
- 1.6.8 Logon using SSH
- 1.6.9 Logon using Telnet

1.6.1 Logon using Console

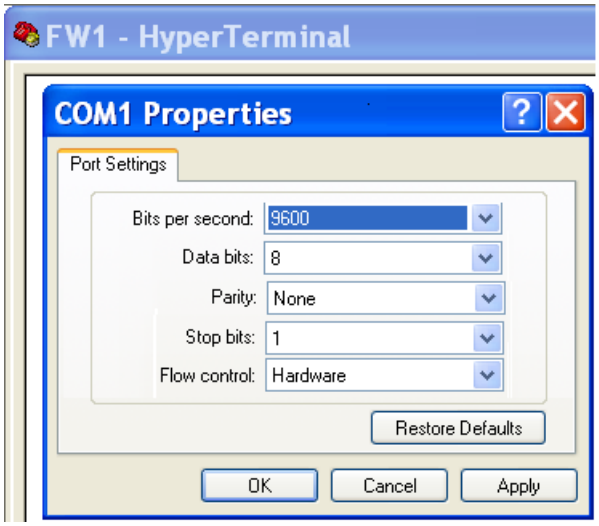
1. On your management PC, choose **Start > All Programs > Accessories > Communications > HyperTerminal**.

   a. Enter the area code and click **OK**.

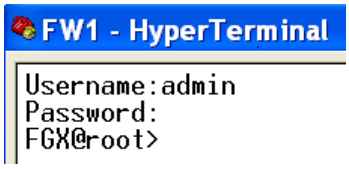
b. Click **OK** in the following dialogs.



c. Select 9600 from the first drop-down list and click **OK**.



2. Press **Enter** key and enter the default user name and password at the following prompt to logon to FGX:



1.6.2 CLI basics

The following example shows how to use the CLI to configure an Ethernet interface IP address.

```
Username:admin
Password:
FGX@root> configure mode override
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] ip address 192.168.231.3 255.255.255.0
FGX@root-system-if-eth0] exit
FGX@root-system] exit
FGX@root> save config_
```

When you first login you get this prompt:

FGX@root>

At this prompt you can enter the following commands:

- **show** commands to view system configuration, such as **show system info**, **show interface brief**, **show service** and **show route**.
- Simple commands such as **clear**, **halt**, **debug**, and **save config**.
- **configure mode override** (example above). If you execute this command, the other administrators cannot continue configuring FGX unless they get the configuration lock again, but their changes submitted will not be lost. After you enter this command, the prompt changes to **FGX@root-system]**. At this prompt you can then enter the commands shown in the following table.

Command	Item to configure	Prompt
vlan *vlan_id*	VLAN	FGX@root-system-vlan1]
interface ethernet *interface_id*	Ethernet Interface	FGX@root-system-if-eth1]
channel *channel_id*	Channel interface	FGX@root-system-if-ch1]
tunnel *tunnel_id*	VPN Tunnel Interface	FGX@root-system-tunnel1]
rint *rint_id*	Redundant Interface	FGX@root-system-rint1]
veth *veth_id*	Virtual Interface	FGX@root-system-veth1]
loopback *lo_id*	Loopback Interface	FGX@root-system-lo1]
pppoe *pppoe_id*	PPPoE Interface	FGX@root-system-pppoe1]
cluster	Cluster	FGX@root-system-cluster]
virtual router *vrid*	Virtual Router	FGX@root-system-vr1]
detection group *group_id*	Virtual Router Detection Group	FGX@root-system-dg1]
policy route *policy_name*	Policy-Based Routing	FGX@root-system-routepolicy-test]
vpn	VPN	FGX@root-system-vpn]
sslvpn	SSL VPN	FGX@root-system-sslvpn]
vsys *vsys _id*	Vsys	FGX@root-system-vsys1]
vnet *vnet_id*	Virtual Network	FGX@root-system-vnet1]

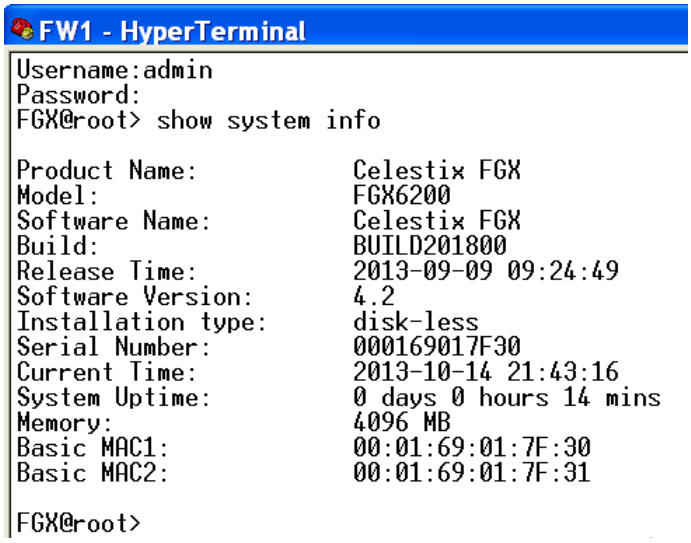
After entering one of the above commands, you can configure the item (interface, cluster/ virtual router, VPN, Vsys, etc.). In the example above you use the **ip address** command to set the IP address of the interface.

CLI supports:

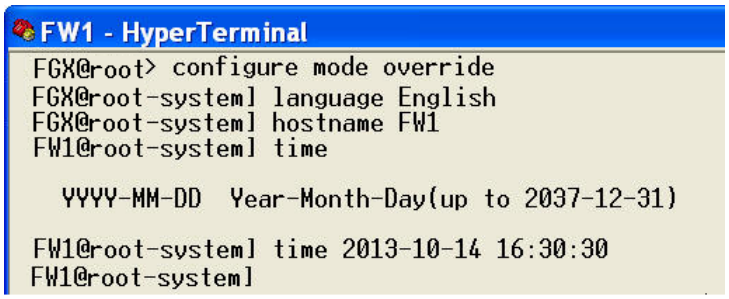
- Enter "?" right after a key word or parameter to get help information about it.
- Enter " ?"after key words or parameters to get prompt about next key word or parameter.
- Press **Tab** to complete key word entering. If there is more than one matching key word, all will be shown.
- Abbreviation. For example, **configure mode** can be abbreviated to **con mo**.

1.6.3 Set system language / host name / system time

1. View the system information using the **`show system info`** command.



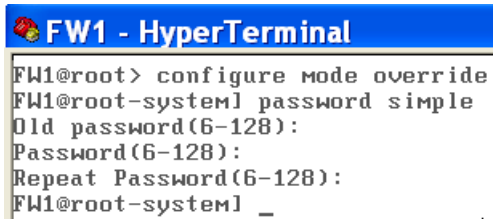
2. Set basic system configuration.



1.6.4 Reset password

To change the default login password:

1. Enter the **`configure mode override`** command and press Enter key.
2. Execute the **`password simple`** command.
3. Type the old password.
4. Type a new password.
5. Repeat the new password.



1.6.5 Configure transparent mode

1. Configure FGX to work in transparent mode:

```
FW1 - HyperTerminal
FW1@root-system] interface ethernet 0
FW1@root-system-if-eth0] working-type layer2-interface
FW1@root-system-if-eth0] exit
FW1@root-system] vlan 1
FW1@root-system-vlan1] hold ethernet 0
FW1@root-system-vlan1] hold ethernet 1
FW1@root-system-vlan1] ip address 192.168.1.100 255.255.255.0
FW1@root-system-vlan1] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-system] zone LAN based-layer2 vlan 1 eth0
FW1@root-system] zone WAN based-layer2 vlan 1 eth1
FW1@root-system] policy access LANtoWAN LAN any WAN any any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any any deny enable
FW1@root-system] end
FW1@root> save config
FW1@root>
```

2. Show interface information:

```
FW1 - HyperTerminal
 FW1@root>
 FW1@root> show interface brief
 Name       Active     IP Address                    MAC               Held In
 terfaces      MTU  Vsys
 eth0       on         192.168.1.100/24(Static)      00:01:69:01:7F:30

              1500 root


 Name       Active     Status     Speed      Duplex     Mode              Vlan Li
 st
 eth0       on         up         1000Mb/s   Full       Layer3
 eth1       on         up         1000Mb/s   Full       Layer3
 eth2       on         down                             Layer2 Access
 eth3       on         down                             Layer2 Access
 eth4       on         down                             Layer2 Access
 eth5       on         down                             Layer2 Access
```

3. Show zone information:

```
FW1@root> show zone
Name               Refcount  Policy                                    Descript
n
LAN                2         Access Policies
WAN                2         Access Policies
FW1@root> _
```

4. Show access policies:

```
FW1@root> show policy access
Number Name                From      To        Source ip       Destination ip
Source users Services      Action State  Tunnel
1      LANtoWAN             LAN       WAN       Any Ip          Any Ip
any user     any           permit enable
2      WANtoLAN             WAN       LAN       Any Ip          Any Ip
any user     any           deny   enable
FW1@root> _
```

5. Show routes (gateway):

```
FW1@root> show route

Routing table:
Type   Destination        Interface Gateway         Metric Weight Lb  IP-Track
C      192.168.1.0/24     vlan1                     0             No

Static default                        192.168.1.1     1             No


connected          1
Total              2


Routing IPv6 table:
Type   Destination                                Interface Gateway         Met
ric Weight Lb  IP-Track
```

6. Show services:

FW1 - HyperTerminal

```
FW1@root> show service

Telnet service:
  Allow Access: No
  Access:


Ssh service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255


Web service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255


Ping service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
FW1@root>
```

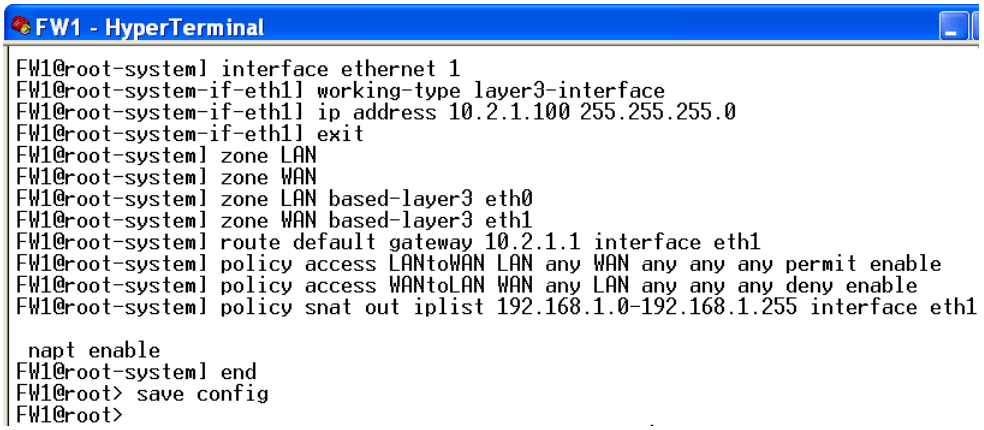
7. Verify the initialized configurations as 1.4.3.4 Verify initialized configurations using WebUI.

1.6.6 Routing Mode

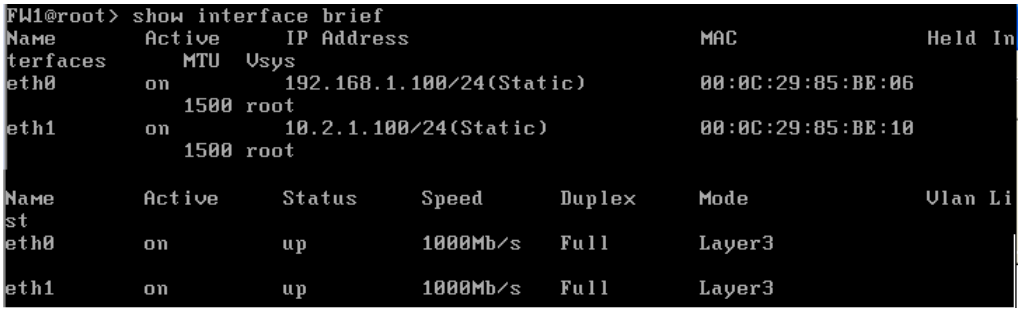
- 1.6.6.1 Ethernet connection
- 1.6.6.2 PPPoE connection

1.6.6.1 Ethernet connection

1. Set FGX to work in routing mode and to access the Internet through an Ethernet interface:

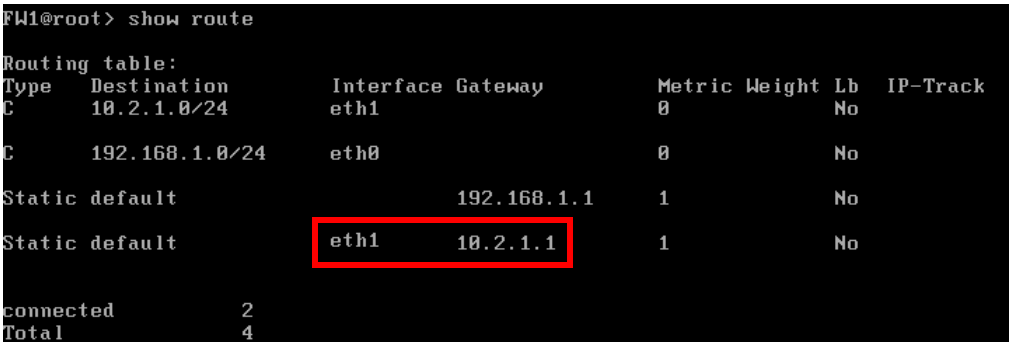


2. Show interface information:



3. Show zones:

4. Show routes (gateway):



5. Show access policies:

```
FW1@root> show policy access
Number Name                From      To        Source ip       Destination ip
Source users Services      Action State  Tunnel
1      LANtoWAN             LAN       WAN       Any Ip          Any Ip
any user     any           permit enable
2      WANtoLAN             WAN       LAN       Any Ip          Any Ip
any user     any           deny   enable
FW1@root> _
```

6. Show SNAT rules:

```
FW1@root> show policy snat

Num   Policy-Name          In-Interface Out-Interface Before-Trans        After
rans          Napt  State
1     out                  Any          Any           192.168.1.0/24      eth1
              True  Enable

FW1@root> _
```

7. Show services:

FW1 - HyperTerminal

```
FW1@root> show service

Telnet service:
  Allow Access: No
  Access:


Ssh service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255


Web service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255


Ping service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
FW1@root>
```

8. Verify the initialized configurations as 1.4.4.5 Verify initialized configurations using WebUI.

1.6.6.2 PPPoE connection

1. Set FGX to work in routing mode and to access the Internet through a PPPoE interface.

FW1 - HyperTerminal

```
FW1@root-system] pppoe 0
FW1@root-system-pppoe0] hold ethernet 1
FW1@root-system-pppoe0] username root password 000000
FW1@root-system-pppoe0] active on
FW1@root-system-pppoe0] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-system] zone LAN based-layer3 eth0
FW1@root-system] zone WAN based-layer3 ppp0
FW1@root-system] route default gateway 10.2.1.1 interface ppp0
FW1@root-system] policy access LANtoWAN LAN any WAN any any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any any deny enable
FW1@root-system] policy snat out iplist 192.168.1.0-192.168.1.255 interface ppp0

 napt enable
FW1@root-system] end
FW1@root> save config
```

2. Show interface information:

```
FW1@root> show interface brief
Name       Active     IP Address                    MAC               Held In
terfaces      MTU  Vsys
eth0       on         192.168.1.100/24(Static)      00:0C:29:3E:50:37
              1500 root


Name       Active     IP Address                    MAC               Held In
terfaces      MTU  Vsys
ppp0       on         10.2.1.100                    -                 eth1
              1454 root


Name       Active     Status     Speed      Duplex     Mode              Vlan Li
st
eth0       on         up         1000Mb/s   Full       Layer3
eth1       on         up         1000Mb/s   Full       Layer2 Access
```

3. Show zones:

```
FW1@root> show zone
Name               Refcount  Policy                                    Descript
n
LAN                2         Access Policies
WAN                2         Access Policies
```

4. Show routes (gateway):

```
FW1@root> show route

Routing table:
Type   Destination        Interface Gateway        Metric Weight Lb  IP-Track
C      10.2.1.100/32      ppp0                     0             No

C      192.168.1.0/24     eth0                     0             No

Static default                       192.168.1.1    1             No


connected          2
Total              3
```

5. Show access policies:

```
FW1@root> show policy access
Number Name                From       To         Source ip       Destination ip
Source users Services      Action State  Tunnel
1      LANtoWAN             LAN       WAN        Any Ip          Any Ip
any user     any           permit enable
2      WANtoLAN             WAN       LAN        Any Ip          Any Ip
any user     any           deny   enable
FW1@root> _
```

6. Show SNAT rules:

```
FW1@root> show policy snat

Num   Policy-Name          In-Interface Out-Interface Before-Trans        After
rans          Napt  State
1     out                  Any          Any           192.168.1.0/24      ppp0
              True  Enable

FW1@root> _
```

7. Show services:

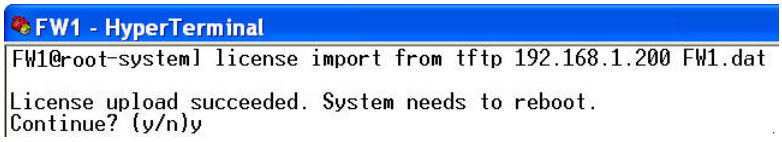
FW1 - HyperTerminal

```
FW1@root> show service

Telnet service:
  Allow Access: No
  Access:


Ssh service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255


Web service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255


Ping service:
  Allow Access: Yes
  Access:
    allow any           0.0.0.0-255.255.255.255
FW1@root>
```

8. Verify the initialized configurations as 1.4.4.5 Verify initialized configurations using WebUI.

1.6.7 Import license

1. Set up a TFTP server on your management PC and put the license file on the download directory.
2. Import license using the **`license import`** command and type "**`y`**" at the prompt to reboot the system.

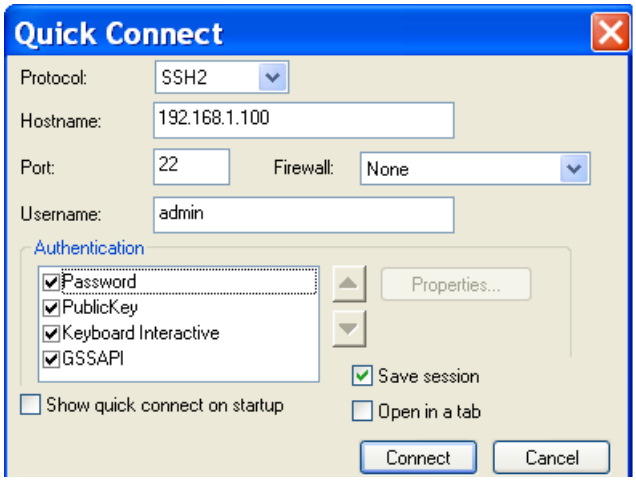


Note: All configurations will be lost if you reboot the system without saving the configurations.

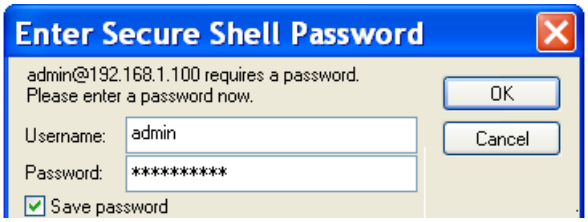
3. After reboot, log in and continue to configure FGX using CLI console.

1.6.8 Logon using SSH

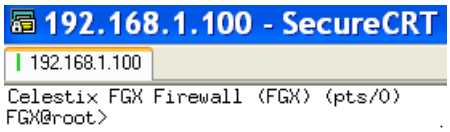
1. Open SecureCRT and click **Quick Connect**. Enter the FGX management IP address in **Hostname** text field and the default user name in **Username** text field. Click **Connect**.



2. Enter the password and click **OK**.



3. Login and configure FGX in the same way as using CLI Console.



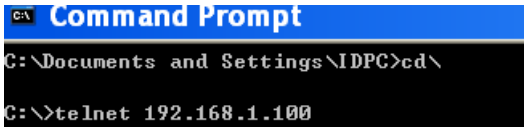
1.6.9 Logon using Telnet

Telnet service is disabled by default.

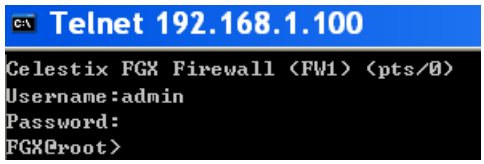
1. Before you use Telnet, enable the service through the CLI console first.

```
FGX@root> configure mode override
FGX@root-system] service telnet on
FGX@root-system] service telnet allow zone any 0.0.0.0 255.255.255.255
```

2. On your management PC, open the command prompt by choosing **Start > All Programs > Accessories > Command Prompt**, and remotely logon to FGX using telnet:



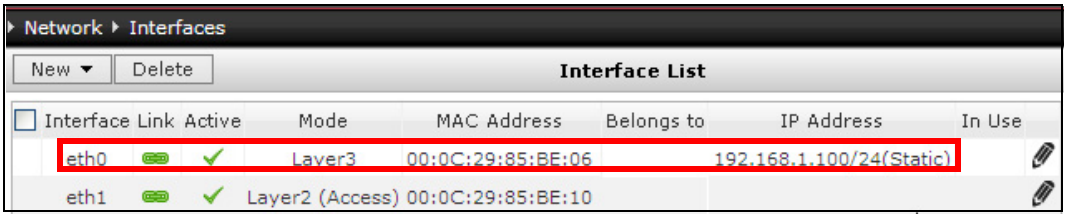
3. Login and configure FGX in the same way as using CLI Console.



1.7 Verify initialized configurations

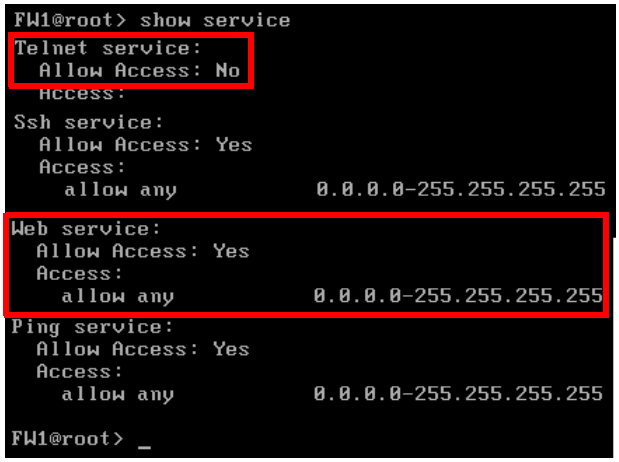
After initialization, do the following to test the network connectivity:

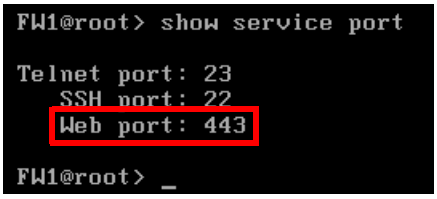
1. Ping the management interface or LAN interface eth0. If the ping fails:
   a. Check the management IP address. (By default, it is 192.168.1.100/24.)
      - WebUI: Choose **Network > Interfaces**.



      - CLI: Execute the `show interface brief` command.

   b. Check whether related service is enabled. Execute the `show service` and `show service port` commands. Telnet is disabled by default. To telnet to FGX, enable Telnet first.





   c. Check whether there is IP conflict.

      Remove the FGX device from the network and ping the management IP address from your computer. If you receive replies, there is an IP conflict.

   d. Use HTTPS instead of HTTP to access FGX through the WebUI (enter "https://" and the management IP address).

   e. Use a different browser or PC to access FGX.

   f. Check the cable connecting your PC and FGX device.

      RJ45 cable should be used and the cable should be connected to eth0 (LAN) on FGX.

      Check whether the management interface eth0 is up.

g. Check routing configurations.

If your computer and the FGX device are connected through routing devices, check whether routes are correctly configured on your computer, FGX, and the routing devices.

Enable the **ping** service on FGX, and ping the FGX management IP address from your computer.

```
FW1@root-system] service ping on
FW1@root-system] service ping allow zone any 0.0.0.0 255.255.255.255
```

If the ping fails, check the routes and the topology. Execute the **`show route`** command to view routes on FGX.

```
FW1@root> show route

Routing table:
Type   Destination        Interface Gateway         Metric Weight Lb  IP-Track
C      192.168.1.0/24     eth0                      0             No

Static default                        192.168.1.1     1             No


connected          1
Total              2


Routing IPv6 table:
Type   Destination                                 Interface Gateway         Met
ric Weight Lb  IP-Track

connected          0
Total              0

FW1@root> _
```

2. Ping the WAN interface connected to the Internet. If the ping fails:

- For transparent mode, check the configurations of zones and access policies on FGX.
- For routing mode, check the configurations of zones, access policies, routes, and NAT rules on FGX and the gateway on your management PC.

  Access policies are matched from the highest priority to the lowest. Once a policy is matched, the others will not be matched any more.

3. Ping the gateway of FGX. If the ping fails:

- Check the default route on FGX.
- Check the cable connecting FGX and its gateway.

4. Access the Internet. If the access fails,

- Check all the above steps. If you can ping the FGX's gateway successfully, trace routes to the website you are accessing to determine whether the problem occurs.
- Check whether you forget to save configurations before you restart the system.

1.8 Common problems

Problem 1

Cannot access the FGX system after initialization.

Solution

- Check whether the management interface or IP has been changed during initialization.
- Check whether the gateway of FGX has been changed during initialization.

Problem 2

Can login but the WebUI displayed is incorrect.

Solution

- Clear browsing cache and try again.
- Check whether there is IP conflict.

Problem 3

Cannot configure functions after login.

Solution

- No configuration lock. Click the configuration lock icon  on WebUI or execute the **`configure mode override`** command in CLI to obtain the configuration lock.
- Not licensed. To upload a license, see 1.4.6 Import license.

Problem 4

Cannot use wizard a second time.

Solution

- Reset the system. Choose **System > System Overview** and click **Reset** on the WebUI, or execute the **`reset`** command in CLI.
- If you exit the wizard without completion, then configurations will be lost.

Problem 5

Cannot activate the license.

Solution

- Check whether FGX IP is on the same subnet with the license server.
- Configure DNS server for FGX to resolve DNS requests.
- Check the connectivity between FGX and the Internet.

Problem 6

Cannot log on to FGX through the WebUI.

Solution

- Check whether the Web service is enabled.
- If you enter the wrong password 5 times in a row, the account is locked for 20 minutes.
- Execute the **df** command in the CLI to make sure that enough storage space is available.

Problem 7

Cannot access the Internet through the PPPoE interface.

Solution

- Active the PPPoE interface on FGX and check the bound Layer 2 Ethernet interface cabling.
- Check the user name and password configured for the PPPoE interface on FGX.
- Check the connectivity between the PPPoE interface and the Internet.

1.9 Next steps

The following are the recommended configuration steps after you finish initialization.

Table 2 Recommended Configuration Steps

WebUI Menu Path	Description	User guide section
System (Users)		
System > Authentication > Administrative Users	Create Vsys administrators if Vsys is used.	3.13 Administrative Users
System > Authentication > Users	Create network users allowed to access network resources through FGX.	3.14 Users
Network (Interfaces & Zones) and Routing (for routing mode only)		
Network > Interfaces	Configure interface IP addresses according to your topology and optionally choose to enable IPv6.	4.1 Interfaces Overview to 4.9 Tunnel Interface
Network > Zones	Create more zones according to your network topology so that you can configure policies according to zones to control access and security.	4.12 Zones
Network > Routing/Multicast	Add static, policy-based, and multicast routes so that FGX can successfully forward data passing through it.	6 Routing
Security (Policies & Attack Defense & UTM)		
Firewall > Access Policies / Multicast Policies	Create access and multicast policies to forward traffic passing through FGX.	8.2.2 Create Access Policy and 8.2.4 Create Multicast Policy
Firewall > Default Policy Settings	Set default inter-zone and intra-zone policy actions.	8.2.3 Configure Default Access Policies
Firewall > IP-MAC Binding Policies / Session Policies	Configure IP-MAC binding policies and session policies to protect the internal network from IP spoofing and session floods.	8.2.1 Configure IP-MAC Binding and 8.2.5 Create Session Policy
Firewall > Attack Defense	Configure attack defense settings to defend against network-layer attacks.	9 Attack Defense
UTM	Update UTM rules, including applications, URL categories, anti-virus rules, anti-spam rules, and attack signature rules. Configure UTM policies and settings to provide deep (higher-layer) security.	10 Unified Threat Management
VPN, HA, Vsys		
VPN (IPSec VPN, SSL VPN Portal, SSL VPN Tunnel)	Configure VPN to provide security tunnels for communication between two sites or between remote users and a site.	6 Routing
System > High Availability	Configure high availability to ensure the availability of FGX.	12 High Availability
System > Virtual Systems	By dividing the root system into virtual systems, you can save device cost and reduce the workload of the root system administrator.	13 Virtual Systems

2 Functional overview

This chapter provides a general overview of FGX functionality.

Basic system/network configuration

- 2.1. System configuration. Setting system date/time, local access control, licenses, users and authentication, certificates, system updates, backup/restore, diagnosis, technical support, centralized management, logging and alert policies, and so on.
- 2.2. Network configuration. Setting interfaces, ARP/CAM, STP, zones, DNS, DHCP, and IPv6 features such as DHCPv6 and Neighbor Discovery.

Routing/security configuration

- 2.3. Packet processing overview. A flow diagram and short description of how packet processing is determined by the routing/security settings for Routing, NAT, Firewall (Policies), Attack Defense, and UTM.
- 2.4. Routing. Routing/multicasting features for forwarding packets, including static routing, policy-based routing, multicast routing, DVMRP, and IGMP snooping.
- 2.5. Network Address Translation (NAT). Includes SNAT, DNAT, and MIP.
- 2.6. Quality of service (QoS). QoS provides better service to selected network traffic.
- 2.7. Firewall policies. Access policies, default policy settings, multicast policies, session policies, IP-MAC binding policies to control the traffic passing through FGX.
- 2.8. Attack defense. Defense against common network attacks.
- 2.9. Unified threat management (UTM). UTM provides advanced security protection.
  - Export Control: 2.9.1. Application control, 2.9.2. HTTP control, and 2.9.3. DNS control
  - 2.9.4. Client protection
  - 2.9.5. Server protection

VPN, HA, and Vsys/Vnet

- 2.10. Virtual private networks (VPN). IPSec VPN and SSL VPN (Web Portal/Tunnel).
- 2.11. High availability (HA). Provides device redundancy and backup through virtual routers, virtual router detection groups, and clusters.
- 2.12. Virtual systems/networks (Vsys/Vnet). The root system can be divided into multiple virtual systems (Vsys). Vsys enables you to have separate administrators, policies and other functions for different subnets and decreases management workload and device cost. Vnet allows communication between virtual systems.

Monitoring, logs and reports

- 2.13. Monitor/Logs. Monitors system running and enables you to search for logs.
- 2.14. Reports. A WebUI-based application. Generates reports about system, traffic, Web security, mail security, anti-virus, attacks, applications, and users on a scheduled basis.

2.1. System configuration

The following table lists WebUI menu items, description and a link to the relevant user guide section.

Table 1 System Configuration Steps

	WebUI Menu Path	Description	User guide section
Basic system information			
1.	**Home** and **System > Overview > System Information**	View general system parameters.	3.1 Home, 3.2 System Overview
2.	**System > Service Configuration> Banners**	Set banner.	3.3 Banners
3.	**System > Asset Information > Asset summary, Copyright information**	Display system assets and copyright information.	3.4 Asset Summary, 3.5 Copyright Information
System time			
4.	**System > Maintenance > Date and Time**	Set the date, time.	3.6 System Time
License and updates			
5.	**System > Maintenance > Licenses**	License information overview. Automatic and manual license activation is supported.	3.7 Licenses
6.	**System > System Update > Update, Manage Installation Packages, Manage Patch Packages**	Manually or automatically upload updates, installation packages and patch packages.	3.8 Update, 3.9 Installation Package Management, 3.10 Patch Package Management
Access settings			
7.	**System > Service Configuration> Access Settings** and **SNMP Configuration**	Access control for telnet, SSH, web, ping, and root access. SNMP configuration.	3.11 Access Services, 3.12 SNMP
Authorization and authentication			
8.	**System > Authentication > Administrative users** and **Users**	Administrators and users.	3.13 Administrative Users, 3.14 Users
9.	**System > Authentication Configuration, Authentication Servers, WebAuth Configuration**	User authentication.	3.15 User Authentication, 3.16 WebAuth Configuration
System maintenance			
10.	**System > Maintenance > Backup/Restore**	Backup the unit or root configuration to a file. Restore from file.	3.17 Backup and Restore
11.	**System > Maintenance > Technical Support**	Generate a system diagnostic file.	3.18 Technical Support
12.	**System > Maintenance > Centralized Management**	Configure whether to allow being managed by a centralized management system.	3.19 Centralized Management
13.	**System>Logging Configuration> Alert Configuration** and **Log Maintenance**	Configure Local_Log, Syslog, SNMP, and email alerts. Download log files.	3.21 Alert Configuration, 3.22 Log Maintenance
System-wide			
14.	**System > Certificates > Local Certificates, CA Certificates**	Import/manage CA and local certificates for user authentication and VPN negotiation.	3.23 Certificates

Table 1 System Configuration Steps (*continued*)

	WebUI Menu Path	Description	User guide section
15.	**System > Objects IP Addresses, Services**	Add IP and service objects for policies and rules.	3.24 Objects

2.2. Network configuration

The following table lists the WebUI menu items for Network Configuration, a short description and a link to the relevant user guide section.

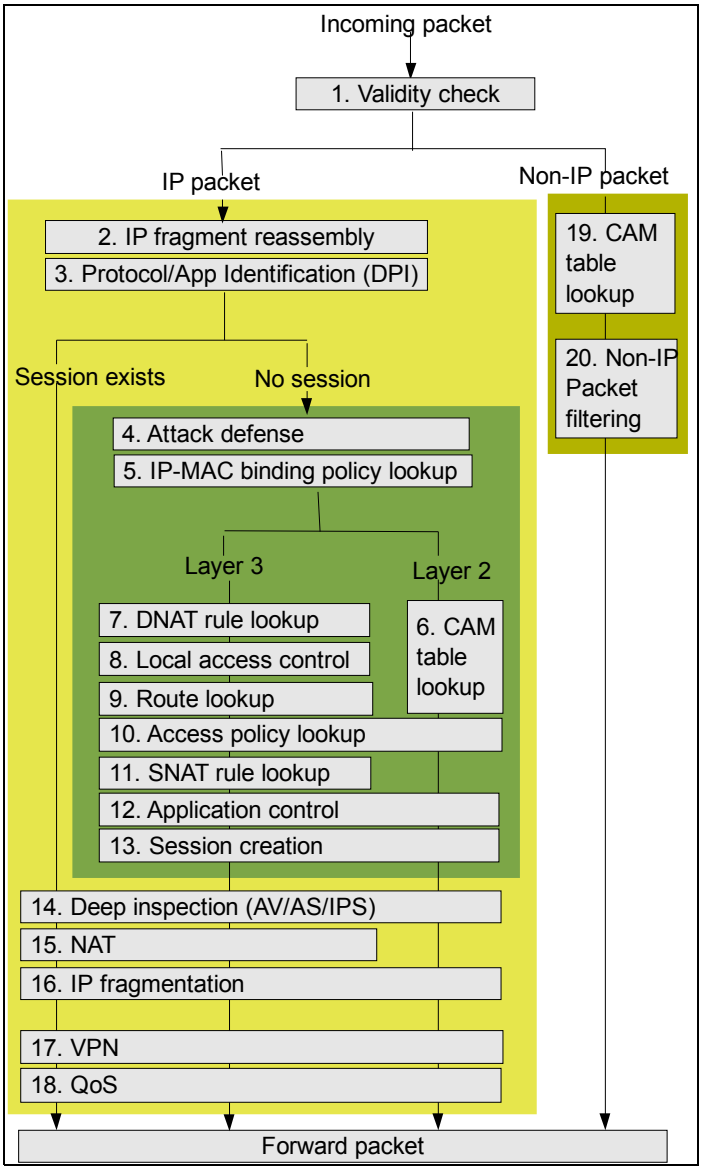
Table 2 Network Configuration Steps

	WebUI Menu Path	Description	User guide section
Interfaces, zones			
1.	**Network > Interfaces**	Interfaces allow traffic to flow in and out of a security device. FGX interfaces can be physical or logical.	4.1 Interfaces Overview 4.2 Ethernet Interface to 4.9 Tunnel Interface
2.	**Network > Zones**	A zone is a collection of interfaces, each connecting to a separate network segment. Binding the interfaces together enables FGX to perform uniform security control over a single logical network.	4.12 Zones
Switching			
3.	**(none)**	Configure ARP and CAM tables through the CLI.	4.10 ARP, 4.11 CAM
4.	**Network > STP**	The Spanning Tree Protocol (STP) is used to eliminate loops on Layer 2 network while providing path redundancy.	4.19 STP
5.	**Network > IPv6 > Neighbor Discovery**	The Neighbor Discovery (ND) protocol is used by nodes (hosts and routers) to discover neighbors on the same link.	4.20 Neighbor Discovery
DNS, DHCP			
6.	**Network > DNS > Host**, **DNS Proxy**, **Static Cache**	Configure DNS servers for FGX working as a DNS host or proxy, and configure DNS static cache for FGX. DNSv6 is also supported.	4.13 DNS Host, 4.14 DNS Proxy, 4.15 DNS Cache
7.	**Network > DHCP** > **DHCP Servers**, **DHCP Server Subnets**	Set FGX to work as a DHCP server, relay agent, or client. Configure DHCP subnets when setting FGX to a DHCP server.	4.16 DHCP Servers, 4.17 DHCP Server Subnets
8.	**Network > IPv6 > DHCPv6**	Stateful DHCPv6 (assigns prefixes to hosts) and stateless DHCPv6 (assigns domain names and server addresses to hosts).	4.18 DHCPv6

2.3. Packet processing overview

The following diagram provides an overview of how FGX processes packets. The numbered items in the diagram are described in more detail on the following page.

Figure 1 Packet Processing



The following table describes the above diagram. "#" is the number in the diagram. "This chapter" and "Other chapters" show where to find more information.

Table 3 Packet Processing Steps

#	IP	Session Layer		FGX packet processing function	This chapter	Other chapters
1.				**Validity check.** Checks packet validity (common errors such as all-zero IP/MAC address). No settings.	---	---
2.	IP			**IP fragment reassembly**. Receive all packet fragments, then re-assemble into a packet for check.	---	---
3.	IP			**Protocol / application identification (DPI)**. Identifies packet protocol and application before sending to specific engine for check.	---	---
4.	IP	No		Run **attack defense**. Checks for DoS, reconnaissance, and ICMP attacks and IP options, and perform TCP evasion control.	2.8. Attack defense	9.3. Basic Configuration Steps
5.	IP	No		Checks packet IP address **IP-MAC binding policies** (prevent IP spoofing).	2.8. Attack defense	9.3. Basic Configuration Steps
6.	IP	No	2	Checks the **CAM table** and forwards the packet to the outgoing interface corresponding to the destination IP address. Then go to Steps 9, 11, 12, 13, 15, 16, 17.	2.2. Network configuration	4.11 CAM
7.	IP	No	3	Checks the packet against **DNAT** rules.	2.5. Network Address Translation (NAT)	5.2.2. Create DNAT Rule
8.	IP	No	3	Checks the packet against **local access control** policies.	2.1. System configuration	3.11 Access Services
9.	IP	No	3	Performs a **route lookup** to find the route to the destination.	2.4. Routing	6.2. Basic Configuration Steps
10.	IP	No		**Access policy lookup.** IP packet filter policies.	2.7. Firewall policies	8.2.2 Create Access Policy
11.	IP	No	3	Checks the packet against **SNAT** rules.	2.5. Network Address Translation (NAT)	5.2.1. Create SNAT Rule
12.	IP	No		**Application-layer control** on application-layer data.	2.9. Unified threat management (UTM)	10.2. Basic Configuration
13.	IP	No		**Session Creation.** Saves the current session request information in the session table and forwards the session request.	---	---
14.	IP			**Deep inspection** (**UTM: AV/AS/IPS**) of traffic.	2.9. Unified threat management (UTM)	10.2. Basic Configuration
15.	IP		3	Performs network address translation (**NAT**).	2.5. Network Address Translation (NAT)	5.1. Overview
16.	IP			**IP fragmentation**. Fragment packet before forward.	---	---
17.	IP			**VPN**. Encrypts and sends packets into VPN tunnels.	2.10. Virtual private networks (VPN)	11.2. Configuration Basics
18.	IP			**QoS**. Controls bandwidth.	2.6. Quality of service (QoS)	7.2. Basic configuration steps
19.	Non-IP			Checks **CAM table** and forwards packet to outgoing interface corresponding to the destination IP address.	2.2. Network configuration	4.11 CAM
20.	Non-IP			Checks packet against default **non-IP packet filter** policy (enabled and allowed by default).	---	---

2.4. Routing

The following introduces basic routing / switching concepts for

- 2.4.1. Layer 3 Unicast.
- 2.4.2 Layer 3 Multicast.
- 2.4.3 Layer 2 Multicast.

2.4.1. Layer 3 Unicast

Layer 3 unicast routing routes a packet based on

- Matching (incoming) policy (specifies packet source parameters) and
- Matching policy's matching (outgoing) route (specifies destination parameters)

The table below summarizes (1) policies and (2) routes.

1. Policy table contains multiple non-default policies and 1 default policy.

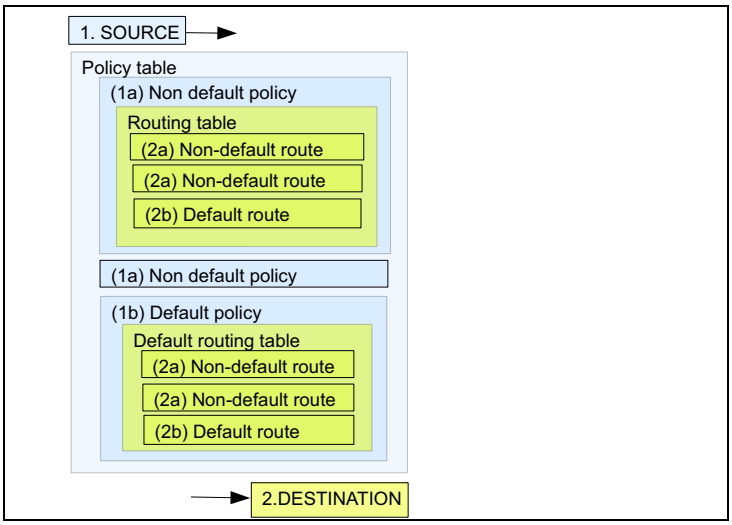
   (1a) Non-default policies define unicast packet source
   - Interface(s) (1 or ALL)
   - IP(s)
   - TOS
   - Service(s)

   (1b) Default policy defines nothing (used if no matching non-default policy with a matching route).

2. Policy routing table (one for each policy) contains multiple non-default routing entries and 1 default routing entry.

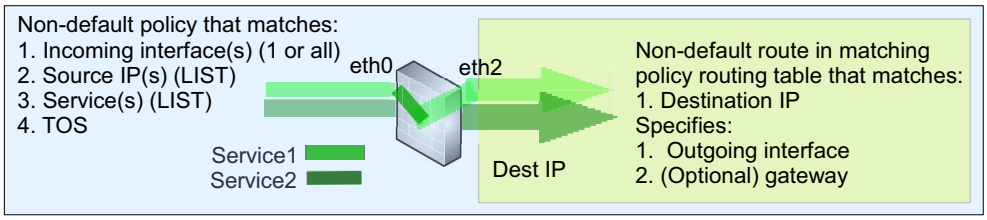
   (2a) Non-default routes defines
   - Unicast packet destination IP.
   - Outgoing interface (+ gateway). If load balancing is enabled, then defines multiple outgoing interfaces/gateways and weight/tracking parameters.

   (2b) Default route defines
   - Outgoing interface (+ gateway). If load balancing is enabled, then defines multiple outgoing interfaces/gateways and weight/tracking.

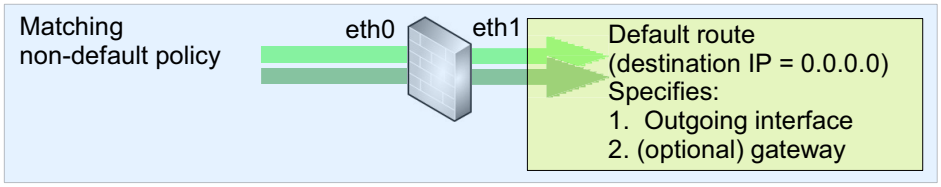


The following shows an overview of the policy/route combinations.

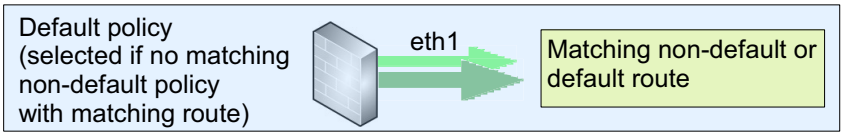
- (1a) Non-default policy / (2a) non-default route.



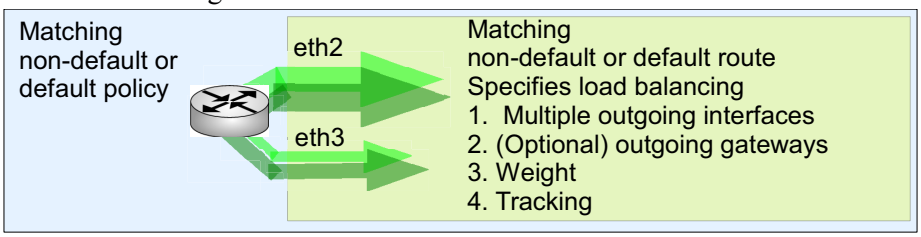
- (1a) Non-default policy, (2b) default route.



- (1b) Default policy.



- Load balancing.



The following table lists the WebUI menu items, a short description and a link to the relevant user guide "Basic Configuration Steps" section.

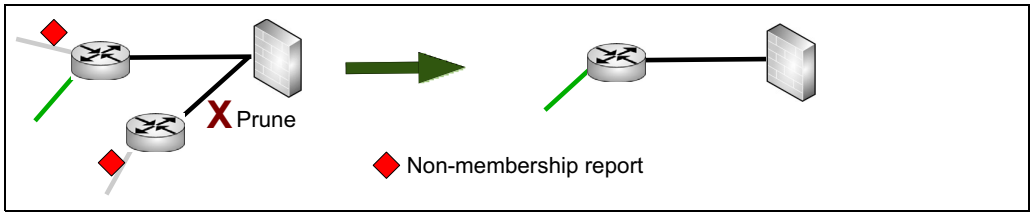
Table 4 Unicast Configuration Steps

	WebUI Menu Path	Description	User guide section
1.	**Network > Routing > Policy-Based Routing**	**Layer 3 unicast policy** For the policy route with the highest "No." (priority) that matches the incoming interface/source_IP/Service/TOS, determine the matching outgoing routing table.	6.1.1 L3 Unicast
2.	**Network > Routing > Default Routing**	**Layer 3 unicast route** The matching route in the routing table that matches the policy determines the outgoing interface(s)/gateway(s).	6.1.1 L3 Unicast

2.4.2 Layer 3 Multicast

- **Layer 3 Multicast dynamic (DVMRP).** Dynamically generate a routing table with distances for the multicast group interfaces based on DVMRP. The metric determines the relative "cost" of the interface (used to determine which interface to forward from), and the threshold defines how high the time-to-live (TTL) of the packets must be to be forwarded.

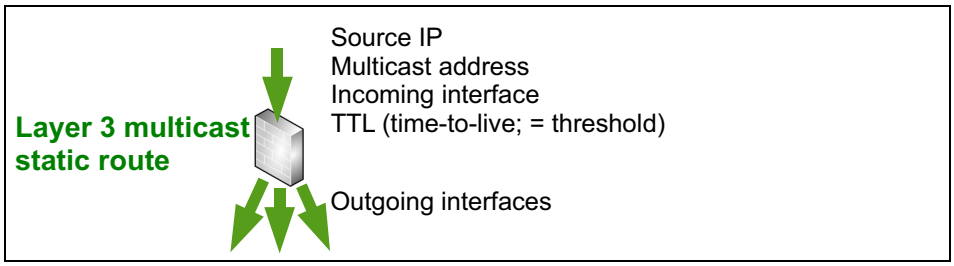
  The cache and prune lifetimes are used to avoid forwarding unrequired multicast packets. When no membership report is received, a multicast group node is pruned.



- **Layer 3 Multicast static.** Layer 3 multicast routing table static routes determine the forwarding interface(s) based on

  1. Source IP address.
  2. Multicast group IP address.
  3. Incoming interface.

  DVMRP must be enabled for the forwarding interface. TTL (time to live) for forwarded packets is also required. It is actually the same as DVMRP threshold.



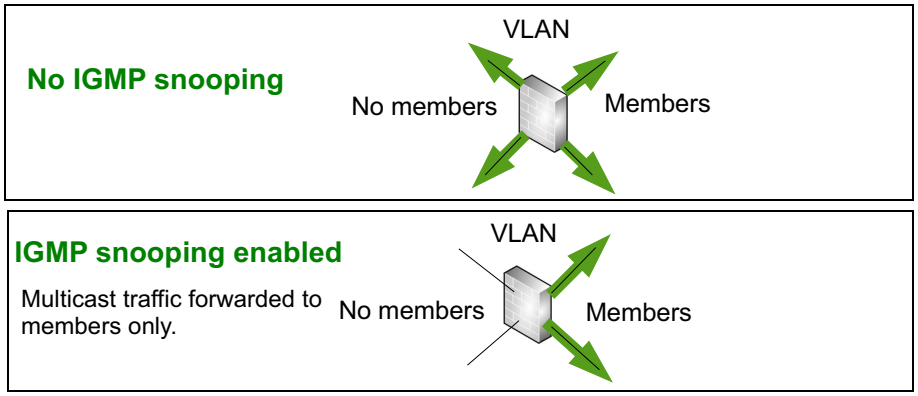
The following table lists the WebUI menu items, a short description and a link to the relevant user guide "Basic Configuration Steps" section.

Table 5 Layer 3 Multicast Configuration Steps

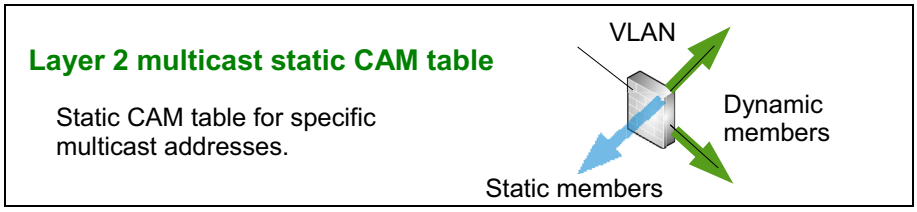
	WebUI Menu Path	Description	User guide section
1.	**Network > Multicast > DVMRP**	**Layer 3 multicast dynamic**. Dynamically generate a routing table with distances for the multicast group interfaces based on DVMRP.	**6.1.2.1 L3 Multicast dynamic**
2.	**Network > Routing > Multicast Routing**	**Layer 3 multicast static**. Based on source IP address, multicast group IP address, and incoming interfaces, multicast routing determines interfaces for forwarding packets.	**6.1.2.2 L3 Multicast static**

2.4.3 Layer 2 Multicast

Layer 2 Multicast dynamic (IGMP snooping). Hosts use IGMP to dynamically join or leave multicast groups. FGX supports IGMPv1 and IGMPv2.



Layer 2 Multicast static. Static CAM tables determine the forwarding interface(s) based on multicast destination IP address (and MAC address).



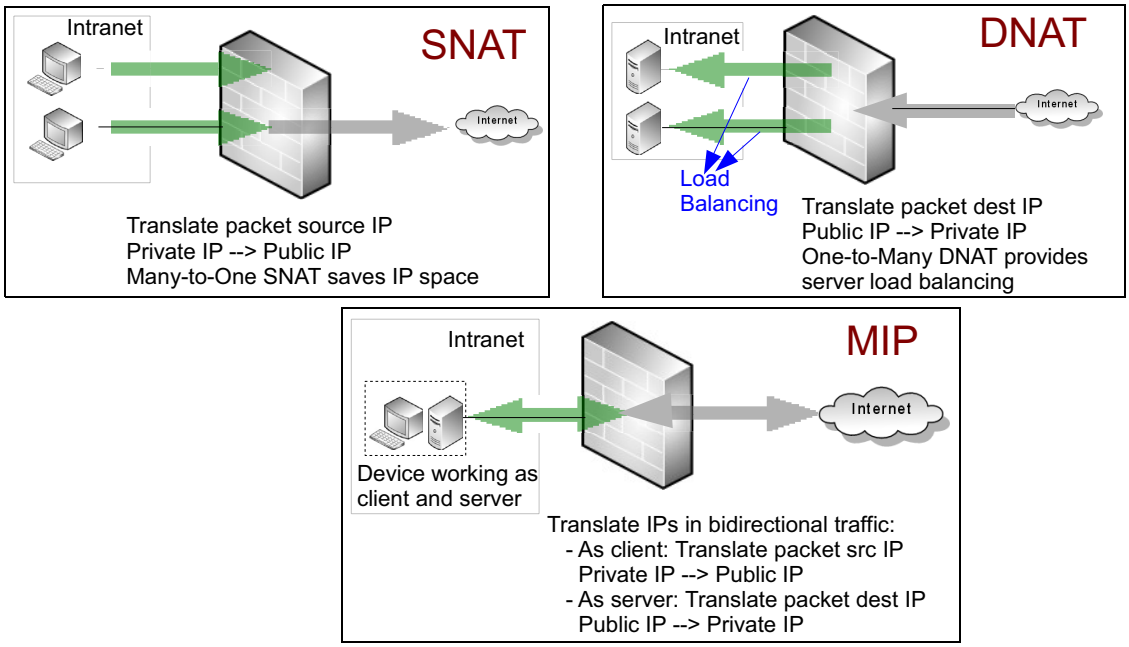
The following table lists the WebUI menu items, a short description and a link to the relevant user guide “Basic Configuration Steps” section.

Table 6 L2 Multicast Configuration Steps

	WebUI Menu Path	Description	User guide section
1.	**Network > Multicast > IGMP Snooping**	**Layer 2 Multicast Dynamic**. Multicast CAM entries for VLAN. Learned from IGMP snooping.	**6.1.3.1 L2 Multicast dynamic (IGMP snooping)**
2	**Network > Multicast > IGMP Snooping**	**Multicast static Layer 2**. Manually created.	**6.1.3.2 L2 Multicast static**

2.5. Network Address Translation (NAT)

The following diagram illustrates **SNAT**, **DNAT** and **MIP** concepts.



The following table gives an overview of NAT types.

Table 7 NAT Types

	NAT type	Priority	Type
1.	SNAT	2	1 to 1 Many to 1 Many to many
2.	DNAT	2	1 to 1 1 to many
3.	MIP	1	1 to 1

The following table lists the WebUI menu items for NAT, a short description and a link to the relevant user guide section.

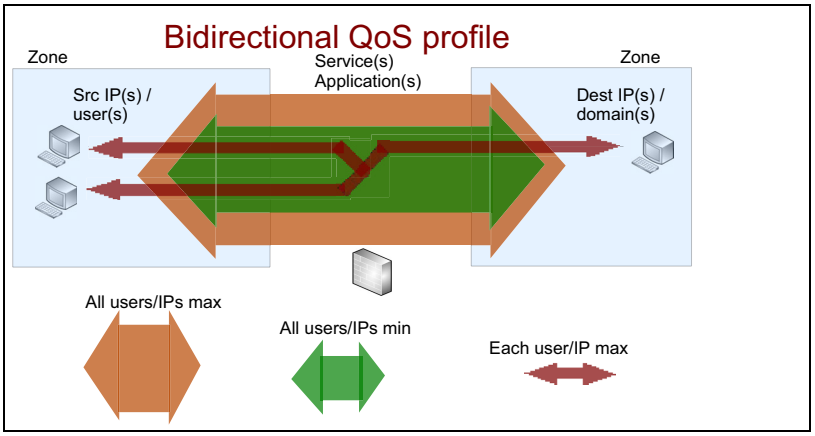
Table 8 NAT Configuration Steps

	WebUI Menu Path	Description	User guide section
1.	**Network > NAT > SNAT**	Source Network Address Translation (SNAT).	5.2.1. Create SNAT Rule
2.	**Network > NAT > DNAT**	Destination Network Address Translation (DNAT).	5.2.2. Create DNAT Rule
3.	**Network > NAT > MIP**	Mapped IP (MIP). Basically a combination of SNAT and DNAT.	5.2.3. Create MIP Rule

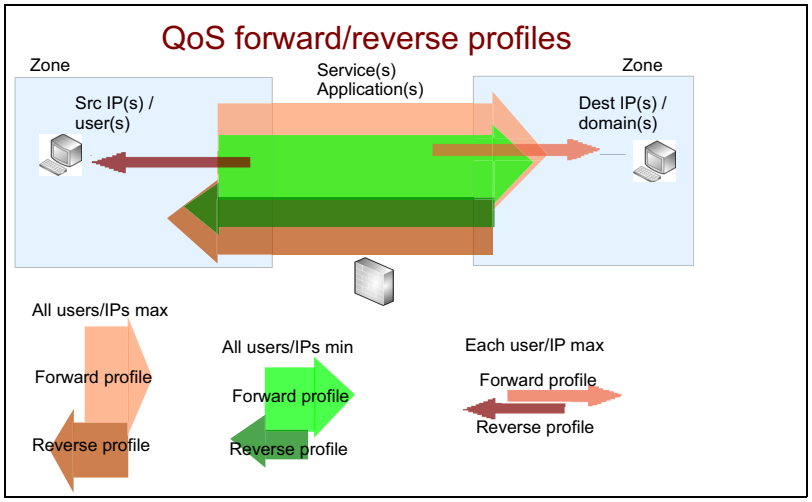
2.6. Quality of service (QoS)

The following diagram illustrates QoS concepts. A QoS policy specifies the

- Application/services maximum / guaranteed minimum bandwidth between a source zone IP's / users and the destination zone IP's / domains (source/destination zones can be any).
- Max bandwidth for user/IP.



The following diagram illustrates QoS forward/reverse profile concepts.



The following table lists the WebUI menu items for QoS, a short description and a link to the relevant user guide section.

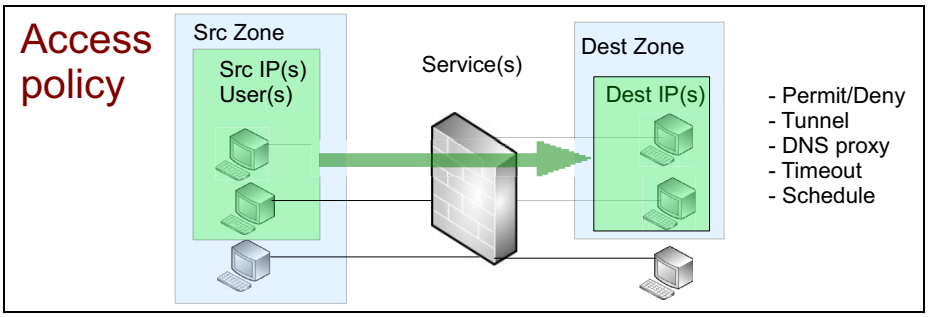
Table 9 QoS Configuration Steps

	WebUI Menu Path	Description	User guide section
1.	**UTM > QoS > QoS Profiles**	Create general QoS profiles to define priority, maximum bandwidth, guaranteed bandwidth, and DSCP value.	7.2.1 Create general QoS profiles
2.	**UTM > QoS > Per IP/User QoS Profiles**	Create per IP/user QoS profiles to define the maximum bandwidth for traffic per IP or user.	7.2.2 Create per IP/ user QoS profiles
3.	**UTM > QoS > QoS Policies**	Create QoS policies to define traffic on which QoS control will be performed.	7.2.3 Create QoS policies

2.7. Firewall policies

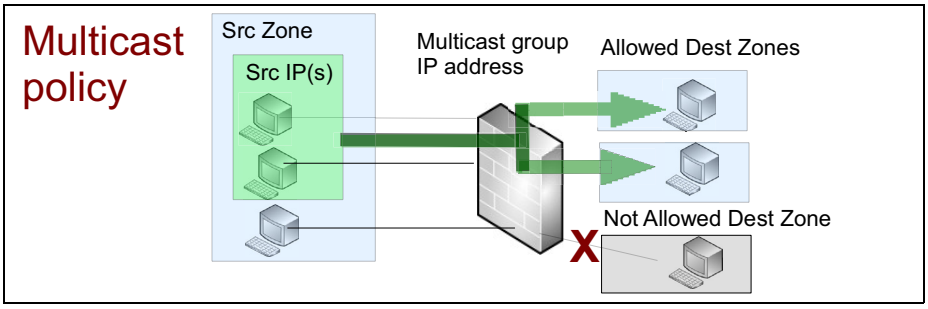
The following diagram illustrates firewall **access policies** (for non-multicast packets):

- Allow/block (Permit / Deny) packets of the service type transmitted between source zone IP's / users and the destination zone IP's (zones can be any). Also match the following optional configuration items:
  - Tunnel: Send the packets via the selected VPN tunnel.
  - Transparent DNS proxy: Enable/Disable.
  - Specific Timeout: Remove the matching session if the specified timeout is reached.
- Schedule determines when the policy takes effect.



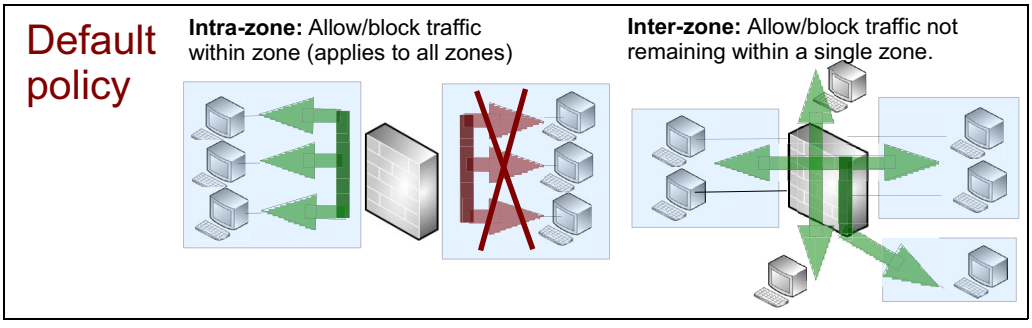
The following diagram illustrates firewall **multicast policies**:

- Allow/block packets (allowed/blocked destination zones) with the multicast group address from the source zone IP's / users (source zone can be any).



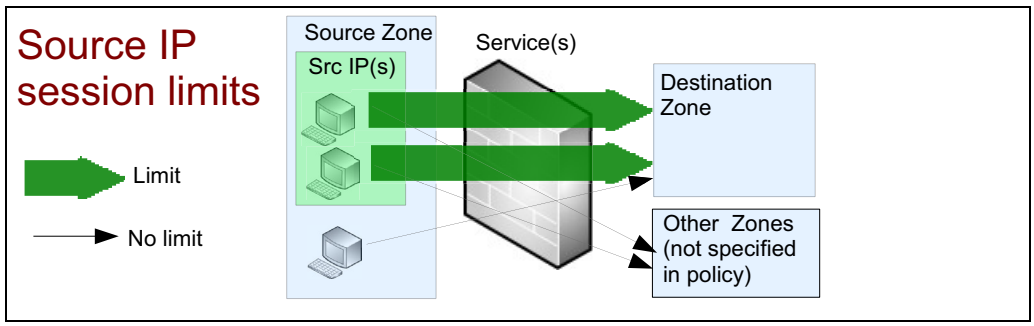
The following diagram illustrates firewall **default policies**:

- **Intra-zone policies**: Allow/block packets within a zone (policy applies to all zones).
- **Inter-zone policy**: Allow/block packets not remaining within a single zone.

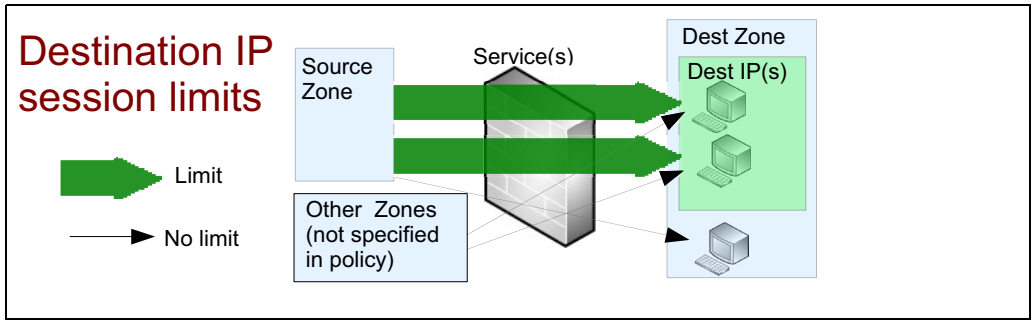


The following 3 diagrams illustrate firewall **session limit policies**. For each policy type, drop/alert (if enabled) any new matching session that would go over the threshold.

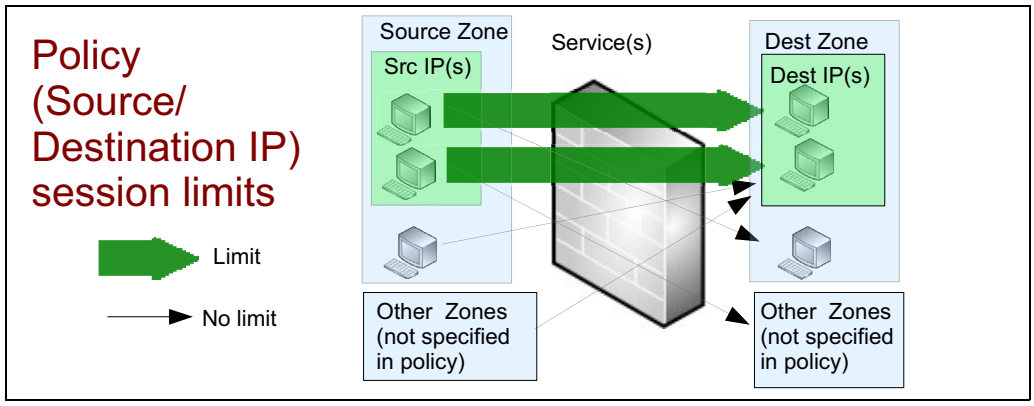
1. **Source IP Based Session Limit policies**: Match the session against the specified source/destination zone, source IP and service.



2. **Destination IP Based Session Limit policies**: Match the session against the specified source/destination zone, destination IP and service.



3. **Policy (source/destination IP) Based Session Limit policies**: Match the session against the the specified source/destination zone/IP and service.



The following table gives an overview of firewall policies. For each policy type the table lists the priority, then packet source/destination criteria and corresponding firewall action.

Table 10 Policy Types

	Firewall policy type	Priority	Packet source criteria	Packet destination criteria	Actions
1.	Default policy settings / Inter-zone	2	(none)	(none)	Permit/Deny
	Default policy settings / Intra-zone	2	Zone	Zone	Permit/Deny
2.	Default policy settings / Default session timeouts	2	(none)	(none)	(timeout)
3.	Access policies	1	Zone IPs Users Services	Zone IPs/Domains Services	Permit/Deny Tunnel DNS proxy Timeout
4.	Multicast policies		Zone (or any) IPs	Multicast group IPs Zones	Permit
5.	Session policies / Session limit based on one of the following: 1. Policy, 2. Source IP, or 3. Destination IP	1	Zone (or any) IPs	Zone (or any) IPs Services	Drop Alert Drop + Alert

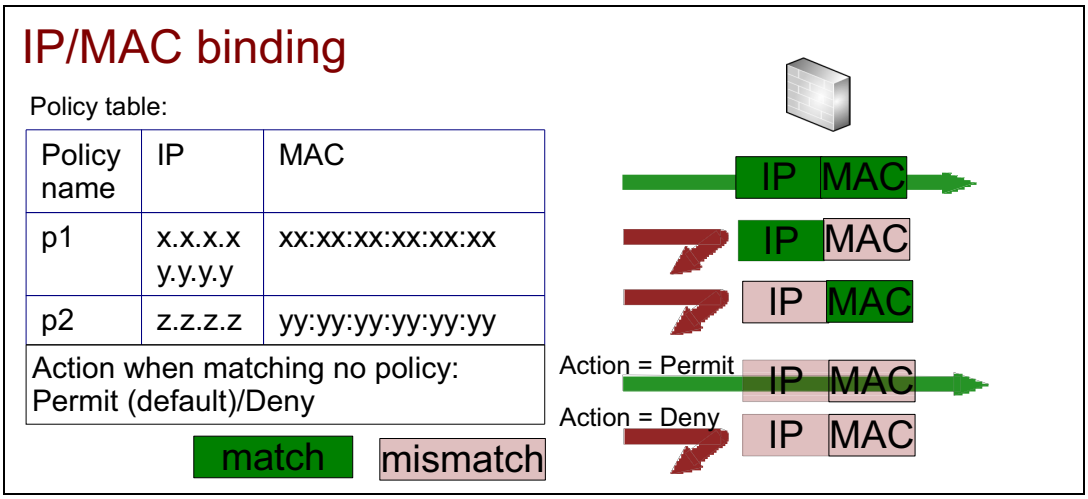
The following table lists the WebUI menu items, description and a link to the user guide.

Table 11 Policy Configuration Steps

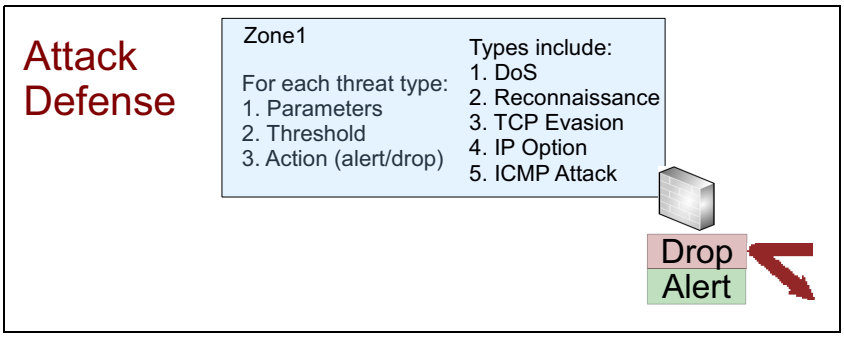
	WebUI Menu Path	Description	User guide section
1.	**Firewall > Access policies**	Zone to zone	8.2.2 Create Access Policy
2.	**Firewall > Default policy settings**	All zones	8.2.3 Configure Default Access Policies
3.	**Firewall > Multicast policies**	Multicast zones	8.2.4 Create Multicast Policy
4.	**Firewall > Session policies**	Sessions limits zone to zone	8.2.5 Create Session Policy

2.8. Attack defense

The following diagram describes IP/MAC binding.



The following diagram describes attack defense.



The following table lists the WebUI menu items, description and a link to the user guide section.

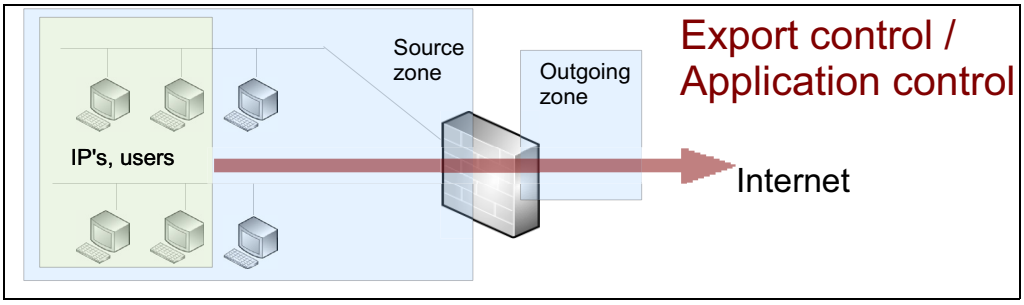
Table 12 Attack Defense Configuration Steps

	WebUI Menu Path	Description	User guide section
1.	**Firewall > IP-MAC binding**	An IP-MAC policy binds an IP address or range to a MAC address.	8.2.1 Configure IP-MAC Binding
2.	**Firewall > Attack defense**	Zone-level detection and defense mechanisms on FGX to defend against common network attacks.	9 Attack Defense

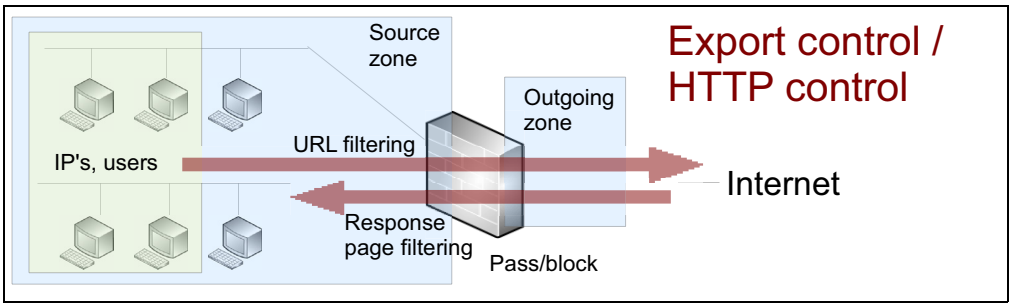
2.9. Unified threat management (UTM)

FGX provides extensive Unified Threat Management (UTM) functionality, including:

- Export control. Consists of
  - 2.9.1. Application control. Controls the application traffic from specified IP's and users from the source zone to the outgoing zone.

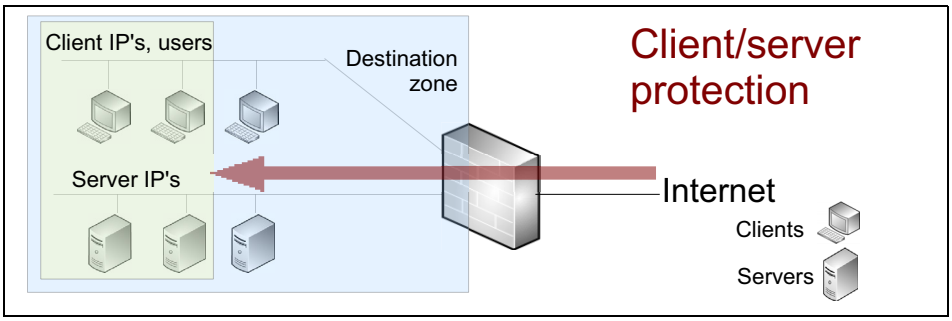


  - 2.9.2. HTTP control. Controls URL requests from specified IP's and users from the source zone to the outgoing zone. Also filters the responses.



  - 2.9.3. DNS control.

- 2.9.4. Client protection, 2.9.5. Server protection. Controls the traffic to specified clients or servers in the destination zone.

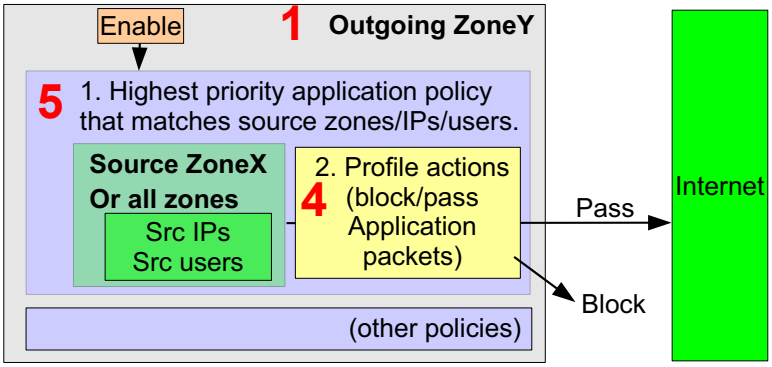


2.9.1. Application control

2.9.1.1 Packet processing

UTM export control / application packet processing steps are shown in the diagram below (black numbers; the red numbers are the configuration steps described in the table below).

1. Determine highest-priority policy that matches the source zone/IPs/users.
2. Perform application control profile (specified in policy) actions.



2.9.1.2 Configuration steps

The following table lists the WebUI menu items for application control (in the order required for configuration), a short description and a link to the relevant user guide section.

Table 13 Application Control Configuration Steps

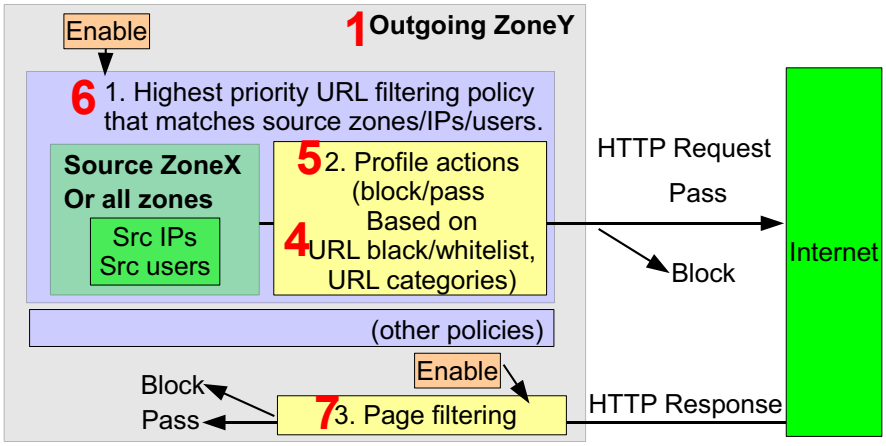
Step	WebUI Menu Path	Description	User guide section
1.	**Network > Zones**	Create zones.	10.2.1.1. Create zones, access policies, default route, NAT rules
2.	**UTM > Export Control > Application Control > Update**	Update application list.	10.2.1.2.1. Update application list
3.	**UTM > Export Control > Application Control > Application List, Custom Applications**	Customize applications.	10.2.1.2.2. Create custom applications
4.	**UTM > Export Control > Application Control > Profiles**	Create required profiles (specifies applications to control and action (including default).	10.2.1.2.3. Create application control profiles
5.	**UTM > Export Control > Policies > Application Control**	For each Zone out: • Create required application policies and • turn on Application control.	10.2.1.2.4. Create application control policies

2.9.2. HTTP control

2.9.2.1 Packet processing

UTM export control / HTTP packet processing steps are shown in the diagram below (black numbers; the red numbers are the configuration steps described in the table below):

1. Determine highest-priority policy that matches the source zone/IPs/users.
2. Perform URL filtering profile (specified in policy) actions.
3. Perform page filtering.



2.9.2.2 Configuration steps

The following table lists the WebUI menu items for URL and HTTP response page filtering (in the order required for configuration), a short description and a link to the relevant user guide section.

Table 14 URL and Response Page Filtering Configuration Steps

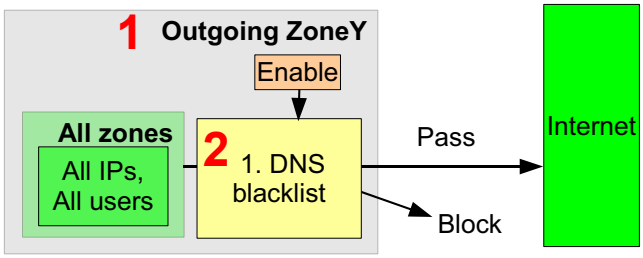
Step	WebUI Menu Path	Description	User guide section
1.	**Network > Zones**	Create zones.	10.2.1.1. Create zones, access policies, default route, NAT rules
2.	**UTM > Export Control > URL Filtering > Update**	Update URL filtering rules.	10.2.1.3.1. Update URL filtering rule base
3.	**UTM > Export Control > URL Filtering > General Settings**	Configure general action for URL filtering engine.	10.2.1.3.2. Configure URL filtering general settings
4.	**UTM > Export Control > URL Filtering > Blacklists and Whitelists**	Configure URL black/whitelist.	10.2.1.3.3. Create URL filtering profiles: Black/white lists
5.	**UTM > Export Control > URL Filtering > Profiles**	Profile specifies blacklist & whitelist, URL filter categories, specific category actions and unknown category default actions.	10.2.1.3.4. Create URL filtering profiles
6.	**UTM > Export Control > Policies > URL Filtering**	For each Zone out: • Create required URL filter policies and • turn on URL filtering.	10.2.1.3.5. Create URL filtering policies
7.	**UTM > Export Control > Page Filtering** and **Policies > Page Filtering**	Configure page filtering for all zone OUTs, but you need to enable it for each outgoing zone.	10.2.1.4. Configure (HTTP response) page filtering

2.9.3. DNS control

2.9.3.1 Packet processing

UTM export control / DNS packet processing steps are shown in the diagram below (black numbers; the red numbers are the configuration steps described in the table below):

1. Block blacklisted DNS requests.



2.9.3.2 Configuration steps

The following table lists the WebUI menu items for DNS domain blacklist (in the order required for configuration), a short description and a link to the relevant user guide section.

Table 15 DNS Domain Blacklist Configuration Steps

Step	WebUI Menu Path	Description	User guide section
1.	**Network > Zones**	Create zones.	10.2.1.1. Create zones, access policies, default route, NAT rules
2.	**UTM > Export Control > DNS Domain Blacklist** and **UTM > Export Control > Policies > DNS Domain Blacklist**	For all zone OUTs, but you need to enable DNS domain blacklist for each outgoing zone.	10.2.1.5. Configure DNS domain blacklist

2.9.4. Client protection

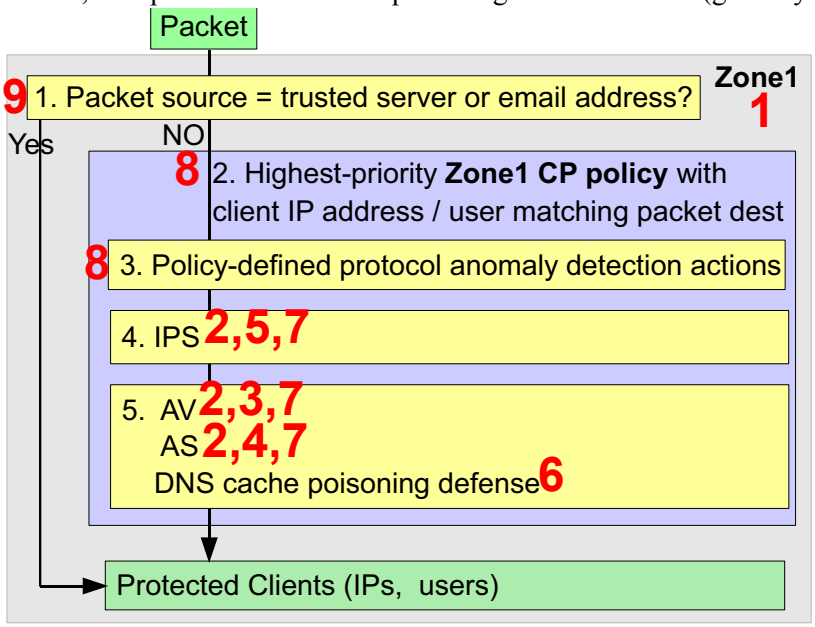
This section describes client protection:

- 2.9.4.1 Packet processing
- 2.9.4.2 Configuration steps

2.9.4.1 Packet processing

Client protection packet processing steps are shown in the diagram below (black numbers; the red numbers are the configuration steps described in 2.9.4.2 Configuration steps):

1. If from a trusted server or email address (zone-defined): Pass.
2. Determine highest-priority policy that matches packet client IP address and/or user for the destination zone.
3. Perform protocol anomaly detection actions (policy-defined).
4. Perform IPS (globally defined, including protocol restriction and attack signature detection).
5. Perform anti-virus (globally defined) and anti-spam (globally defined). For DNS protocol traffic, also perform DNS cache poisoning defense actions (globally defined).



2.9.4.2 Configuration steps

The following table lists 1. The configuration step number in the above diagram. 2. The WebUI menu path. 3. A short description. 4. A link to the relevant user guide section.

Table 16 Client Protection Configuration Steps

Step	WebUI Menu Path	Description	User guide section
1.	**Network > Zones**	Create the CP zone.	10.2.2.1. Create zones, access policies, default route, NAT rules
2.	**UTM > Anti-Virus/Anti-Spam/IPS > Update**	AV, AS, IPS update	10.2.2.2. Update AV, AS, IPS rules
3.	**UTM > Anti-Virus > General Settings, Trusted URLs / Web Servers / Clients**	Global AV actions (scanning, trickling, trusted).	10.2.2.3. Configure global AV actions (trusted list, action when virus detected, heuristic, scan limits)
4.	**UTM > Anti-Spam > General Settings, Allow/Block List, Spam Word List**	Global AS actions (scan, allow/block list, word list).	10.2.2.4. Configure global AS actions (allow/block list, spam word list, scan)
5.	**UTM > IPS > Protocol Restriction**	IPS SMTP, POP3, IMAP, DNS protocol restriction.	10.2.2.5. Configure IPS client SMTP, POP3, IMAP, DNS protocol restriction
6.	**UTM > Client Protection > DNS Cache Poisoning Defense**	For all zones: Configure DNS cache poisoning defense (must be enabled in zone).	10.2.2.6. Configure DNS CPD global actions
7.	**UTM > Anti-Virus, Anti-Spam, IPS > Profiles**	For all zones: Create IPS, anti-virus and anti-spam profiles.	10.2.2.7. Create AV, AS, IPS action profiles
8.	**UTM > Client Protection > Policies**	For selected zone: Create CP policies that define 1. Protected clients 2. AV/AS/IPS profiles 3. Policy-specific actions.	10.2.2.8. Create client protection policies
9.	**UTM > Client Protection > Trusted Server List, Trusted Mail Address List**	For selected zone: Create list of trusted servers and mail addresses.	10.2.2.9. Create trusted server / email list

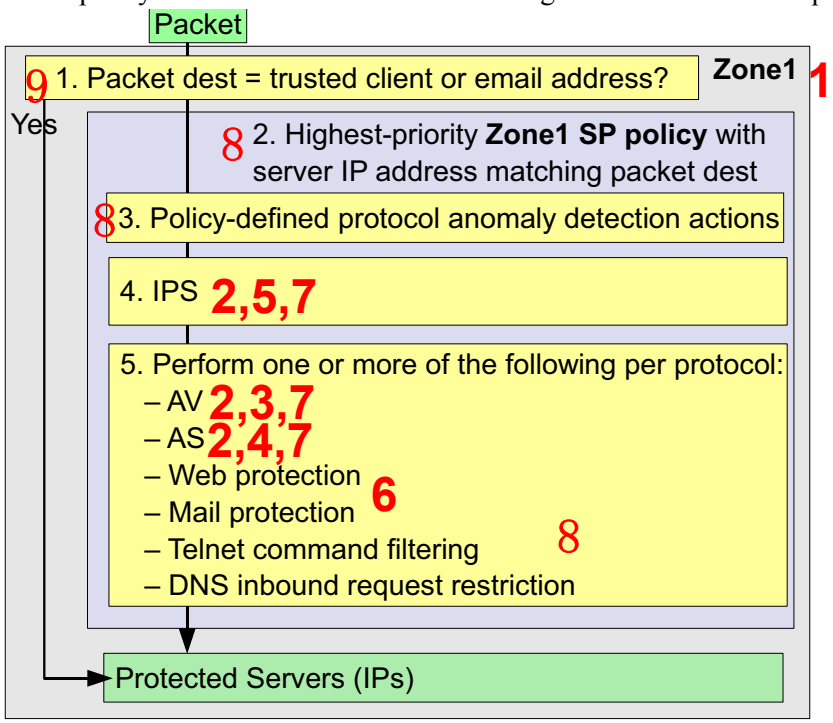
2.9.5. Server protection

- 2.9.5.1 Packet processing
- 2.9.5.2 Configuration steps

2.9.5.1 Packet processing

UTM server protection packet processing steps are shown in the diagram below (black numbers; the red numbers are the configuration steps described on the next page):

1. If from a trusted client or email address (zone-defined): Pass.
2. Determine highest-priority policy that matches packet server IP address for the destination zone.
3. Perform protocol anomaly detection actions (policy-defined).
4. Perform IPS (globally defined, including protocol restriction and attack signature detection).
5. Perform according to the protocol:
   - globally defined anti-virus, anti-spam, and web / mail protection actions, and
   - policy-defined Telnet command filtering and DNS inbound request restriction.



2.9.5.2 Configuration steps

The following table lists 1. The configuration step number in the above diagram. 2. The WebUI menu path. 3. A short description. 4. A link to the relevant user guide section.

Table 17 Server Protection Configuration Steps

Step	WebUI Menu Path	Description	User guide section
1.	**Network > Zones**	Create the SP zone.	10.2.3.1. Create zones, access policies, default route, NAT rules
2.	**UTM > Anti-Virus/Anti-Spam/IPS > Update**	AV, AS, IPS update.	10.2.3.2. Update AV, AS, IPS rules
3.	**UTM > Anti-Virus > General Settings, Trusted URLs / Web Servers / Clients**	Global AV actions (scanning, trickling, trusted).	10.2.3.3. Configure global AV actions (trusted list, action when virus detected, heuristic, scan limits)
4.	**UTM > Anti-Spam > General Settings, Allow/Block List, Spam Word List**	Global AS actions (scan, trusted, word list).	10.2.3.4. Configure global AS actions (allow/block list, spam word list, scan failures)
5.	**UTM > IPS > Protocol Restriction**	IPS HTTP, SMTP, POP3, IMAP, DNS protocol restriction.	10.2.3.5. Configure IPS server HTTP, SMTP, POP3, IMAP, DNS protocol restriction
6.	**UTM > Server Protection > Web/Mail Protection**	For all zones: Configure web and mail server protection (must be enabled in zone).	10.2.3.6. Configure web/mail protection global actions
7.	**UTM > Anti-Virus, Anti-Spam, IPS > Profiles**	For all zones: Create IPS, anti-virus and anti-spam profiles.	10.2.3.7. Create AV, AS, IPS action profiles
8.	**UTM > Server Protection > Policies**	For selected zone: Create SP policies that define 1. Protected servers 2. AV/AS/IPS profiles 3. Policy-specific actions.	10.2.3.8. Create server protection policies
9.	**UTM > Server Protection > Trusted Client List, Trusted Mail Address List**	For selected zone: Create list of trusted clients and mail addresses.	10.2.3.9. Create trusted client / mail address list

2.10. Virtual private networks (VPN)

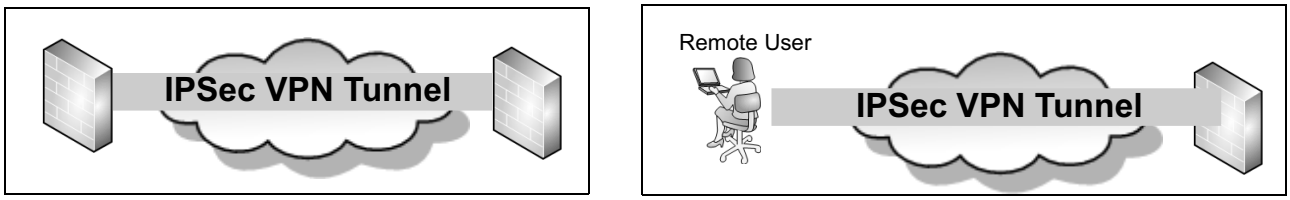
FGX provides high-performance VPN functionality, including:

- 2.10.1. IPSec VPN
- 2.10.2. SSL VPN Web Portal
- 2.10.3. SSL VPN Tunnel

2.10.1. IPSec VPN

The following figure shows basic IPSec site-to-site and remote access VPN scenarios.

Figure 2 Site-to-Site, Remote Access (dialup) VPN



The following table lists the WebUI menu items, a description and a link to the configuration steps.

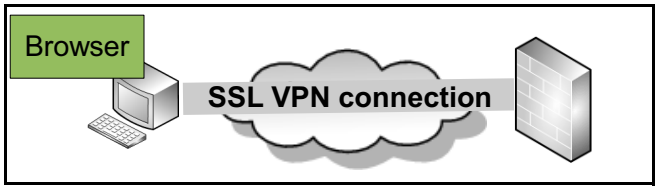
Table 18 IPSec VPN Configuration Steps

	WebUI Menu Path	Description	User guide section
1.		Configure the interfaces, default route, default access policy.	3.1. Configure I/F IP Addresses, Default Policy
2.	**System > Certificates > Local Certificates, CA Certificates**	Import certificates or set pre-shared key	3.4.1. Create Tunnel Using Pre-Shared Key for Authentication/3.4.2. Create Tunnel Using Certificate for Authentication
3.	**System > Authentication > Users (Auto IKE)**	Create IPSec VPN users/user group	3.3. Create IPSec VPN User
4.	**VPN > IPSec VPN > AutoIKE or Manual Tunnels**	Create auto IKE or manual tunnel.	1.2. Create Manual Tunnel (Authentication/ Encryption)/2.2. Create Auto IKE tunnel
5.	**Network > Routing > Default Route** OR **Firewall > Access Policies**	Create default route OR access policy that specifies the tunnel.	1.3. Route Tunnel
6.		Configure remote peer (dialup only).	3.2. Configure Remote PC client

2.10.2. SSL VPN Web Portal

The following figure shows a basic SSL VPN web portal scenario.

Figure 3 Basic SSL VPN Web Portal Scenario



The following table lists the WebUI menu items for SSL VPN web portals (in the order required for configuration), a short description and a link to the user guide description of the basic configuration steps.

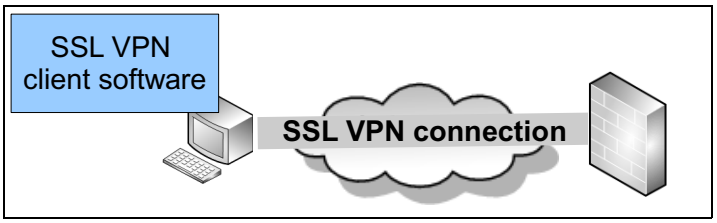
Table 19 SSL VPN Portal Configuration Steps

	WebUI Menu Path	Description	User guide section
1.		Configure interface IP addresses.	4.1. Configure IP Addresses for Interfaces
2.	**System > Authentication > Users, User Groups**	Create SSL VPN users and user groups	4.2. Create an IP Address Pool, VPN User, Group
3.	**System > Certificates > Local Certificates, CA Certificates**	Import CA and local certificates	4.4. Import CA/Local Certificates
4.	**VPN > SSL VPN Web Portal > Applications, Portal Templates**	Applications Include HTTP and HTTPs. Portal templates define portal page, including content, layout, and style.	4.3. Create SSL VPN Applications, Template
5.	**VPN > SSL VPN Web Portal > Portal Services**	Enable HTTPS services provided at specified IP addresses and ports for user groups.	4.5. Create SSL VPN Services

2.10.3. SSL VPN Tunnel

The following figure shows a basic SSL VPN tunnel scenario.

Figure 4 Basic SSL VPN Tunnel Scenario



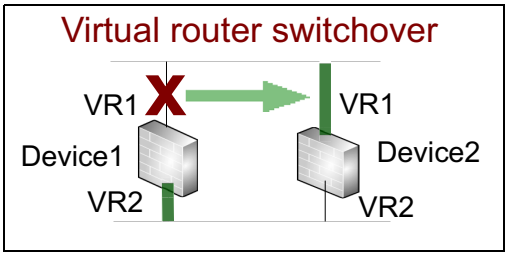
The following table lists the WebUI menu items for SSL VPN tunnels (in the order required for configuration), a short description and a link to the user guide description of the basic configuration steps.

Table 20 SSL VPN Tunnel Configuration Steps

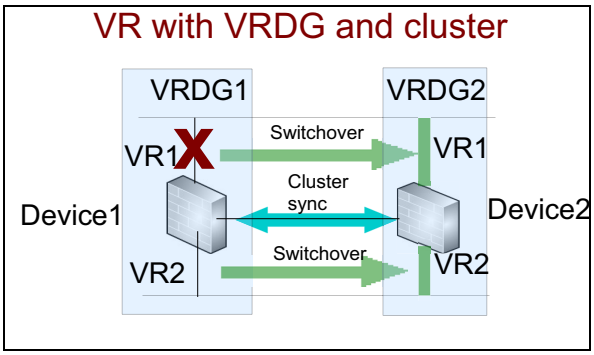
	WebUI Menu Path	Description	User guide section
1.		Configure interface IP addresses.	5.1. Configure IP Addresses for Interfaces
2.	**System > Authentication > Users, User Groups**	Create SSL VPN users and user groups	5.3. Create IP Address Pool, VPN User, Group
3.	**VPN > SSL VPN Tunnels > Tunnels**	Establish an SSL VPN tunnel between servers and clients.	5.4. Create an SSL VPN Tunnel
4.		Install SSL VPN client software.	5.2. Remote PC: Install Client Software / Add Client Connection

2.11. High availability (HA)

The following diagram illustrates HA virtual router switchover concepts. Device1 VR1 (virtual router) fails and a switchover to Device2 VR1 occurs. A switchover for VR2 does not occur.



The following diagram illustrates HA VR switchover with VDRG and cluster synchronization concepts. Device1 VR1 fails, VRDG1 adjusts VR2 priority so that a switchover of both VR1 and VR2 occurs. Device1/Device2 settings are synchronized, allowing a seamless switchover,



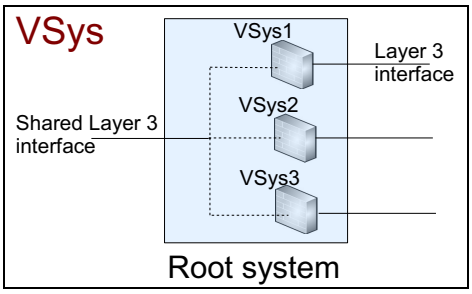
The following table lists the WebUI menu items for high availability (in the order required for configuration), a short description and a link to the user guide description of the basic configuration steps.

Table 21 HA Configuration Steps

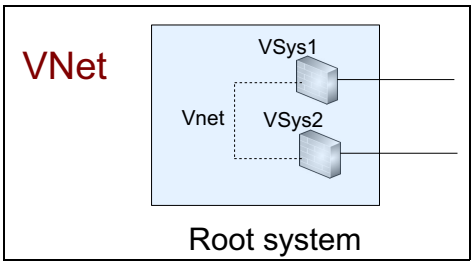
	WebUI Menu Path	Description	User guide section
1.	**System > High Availability > Virtual Routers**	Uses VRRP to achieve backup and redundancy. A virtual router works as a default gateway representing a group of physical routers. One physical router is selected as the master, and the others act as backup.	12.2.1.1. Device1: Configure VR
2.	**System > High Availability > Virtual Router Detection Groups**	Enhanced FGX feature. A detection group binds multiple virtual routers together to achieve entire-unit switchover.	12.2.2.2. Device1: Configure VRDG
3.	**System > High Availability > Clusters**	A cluster is composed of devices sharing the same configurations. Any configuration change of a member device should be synchronized to the others in the cluster. FGX supports synchronization of configurations, runtime information, and system time for clustered devices.	12.2.2.3. Device1: Configure cluster

2.12. Virtual systems/networks (Vsys/Vnet)

The following diagram illustrates Vsys concepts. The device system is the default Vsys 0. You can create other Vsys's each with its own resource limits, interfaces, management IPs, UTM settings, and users/admins.



The following diagram illustrates Vnet concepts.



The following table lists the WebUI menu items for virtual systems and networks (in the order required for configuration), a short description and a link to the user guide description of the basic configuration steps.

Table 22 Vsys Configuration Steps

	WebUI Menu Path	Description	User guide section
1.	**Network > Interfaces**	Create new Layer 3 interfaces, such as VLAN and channel interfaces.	13.2.1. Create Layer 3 Interfaces
2.	**System > Virtual Systems > Virtual Systems**	Create virtual systems. Specify the maximum resource, Layer 3 interfaces, management interface/ IP, and UTM functions.	13.2.2. Create Vsys (resources, interfaces, management IP, UTM)
3.	**System > Authentication > Administrative Users**	Create Vsys admins.	13.2.3. Create Vsys administrators
4.	Enter "https:// +vsys_management_IP" in a browser to login to the Vsys.	Configure Vsys. Each vsys has its own admins, policies, etc.	13.2.4. Logon to /switch Vsys, 13.2.5. Manage Vsys
5.	**System > Virtual Systems > Virtual Networks**	Create virtual networks to connect virtual systems. Allocate virtual interfaces to specified virtual systems.	13.2.6. Create Vnet

2.13. Monitor/Logs

The following table lists the WebUI menu items for monitoring and logs.

Table 23 Monitor/Log Configuration Steps

	WebUI Menu Path	Description	User guide
1.	**Monitor > Topology, Traffic Statistics, Vsys, STP, Route, NAT, ARP, CAM, DHCP IP Address Binding, DHCPv6 Client, DNS Cache, High Availability, System Utilization, Online Users, IPSec VPN Tunnel, Multicast, Alerts/Logs**	Real-time monitoring of all FGX functions.	14 Monitoring

2.14. Reports

The following table lists the WebUI menu items for reports (in the order required for configuration), a short description and a link to the user guide description of the basic configuration steps.

Table 24 Report Configuration Steps

	WebUI Menu Path	Description	User guide section
1.	**Monitor > Reports > General Settings**	Global settings for all reports.	15.2.1 Configure General Settings
2.	**Monitor > Reports > Schedules**	Create a report template.	15.2.2 Create a Report Schedule
3.	**Monitor > Reports > Results**	View generated reports.	15.2.3 Manage Report Results

3 System Configuration

This chapter describes system configuration functions.

- Basic system information
  - 3.1 Home
  - 3.2 System Overview
  - 3.3 Banners
  - 3.4 Asset Summary
  - 3.5 Copyright Information
  - 3.6 System Time
- Licenses and updates
  - 3.7 Licenses
  - 3.8 Update
  - 3.9 Installation Package Management
  - 3.10 Patch Package Management
- Access
  - 3.11 Access Services
  - 3.12 SNMP
- Users and authentication
  - 3.13 Administrative Users
  - 3.14 Users
  - 3.15 User Authentication
  - 3.16 WebAuth Configuration
- Maintenance
  - 3.17 Backup and Restore
  - 3.18 Technical Support
  - 3.19 Centralized Management
  - 3.20 Diagnosis Tools
- Alert and log
  - 3.21 Alert Configuration
  - 3.22 Log Maintenance
- System-wide
  - 3.23 Certificates
  - 3.24 Objects

3.1 Home

The **Home** page shows system information, system resources, interface state, logs, alerts, and so on.

Click the **Home** tab to view detailed system information. You can personalize the **Home** page as needed. Click to refresh the page; Click to close a widget; Click to edit settings such as the refresh time, the refresh method, the number of messages to display, and data display format. When the mouse pointer becomes , you can drag a widget to change the page layout. Click **More** to open the corresponding editing page and configure more settings.

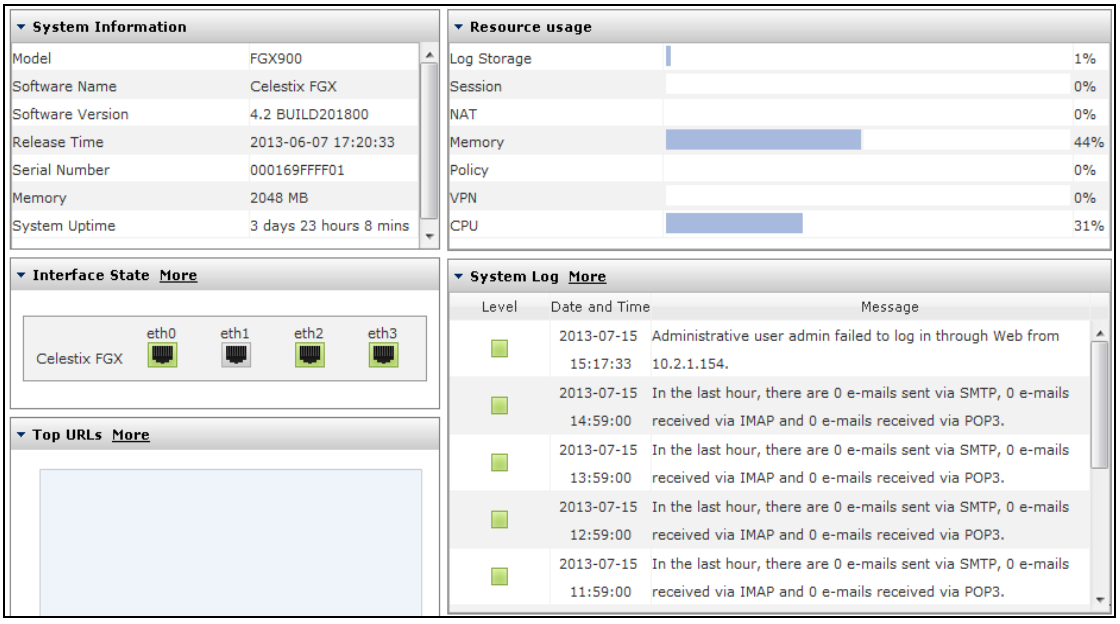


Table 25 Home Page Information

Parameter	Description
System Information	Shows information about product model, software name and version, release time, serial number, memory, and system uptime.
Resource Usage	Shows information about CPU, memory, log storage, sessions, policies, VPN, and NAT resources.
Interface State	Shows the state of system interfaces. The interfaces enabled and connected are shown in green, and those disabled are shown in grey.
System Log	Shows log messages of different security levels. Emergency and Alert are shown in red, Critical and Error are shown in yellow, Warning and Notice are shown in green, and Informational and Debugging are shown in blue.
Anti-Virus Alerts	Shows information about the quarantined files logged by the system after anti-virus scanning, including date and time, file name, file type, detailed log message, and action.
Anti-Spam Alerts	Shows information about the quarantined files logged by the system after anti-spam inspection, including date and time, sender, subject, status, and action.
Top URLs	Shows information about top URLs.
Top Users	Shows information about top users.

Table 25 Home Page Information (*continued*)

Parameter	Description
Top IP Addresses	Shows information about top IP addresses.
Top Applications	Shows information about top applications.
WebAuth Users	Shows information about online WebAuth users, including user, IP address, online time, real-time traffic, total traffic, and idle time.
SSL VPN Users	Shows information about online SSL VPN users, including user, login type, IP address, online time, sent and received bytes, and idle time.

3.2 System Overview

The **Overview** page shows information about system information, access settings, and system maintenance methods.

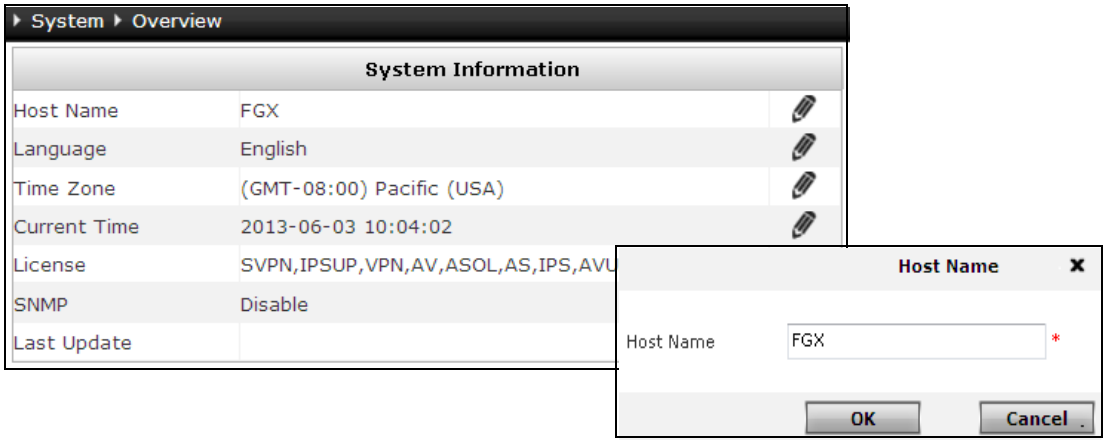
3.2.1 Basic Configuration Steps

3.2.2 Parameters

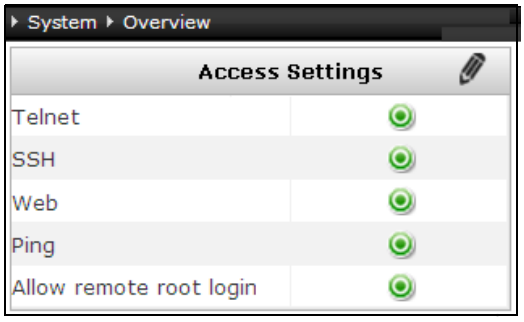
3.2.1 Basic Configuration Steps

Choose **System > Overview**.

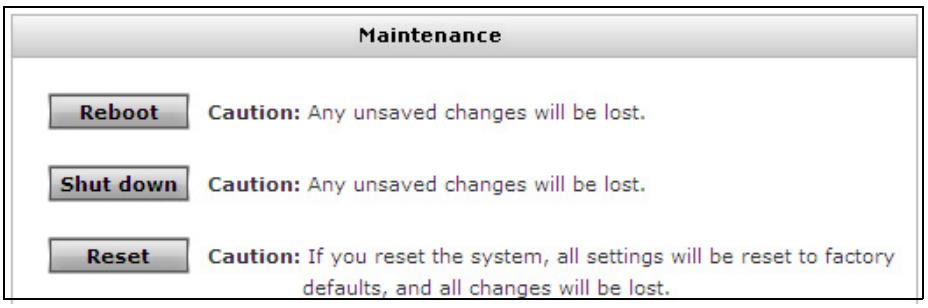
1. Click corresponding to each parameter and edit system information.



2. Click to open the **System** > **Service Configuration** > **Access Settings** page and configure access services. For more information about access services, see 3.11 Access Services.



3. Reboot, shut down, or reset the system in the **Maintenance** section.



Configuration Notes

- To reboot or shut down the system, you need to log in as the root administrator or an administrator. To reset the system, you need to log in as an administrator.
- Unsaved configurations will be lost after rebooting, shutting down, or resetting the system. Make sure that all necessary configurations have been saved before you do any of the operations above.

Table 26 System Information Commands

show system info	Shows system information.
hostname *name*	Changes host name.
language {**Chinese** | **English**}	Sets system language.

Table 27 Restart Commands

reboot	Reboots the system.
halt	Shuts down the system.
reset	Resets the system.

3.2.2 Parameters

Table 28 Parameters of System Information

Parameter	Description
Host Name	System host name. 1-24 UTF-8 characters except spaces and ? , " ' \ < > &, and it cannot start with “-”. The default host name is FGX.
Language	System languages, including Simplified Chinese and English. English by default.
Time Zone	The time zone you can set for the system. (GMT-08:00) Pacific (USA) by default.
Current Time	Shows system time.
License	Shows system license information.
SNMP	Indicates the SNMP state in the system.
Last Update	Shows when the last update was done.

3.3 Banners

3.3.1 Overview

3.3.2 Basic Configuration Steps

3.3.1 Overview

A banner is the identification information you can see when you log on to FGX through the CLI. 1-64 characters.

3.3.2 Basic Configuration Steps

Choose **System > Service Configuration > Banners**. Set Console and Telnet/SSH login banners.

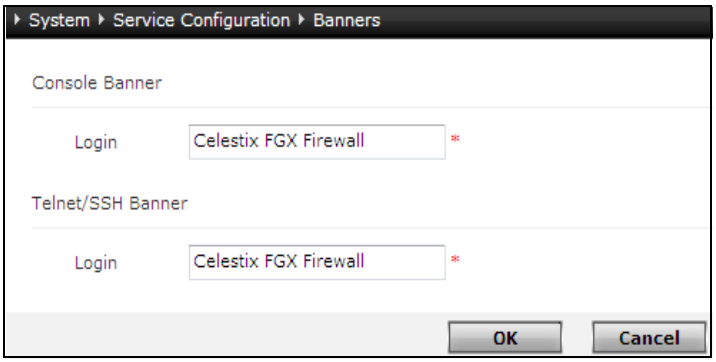


Table 29 Banner Command

banner {**console** | **vty**} *string*	Adds console or Telnet/SSH login banner.

3.4 Asset Summary

Choose **System** > **Asset Information** > **Asset Summary**. View the asset summary information.

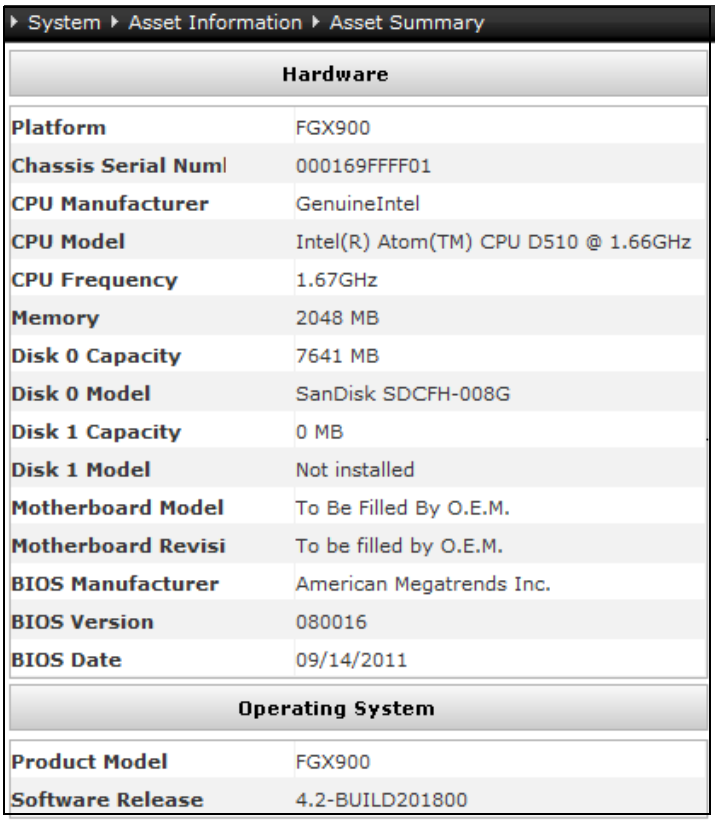


Table 30 Asset Information Command

show assetinfo	Shows asset information.

3.5 Copyright Information

Choose **System** > **Asset Information** > **Copyright Information**. View the copyright information.

3.6 System Time

- 3.6.1 Overview
- 3.6.2 Basic Configuration Steps
- 3.6.3 Parameters

3.6.1 Overview

You can perform the following operations about system time:

- Manual synchronization

  System time ranges from 1970-01-01 00:00:00 through 2037-12-31 23:59:59.

- NTP synchronization

  There are immediate and scheduled automatic NTP synchronizations, and scheduled automatic synchronization is disabled by default. You need to set NTP server addresses for synchronization. FGX supports one primary server and two backup servers, and it always sends synchronization requests to the primary NTP server first.

  FGX supports NTP synchronization authentication, and it is disabled by default. To enable the authentication, you must contact with NTP server administrators beforehand to set key IDs and preshared keys.

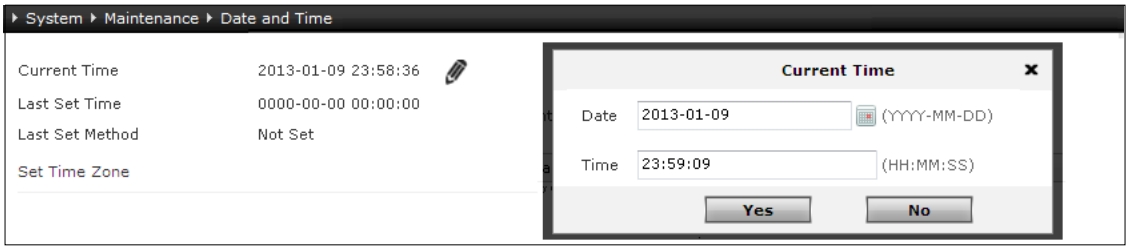
- Time zone configuration

  You can view and configure the time zone where your system clock works and enable or disable daylight saving time (DST) for the time zone you set.

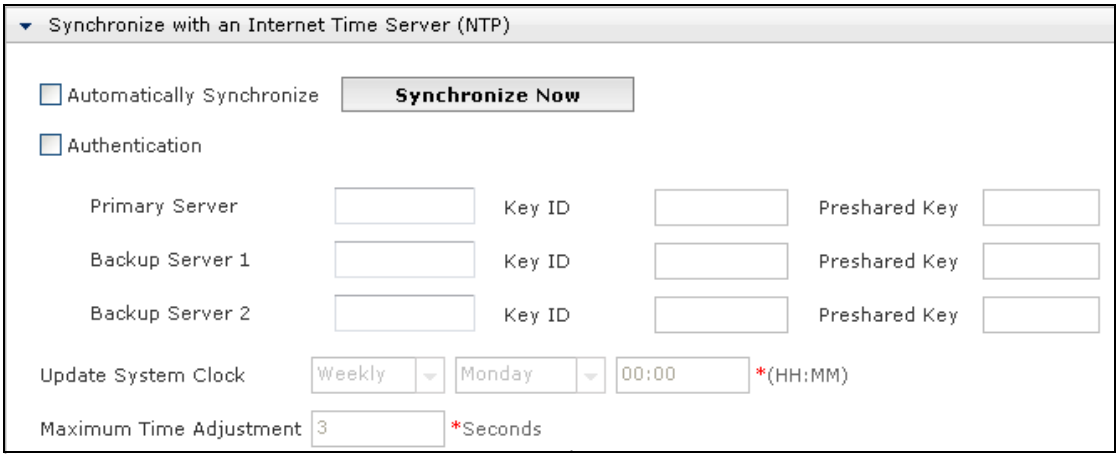
3.6.2 Basic Configuration Steps

Choose **System > Maintenance > Date and Time**.

1. Manual synchronization. Click and synchronize system time in the popup **Current Time** window.



2. NTP synchronization. Enable immediate synchronization or scheduled automatic synchronization. Set NTP servers, update schedule, and maximum time adjustment. Enable synchronization authentication.



3. Time zone configuration. Set a time zone and enable or disable DST.

Configuration Notes

- To set system time, you need to log in as an administrator.
- After modifying the time zone, save the settings and reboot the system for the changes to take effect.

Table 31 System Time Commands

time *date time*	Synchronizes system time manually.
ntp auto-syn {**enable** | **disable**}	Enables or disables scheduled automatic NTP synchronization.
ntp synchronize	Enables or disables immediate NTP synchronization.
ntp authentication {**enable** | **disable**}	Enables or disables synchronization authentication.
ntp server {**server1** | **server2** | **server3**} {*ipv4* | *domain_name*} [**key_id** *id_num* **key** *password*]	Adds NTP servers.
unset ntp server {**server1** | **server2** | **server3**}	Deletes NTP servers.
ntp auto-syn adjust *max_adjustment*	Sets maximum time adjustment.
timezone *timezone_id*	Sets time zone.
timezone dst {**on default** | **off**}	Enables or disables DST.

3.6.3 Parameters

Table 32 Parameters of Manual Synchronization

Parameter	Description
Date	The format is YYYY-MM-DD.
Time	The time format is HH:MM:SS. Hour range 0-23. Minute range 0-59. Second range 0-59.

Table 33 Parameters of NTP Synchronization

Parameter	Description
Synchronize with an Internet Time Server (NTP)	To enable NTP synchronization, you need to set IP addresses or domain names for the primary server and backup servers (if necessary): • IP address range [1-223].[0-255].[0-255].[0-255]. • Domain name length 2-255 characters.
Authentication	To enable NTP synchronization authentication, you need to set key IDs and preshared keys for the primary and backup servers (if necessary): • The key ID range is 1-65,535. • The preshared key is a string of 1-32 characters. The key ID and the preshared key must appear in pairs.
Update System Clock	Sets an automatic synchronization period, every day, every week, or every month. An automatic synchronization is done at 00:00 every Monday by default.
Maximum Time Adjustment	The maximum time difference between the system time and the NTP server time. 0-3,600 seconds. 3 seconds by default. • Only when the time difference is less than the maximum time adjustment value will FGX adjust system time based on the NTP server time. • When the maximum time adjustment is 0, FGX synchronizes the system time based on the NTP server whenever there is a time difference.

Table 34 Parameters of Time Zones

Parameter	Description
Time Zone	Shows the time zone where your system clock works. (GMT-08:00) Pacific (USA) by default.
Enable Daylight Saving Time (DST)	Enables or disables the DST function. Disabled by default.

3.7 Licenses

- 3.7.1 Overview
- 3.7.2 Basic Configuration Steps
- 3.7.3 Parameters

3.7.1 Overview

To apply for a license, open the Home tab System Information section to get the device model and serial number.

- Obtaining licenses automatically

  The MAC address and software information of the FGX device will be automatically sent to the online license server for authentication. A license will be returned and uploaded automatically if the authentication succeeds.

- Scheduled license checking

  FGX automatically sends yearly queries to the online license server to check license status. If the license is invalid or FGX fails to query the license server within one year, the license will be deleted and the functions defined by the license will be disabled.

- Configuring licenses

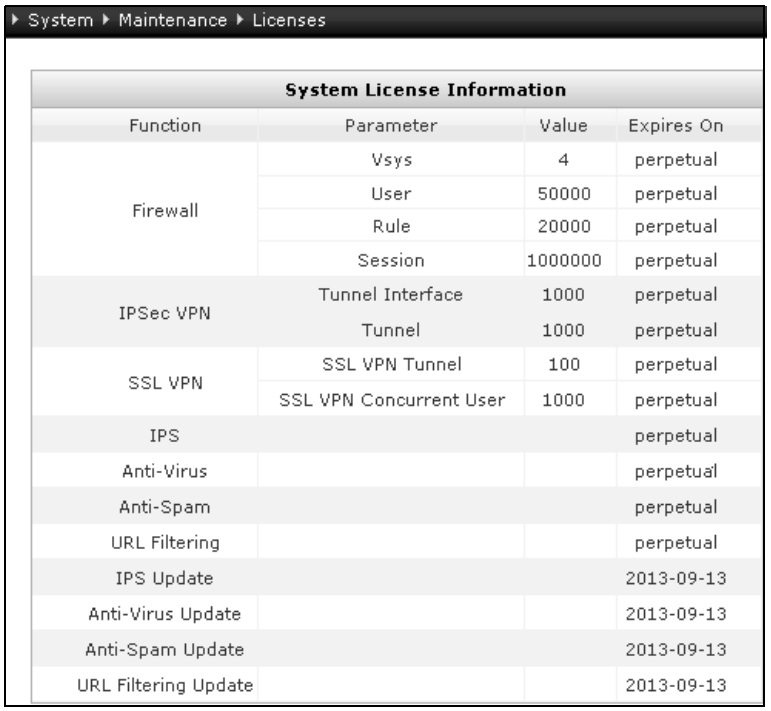
  To import licenses of other functions, you need to import the FW license first. You can import a maximum of 20 licenses. When two licenses limit the same function(s), the function defined by the new license is valid.

  You can log in as the root administrator or an administrator to download licenses and save them to local hosts or TFTP or SFTP servers for license backup.

3.7.2 Basic Configuration Steps

Choose **System > Maintenance > Licenses**.

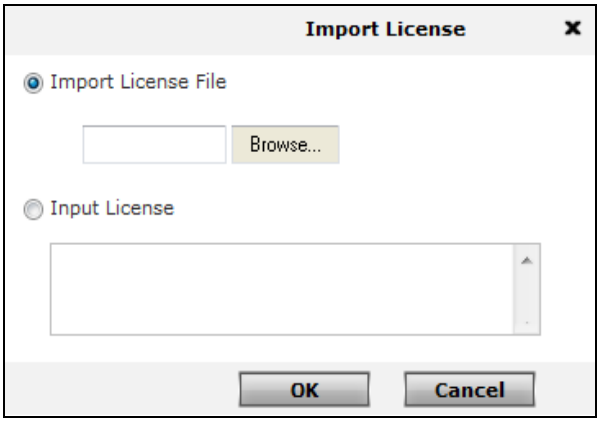
1. View license information.



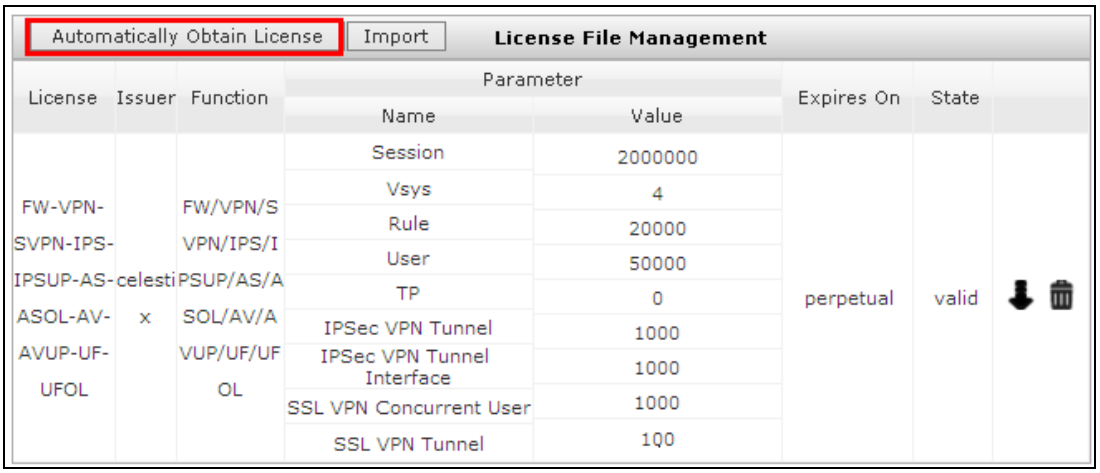
System License Information

Function	Parameter	Value	Expires On
Firewall	Vsys	4	perpetual
	User	50000	perpetual
	Rule	20000	perpetual
	Session	1000000	perpetual
IPSec VPN	Tunnel Interface	1000	perpetual
	Tunnel	1000	perpetual
SSL VPN	SSL VPN Tunnel	100	perpetual
	SSL VPN Concurrent User	1000	perpetual
IPS			perpetual
Anti-Virus			perpetual
Anti-Spam			perpetual
URL Filtering			perpetual
IPS Update			2013-09-13
Anti-Virus Update			2013-09-13
Anti-Spam Update			2013-09-13
URL Filtering Update			2013-09-13

2. Import license files.



3. Delete, download, or automatically obtain licenses.



Configuration Notes

- To configure license files, you need to log in as the root administrator or an administrator.
- When importing a license in the CLI, the license filename cannot contain spaces.
- When importing some licenses, such as FW and VPN licenses, you need to reboot the system for the licenses to take effect.

Table 35 License Commands

show license	Shows license information.
license import from {**x/zmodem** | **tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *password file_name*}	Imports license files.
license word import *string*	Imports license strings.
unset license word *trait_name*	Deletes license files.
license download to {**x/zmodem** *trait_name* | **tftp** *ip_tftp trait_name* | **sftp** *ip_sftp* **username** *user_name* **password** *password file_name*}	Downloads license files.
license automatic activate	Automatically obtains license files.

3.7.3 Parameters

Table 36 Permissions When No Licenses Obtained

Module	Permission
System	• View asset and copyright information • View and set system information, system time, licenses, administrative users, and access services • Modify root and administrator passwords • Use the ping, ping6, and traceroute functions • Reboot, halt, and reset the system
Network	• View neighbor discovery and DHCPv6 configuration • View and configure interfaces, STP, zones, DNS hosts, DNS proxy, DHCP servers, DHCP server subnets, default routing, multicast routing, SNAT, DNAT, MIP, DVMRP, and IGMP Snooping
Firewall	• View and configure access policies, multicast policies, and default policy settings
Monitor	• View monitoring information about topology, interface traffic, STP, routing, NAT, DVMRP neighbor, and IGMP Snooping state

Table 37 FGX License-Controlled Functions

Function	Detail
FW	The maximum number and expiration date of Vsys, users, policies, and sessions.
IPSec VPN	The maximum number and expiration date of IPSec VPN tunnels and tunnel interfaces.
SSL VPN	Maximum number and expiration date of SSL VPN tunnels and concurrent SSL VPN users.
UTM	IPS, anti-virus, anti-spam, and URL filtering and updates of IPS, anti-virus, anti-spam, and URL filtering rules.

3.8 Update

- 3.8.1 Overview
- 3.8.2 Basic Configuration Steps
- 3.8.3 Parameters

3.8.1 Overview

Installation packages and patch packages are used for updates. Installation packages can be used only in manual updates, while patch packages can be used in both manual and automatic updates.

- Manual updates

  In a manual update, you can upload an update package through the WebUI or CLI.

- Automatic updates

  FGX supports immediate and scheduled automatic updates. For a scheduled update, you need to specify an update mode and schedule.

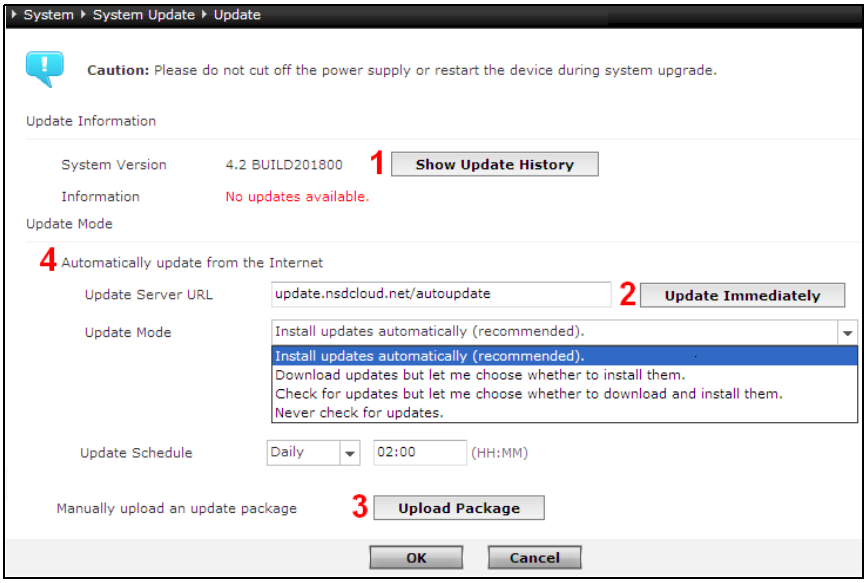
- Update history

  Up to 50 update records are supported.

3.8.2 Basic Configuration Steps

Choose **System > System Update > Update**.

1. Show or export update history.
2. Update now.
3. Update manually using:
   - WebUI using HTTPS.
   - CLI using X/Zmodem (local package) or SFTP/TFTP (another server).
4. Update automatically. Set update server address, update mode, and update schedule.



Configuration Notes

- During system update, the system will prompt you to reboot the system to make changes take effect. Before rebooting the system, make sure that all necessary configurations have been saved.
- When the update server cannot be reached, FGX will attempt to connect to the server three times in automatic updates and only one time in immediate updates. If these attempts all fail, FGX will try when next update starts.
- When there are several patch packages, FGX will download and install them all at a time and prompt you to reboot if required by the patch.

Table 38 Update Commands

show package upgrade config	Shows system update configuration.
package upgrade immediately	Updates the system immediately.
package upgrade from {**x/zmodem** | **tftp** *ip_tftp file_name* | **sftp** *ip_sftp* **username** *user_name* **password** *password file_name* | **internal** *file_name*}	Installs update packages.
package upgrade server {*server_name* | *server_ip*}	Sets update servers.
package upgrade mode {**install update-schedule** {**daily** *time* | **weekly** *weekday* | **monthly** *date*} | {**download** | **check**} **check-schedule** {**daily** *time* | **weekly** *weekday* | **monthly** *date*} | **never**}	Sets update modes.

3.8.3 Parameters

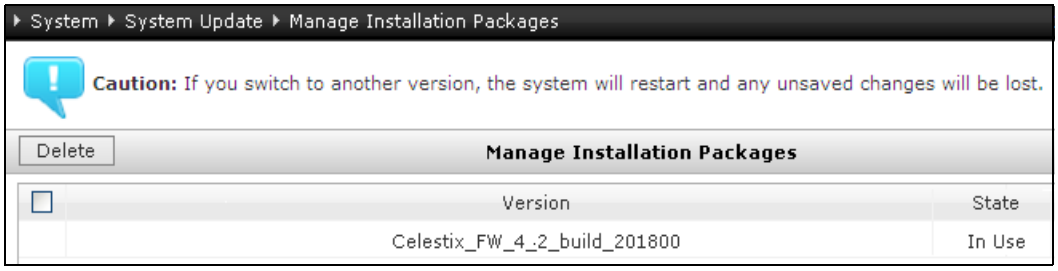
Table 39 Parameters of Updates

Parameter	Description
Update Information	• **System Version—**current update package version. • **Information—**information about available update packages.
Update Mode	Manually or automatically update the system. An automatic update can be done immediately or as scheduled. You need to set: • **Update Server URL—**the default address is update.nsdcloud.net/autoupdate. • **Update Mode—**FGX supports: -Install updates automatically (recommended). -Download updates but let me choose whether to install them. -Check for updates but let me choose whether to download and install them. -Never check for updates. This is the default update mode. • **Update Schedule—**an automatic update can be done every day, every week, or every month, and it is done every day at 2 o'clock by default.

3.9 Installation Package Management

Choose **System > System Update > Manage Installation Packages**.

1. Switch installation packages.
2. Delete installation packages.



Configuration Notes

- Only administrators can switch or delete installation packages.
- After an installation package is installed, the system will be rebooted. Make sure that all necessary configurations have been saved.
- FGX allows only one installation package to be active at a time. An active installation package cannot be deleted.

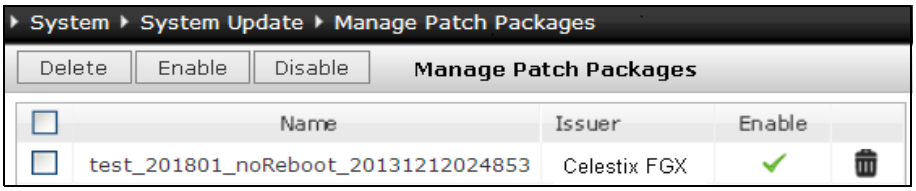
Table 40 Installation Package Commands

system switch *file_name*	Switches system.
delete system *file_name*	Deletes installation packages.

3.10 Patch Package Management

Choose **System > System Update > Manage Patch Packages**.

1. Enable or disable patch packages.
2. Delete patch packages.



Configuration Notes

- Only the root administrator and administrators can view the patch package information.
- Only administrators can enable, disable, and delete patch packages.
- In a manual update, you can upload only one patch package at a time; while in an automatic update, the update server can upload more than one at a time.
- When patch packages are enabled or deleted, the system may prompt you to reboot the system. Make sure that all necessary configurations have been saved before rebooting the system.
- By disabling an active patch package, you can roll back the system to the previous version. You can keep only one patch package and roll back only once.
- When you delete an active patch package, the system will prompt you to reboot the system. Make sure that all necessary configurations have been saved.

Table 41 Patch Package Commands

patch {**enable** | **disable**}	Enables or disables patch packages.
delete patch *file_name*	Deletes patch packages.

3.11 Access Services

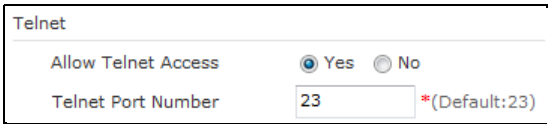
FGX supports access through Telnet, SSH, and Web; the ping function to test the connectivity between remote hosts and FGX; and the remote login of root.

- 3.11.1 Basic Configuration Steps
- 3.11.2 Parameters

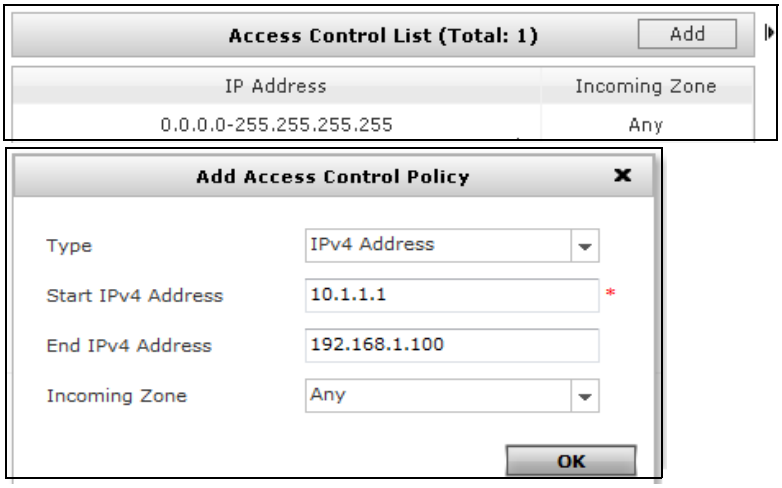
3.11.1 Basic Configuration Steps

Choose **System** > **Service Configuration** > **Access Settings**.

1. Enable access services and set service port numbers.



2. Set access control policies.



3. Allow or block remote login of root.

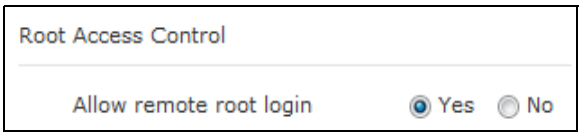


Table 42 Access Service Commands

show service [**telnet** | **web** | **ping** | **ssh**]	Shows access service information.
show root-net-login	Shows remote access control for the root administrator.
service {**telnet** | **web** | **ping** | **ssh**} {**on** | **off**}	Enables or disables access services.
service {**telnet** | **ssh** | **web**} **port** *num*	Sets access service port number.
service {**telnet** | **web** | **ping** | **ssh**} **allow** {**mgt-interface** | **zone** {*zone_name* | **any**} } *start_ip* [*end_ip*]	Adds access control policies.
unset service {**telnet** | **web** | **ping** | **ssh**} [**allow** {**mgt-interface** | **zone** {*zone_name* | **any**}} *start_ip* [*end_ip*]]	Deletes access control policies.
service root-net-login {**enable** | **disable**}	Allows or blocks remote login of root.

3.11.2 Parameters

Table 43 Parameters of Access Services

Parameter	Description
Allow Access	Shows the state of an access service. By default, Telnet is disabled, and SSH, Ping, and Web are enabled.
Port Number	The port number range is 1-65535 for Telnet, SSH, and Web. The default port numbers for Telnet, SSH, and Web are 23, 22, and 443.
Access Control List	Contains access control entries. An access control list contains a maximum of 32 entries. Each entry consists of an IP address range and an incoming zone. Hosts within the IP address range and the zone can access FGX through corresponding access service. • For Web, SSH, and Ping, the default IP address range is 0.0.0.0-255.255.255.255, and the default incoming zone is Any. • When the access control list is empty, no host can access FGX through any service even when the service is enabled.
Root Access Control	Allows or blocks the remote login of the root administrator. It is allowed by default.

3.12 SNMP

- 3.12.1 Overview
- 3.12.2 Basic Configuration Steps
- 3.12.3 Parameters

3.12.1 Overview

FGX supports SNMP. As an agent, it can be accessed by a manager, and it allows the manger to view system status information.

- Supported SNMP versions

  FGX supports SNMP v1, v2, and v3.

- SNMP users

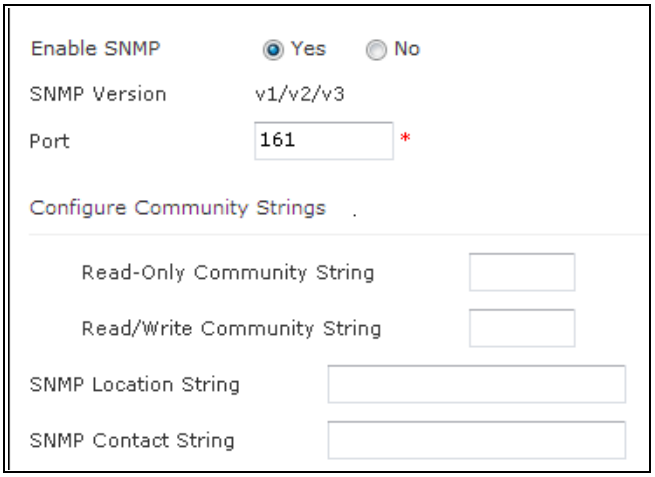
  In SNMP v3, authentication is done according to SNMP user information. When FGX works as an SNMP agent and is accessed by the NMS, it performs an authentication according to the SNMP user information saved in the system.

  SNMP users are maintained separately from system users, though they can have the same name.

3.12.2 Basic Configuration Steps

Choose **System > Service Configuration > SNMP Configuration**.

1. View SNMP configuration information; enable or disable SNMP; and set port number and community, location, and contact strings.



2. Set SNMP users.

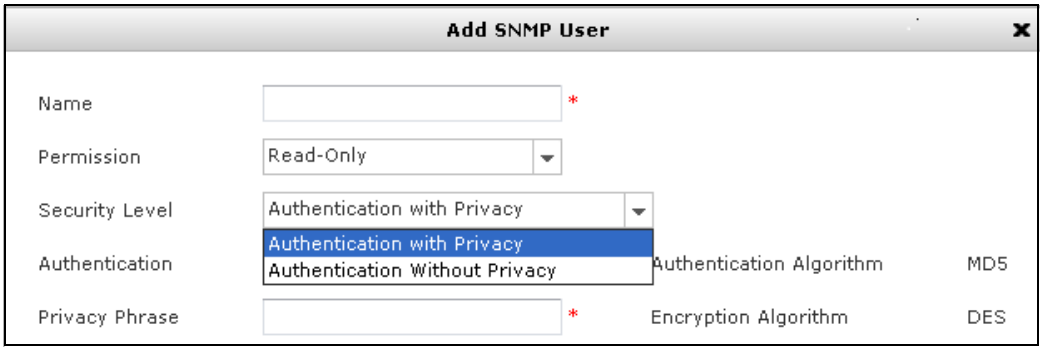


Table 44 SNMP Commands

show snmp {**daemon** | **port** | **community** {**read-only** | **read-write**} | **location** | **contact**}	Shows SNMP configuration information.
snmp daemon {**on** | **off** }	Enables or disables SNMP.
snmp port *port_num*	Sets SNMP port number.
snmp community *string* {**read-only** | **read-write**}	Adds SNMP community strings.
snmp {**location** | **contact**} *string*	Adds SNMP location or contact strings.
unset snmp {**community** {**read-only** | **read-write**} | **location** | **contact**}	Deletes SNMP community, location, or contact strings.
show snmp usm user [*user_name*]	Shows SNMP user information.
snmp usm user *user_name* **seclvl authNoPriv authpro MD5 authpassphrase** *auth_password* {**read-only** | **read-write**}	Adds SNMP users whose security level is Authentication without Privacy.
snmp usm user *user_name* **seclvl authPriv authpro MD5 authpassphrase** *auth_password* **privpro DES privpassphrase** *privacy_password* {**read-only** | **read-write**}	Adds SNMP users whose security level is Authentication with Privacy.
unset snmp usm user [*user_name*]	Deletes SNMP users.

3.12.3 Parameters

Table 45 Parameters of SNMP

Parameter	Description
Enable SNMP	Enables or disables the SNMP function. Disabled by default.
SNMP Version	SNMP v1, SNMP v2, and SNMP v3.
Port	1-65535. 161 by default.
Configure Community Strings	Used for authentication and identification between a manager and an agent. Two types, read-only and read/write. A community string can be basic Latin letters, digits, at signs, underscores, periods, and hyphens. 0-128 characters.
SNMP Location String	The description of the system's location. A location string can be basic Latin letters, digits, at signs, underscores, periods, and hyphens. 0-128 characters.
SNMP Contact String	The contact information of the admin user. A contact string can be basic Latin letters, digits, at signs, underscores, periods, and hyphens. 0-128 characters.

Table 46 Parameters of SNMP Users

Parameter	Description
Name	SNMP user name. 1-63 UTF-8 characters except spaces and * ? , " ' \ < > & #. Up to five SNMP users are supported.
Permission	SNMP user permissions: • **Read-Only—**permission to view system status and configuration. • **Read/Write—**permissions to view system information and modify system configuration, including the community string, location string, and contact string.
Security Level	Security levels of SNMP packets in the network, Authentication with Privacy and Authentication Without Privacy. Authentication with Privacy by default.
Authentication	A character string used for identity authentication. 8-128 ASCII characters except spaces and ? " ' < > &.
Authentication Algorithm	The algorithm used for authentication. MD5 by default.
Privacy Phrase	A character string used for encryption. 8-128 ASCII characters except spaces and ? " ' < > &.
Encryption Algorithm	The algorithm used for encryption. DES by default.

3.13 Administrative Users

- 3.13.1 Overview
- 3.13.2 Basic Configuration Steps
- 3.13.3 Parameters

3.13.1 Overview

- 3.13.1.1 Administrative Users
- 3.13.1.2 Configuration Lock

3.13.1.1 Administrative Users

Administrative users include:

- Root administrator

  It is the initial admin user and cannot be deleted. The default user name and password are "root" and "[Celest1x]."

- Administrators

  Administrators are created and managed by the root administrator. They have read/write permission and can view and configure the system. There is a default administrator "admin," and the initial password is "[Celest1x]."

- Auditors

  Auditors are created and managed by an administrator. They have read-only permission, so they cannot configure the system, but they can view system configuration and modify their own configuration.

- Vsys administrators

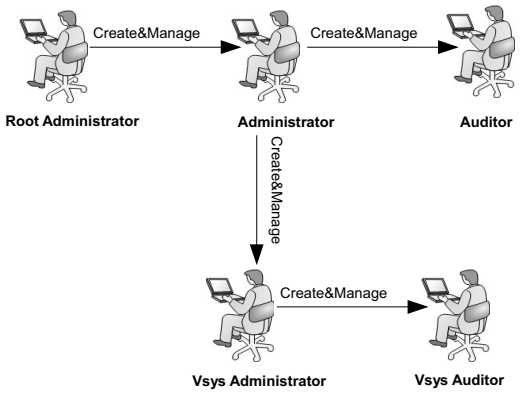
  Vsys administrators are created and managed by an administrator, and they are also assigned Vsys resource by the administrator. They have read/write permission and can configure one or more virtual systems at the same time and view the configuration information.

- Vsys auditors

  Vsys auditors are created and managed by a Vsys administrator, and they are also assigned Vsys resource by the Vsys administrator. Vsys auditors have read-only permission, so they can only view system configuration.

Figure 5 shows the relationships between different administrative roles.

Figure 5 Relationships Between Administrative Roles



3.13.1.2 Configuration Lock

FGX also provides a configuration lock to avoid configuration conflicts between administrative users. It allows only one administrative user to configure the system at a time.

- Configuration Lock in the WebUI

  When you need to configure the system, after you log in, you need to acquire the configuration lock. If you've logged in without the configuration lock, you can see  on the upper right of the WebUI. You can click this icon to acquire the configuration lock. After you successfully get the configuration lock, the administrative user that had the configuration lock now can only view the configuration.

  Click  on the upper right of the WebUI to log off, the configuration lock will be released automatically. If you acquire the configuration lock and then close your browser without logging off, the configuration lock remains effective until the session times out or someone else manually overrides the lock. Therefore, when you complete the configuration, it is recommended to release the configuration lock for others to use it.

  If you log in and do not perform any operations within 30 minutes, the system will automatically disconnect. If you have the configuration lock, your configuration lock will be released automatically.

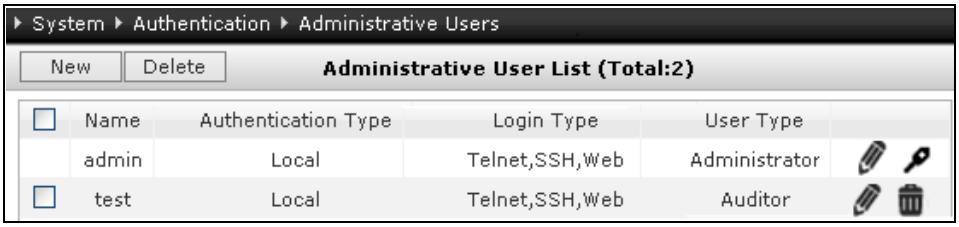
- Configuration Lock in the CLI

  When you log in through the CLI, if the configuration lock has not been acquired by another administrative user, you can use the command **configure mode** to enter the global configuration mode. If it has been acquired by others, you can acquire the lock through the command **configure mode override**. You can release the configuration lock through the command **exit** when you exit the global configuration mode.

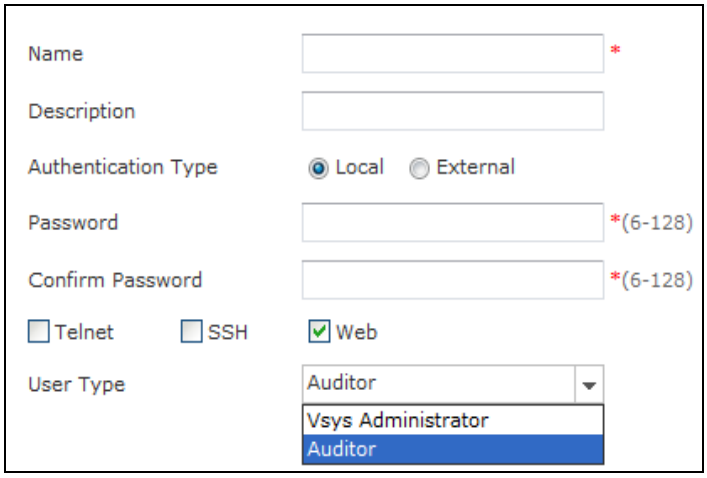
3.13.2 Basic Configuration Steps

Choose **System > Authentication > Administrative Users**.

1. View and delete administrative users and change password.



2. Create and edit administrative users.



Configuration Notes

- Administrative user name must be unique.
- Administrators belong to the root system by default. They can also be added to multiple Vsys, thus obtaining the corresponding permissions of a Vsys administrator.

Table 47 Administrative User Commands

show user administrator	Shows administrative users.
password	Changes administrative user password.
user administrator	Creates administrative users.
unset user administrator	Deletes administrative users.

3.13.3 Parameters

Table 48 Permissions of Different Administrative Roles

Administrative Role	Permission
Root Administrator	• Set administrative users -Create, delete, and edit administrators -Modify root administrator and administrator passwords • Configure the system -Upload, download, and delete licenses -Reboot and shut down the system -Set local authentication for administrative users -Switch languages • View system configuration information
Administrator	• Set administrative users -Create, delete, and edit auditors and Vsys administrators -Modify auditor and Vsys administrator passwords -Assign administrators to Vsys • Configure the system -Switch Vsys -Set system maintenance, network configuration, service configuration, objects, users, authentication, HA, routing, NAT, policies, VPN, attack defense, UTM, and Vsys • View system configuration information
Auditor	• Modify auditor passwords • View system configuration information
Vsys Administrator	• Set administrative users -Create, delete, and edit auditors for the current Vsys -Modify Vsys administrator and Vsys auditor passwords • Configure Vsys -Switch Vsys -Configure the Vsys they reside in • View Vsys configuration information
Vsys Auditor	• Modify Vsys auditor passwords • View Vsys configuration information

Table 49 Parameters of Administrative Users

Parameter	Description
Name	Administrative user name. 1-63 UTF-8 characters except spaces and * ? , " ' \ < > & #.
Description	Description about an administrative user. 0-255 UTF-8 charactersexcept ? " ' \ < > &.
Authentication Type	Administrative user authentication types, local and external. Local by default.
Password	Administrator and Vsys administrator password. 6-128 characters.
Login Type	Administrative user login types, Telnet, SSH, and Web. Web by default.
Vsys List	Vsys a Vsys administrator or a Vsys auditor belongs. One Vsys administrator can belong to multiple Vsys. One Vsys auditor can belong to only one Vsys.

3.14 Users

- 3.14.1 Overview
- 3.14.2 Basic Configuration Steps
- 3.14.3 Parameters

3.14.1 Overview

Users refer to those who need to pass the authentication supported by the system for access to network resources. Users include:

- WebAuth users

  You need to specify an IP address and a port number for the WebAuth server on the system. WebAuth users need to select an access mode and provide a valid user name and password for authentication. A WebAuth user can be authenticated in an active or a passive authentication. For more information about WebAuth authentication, see 3.16 WebAuth Configuration.

- IPSec VPN users

  IPSec VPN users include Xauth users and L2TP users, and they can be authenticated locally or externally. FGX manages IPSec VPN users through remote dialup mechanism. IPSec VPN users must pass authentication before they can connect to the VPN gateway.

- SSL VPN users

  SSL VPN users refer to those who log in through SSL VPN. An SSL VPN user can be assigned to an SSL VPN user group. An SSL VPN user can be authenticated locally or externally.

FGX supports multiple logins for users. A user can log in through a single login or multiple logins.

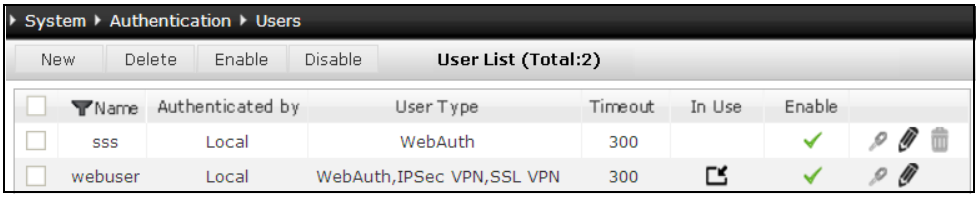
FGX records the online and offline time and traffic of a user, and RADIUS servers are used for user fare accounting. If there is no traffic within the specified timeout, a user will be considered offline. The timeout can be manually set for each user. If no timeout is set for a user, the user will get the default timeout of the Vsys to which it belongs.

FGX also provides users that have not been configured locally with default configuration. You can specify the default configuration (user timeout and type information) by clicking Default configuration for users that have not been configured locally.

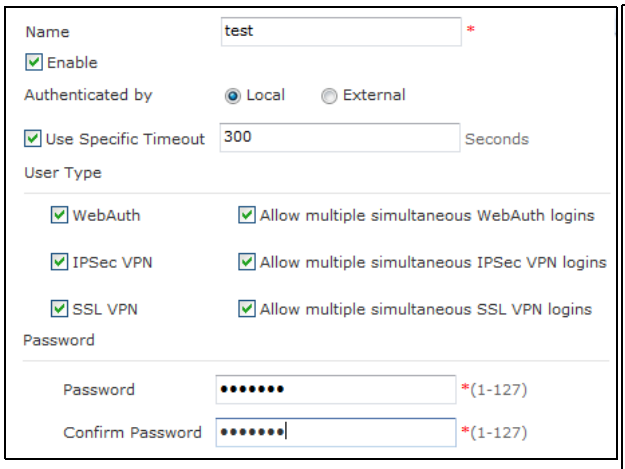
3.14.2 Basic Configuration Steps

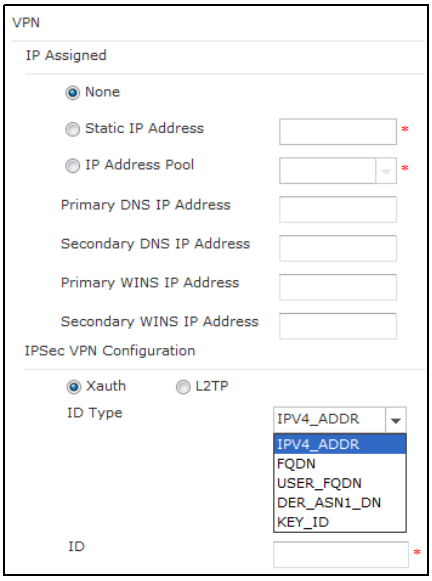
Choose **System > Authentication > Users**.

1. View, delete, enable, and disable users and change user password.



2. Create and edit users.





3. Specify default configuration for users that have not been configured locally.

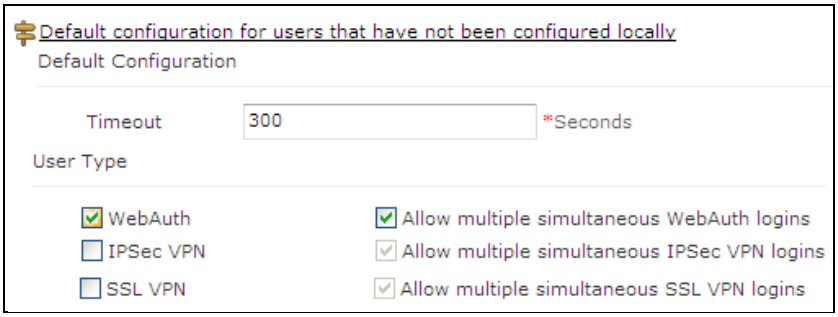


Table 50 User Commands

show user authuser	Shows users.
user authuser enable,disable	Enables or disables users.
user authuser password	Changes user password.
user authuser	Creates users.
unset user authuser	Deletes users.

3.14.3 Parameters

Table 51 Parameters of Users

Parameter	Description
Name	User name. 1-63 UTF-8 characters except spaces and * ? , " ' \ < > & #.
Authenticated By	User authentication types, local and external. Local by default.
User Type	User types, WebAuth, IPSec VPN, and SSL VPN. WebAuth by default.
Timeout	User timeout. 0-3,600 seconds. 300 seconds by default. If the timeout is set to 0, the user will not be considered offline until logging off or being forced offline.
In Use	The list of access policies using a user.
Enable	Enables or disables a user. Only after a user is enabled can the user access network resources through FGX.
Password	Password for a user to pass authentication. 0-127 characters.
IP Assigned	Assigns IP addresses for IPSec VPN and SSL VPN users, including user IP addresses, primary and secondary DNS server addresses, and primary and secondary WINS server addresses. User IP address can be a static IP address or one from an IP address pool.
IPSec VPN Configuration	Required for IPSec VPN users: • **User Type—**Xauth and L2TP. • **ID Type—**IPV4_ADDR, FQDN, USER_FQDN, DER_ASN1_DN, and KEY_ID.

3.15 User Authentication

- 3.15.1 Overview
- 3.15.2 Basic Configuration Steps
- 3.15.3 Parameters

3.15.1 Overview

- 3.15.1.1 Local&External Authentications
- 3.15.1.2 External Authentication Servers

3.15.1.1 Local&External Authentications

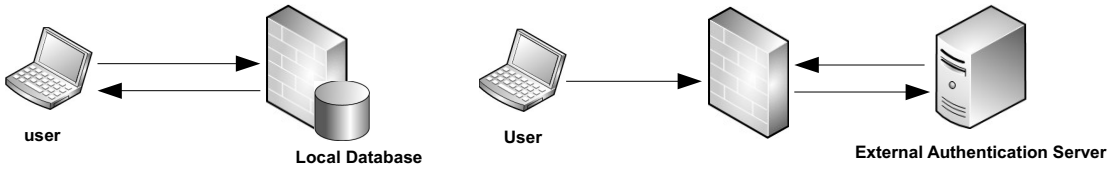
Administrative users and users can be authenticated through either the local database or an external authentication server.

- Local authentication (FGX)
- External authentication (external authentication servers)

  Local authentication has priority over external authentication. For administrative users that are created locally, even the authentication type is external, FGX still performs local authentication on it first, then external authentication.

Figure 6 shows the local and the external authentications.

Figure 6 Local/External Authentication



3.15.1.2 External Authentication Servers

FGX supports the following external authentication servers:

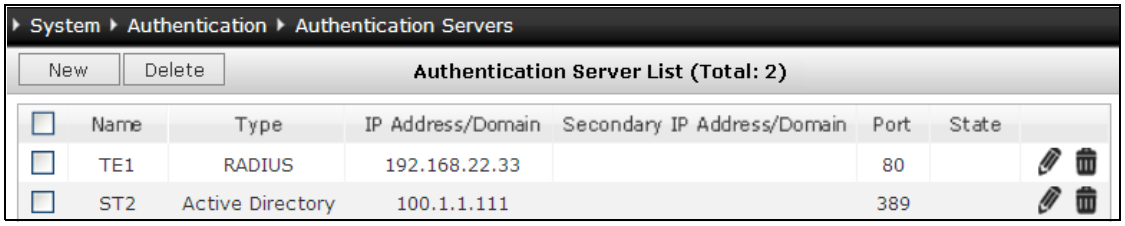
- RADIUS servers (can also be used as an account server for users)
- LDAP servers (based on LDAPv3)
- Active Directory servers (based on LDAPv3)
- eDirectory servers (based on LDAPv3)

FGX supports secondary authentication server. When the primary server cannot be reached or the primary server cannot respond within the default timeout (30 seconds), the secondary authentication server will be used. The primary and secondary servers must have the same port number.

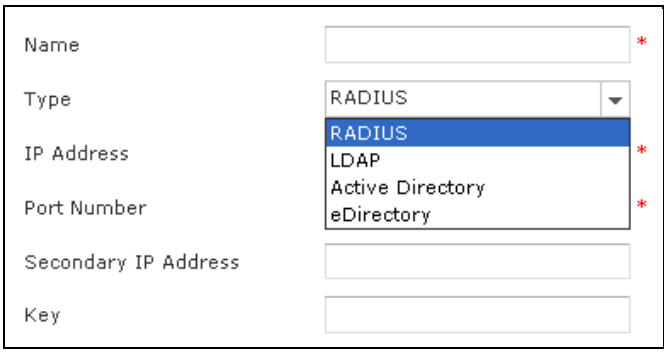
3.15.2 Basic Configuration Steps

Choose **System > Authentication > Authentication Servers**.

1. View and delete authentication servers.



2. Add and edit authentication servers.



Choose **System > Authentication > Authentication Configuration**. Specify authentication and accounting servers for users.

Configuration Notes

- Authentication server name must be unique.
- Up to four external authentication servers are supported.
- An authentication server that is being used cannot be deleted. To delete it, you must specify another external server for authentication first.
- Parameter changes done to an authentication server will not affect the connections that have already authenticated by it.
- The root administrator can configure the authentication server only for administrative users, and the authentication type can only be local.

Table 52 Authentication Configuration Commands

server authentication type administrator	Specifies authentication server for administrative users.

Table 52 Authentication Configuration Commands (*continued*)

server authentication type authuser	Specifies authentication server for users.
server account	Specifies accounting server for users.

Table 53 Authentication Server Commands

show server authentication	Shows authentication servers.
radius server	Adds RADIUS servers.
ldap server	Adds LDAP servers.
active-directory server	Adds Active Directory servers.
edirectory server	Adds eDirectory servers.
unset radius server	Deletes RADIUS servers.

3.15.3 Parameters

Table 54 Parameters of Authentication and Accounting Servers

Server	Description
Authentication Server for Administrators	Administrative users can be authenticated through the local database or an external authentication server. Local by default.
Authentication Server for Users	Users can be authenticated through the local database or an external authentication server. Local by default.
Accounting Server for Users	RADIUS servers can be used for accounting. No accounting server is set by default.

Table 55 Parameters of External Authentication Servers

Parameter	Description
Name	Authentication server name. 1-63 UTF-8 characters except spaces and ? , " ' \ < > & #.
IP Address/ Domain	Authentication server IPv4 address or domain name. FGX sends authentication requests to this IP address or domain name (2-255 characters).
Port Number	Authentication server port number. 1-65535. • **RADIUS—**the default authentication port number is 1812, and the default accounting port number is 1813. • **LDAP, Active Directory, and eDirectory—**when the secure connection type is None or STARTTLS, the default port number is 389; when the secure connection type is SSL/TLS, the default port number is 636.
Secondary IP Address/Domain	Authentication server secondary IPv4 address or domain name (2-255 characters).
Key	The shared key produced by a RADIUS server and FGX and used to verify RADIUS packets. 0-64 characters. Only when their shared key is consistent can the server and FGX receive and respond to the packets sent by each other.
Secure Connection	Encrypts the communication between FGX and authentication servers. FGX supports SSL/TLS and STARTTLS.
Certificate	The CA certificate used for authentication when the secure connection type is SSL/ TLS or STARTTLS.
Common Name Identifier	Used by authentication servers to identify an entry. 0-80 UTF-8 characters except question marks and spaces.
Distinguished Name (DN)	Used by authentication servers before they identify an entry using a common name identifier. 0-511 UTF-8 characters except question marks and spaces.
Admin DN	The DN of an authentication server's administrator. FGX sends it to the authentication server for getting the permission to search. 0-511 UTF-8 characters except question marks and spaces.
Password	The password of an authentication server's administrator. 0-127 characters.
State	Authentication server state. An authentication server being used is shown as In Use.

3.16 WebAuth Configuration

WebAuth authentication controls user access through FGX.

- 3.16.1 Overview
- 3.16.2 Basic Configuration Steps
- 3.16.3 Parameters
- 3.16.4 Example: User Authentication

3.16.1 Overview

WebAuth authentication can be enabled on the following Layer 3 interfaces:

- Ethernet
- Channel
- Redundant
- PPPoE
- VLAN

You can specify WebAuth port number (default is 4325).

WebAuth is invoked if all of the following are satisfied:

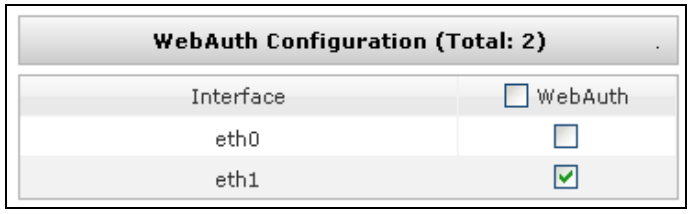
1. User tries to access through an interface that has webAuth enabled.
2. User IP and the destination IP are specified in a WebAuth (automatic redirection) policy.
3. User was not previously authenticated.

The user can only access the destination IP if he is allowed WebAuth access.

3.16.2 Basic Configuration Steps

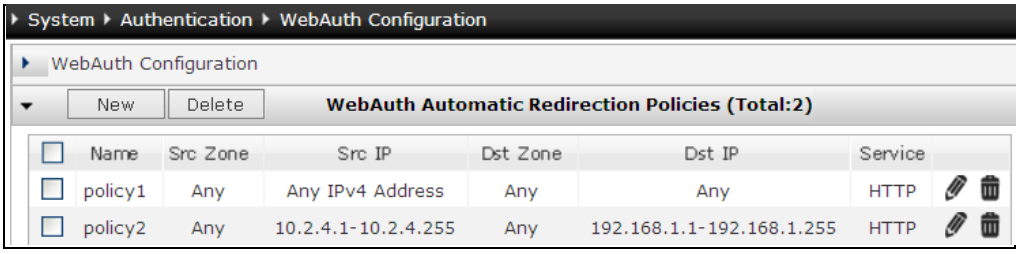
Choose **System > Authentication > WebAuth Authentication**.

1. Enable WebAuth authentication on Layer 3 interfaces.

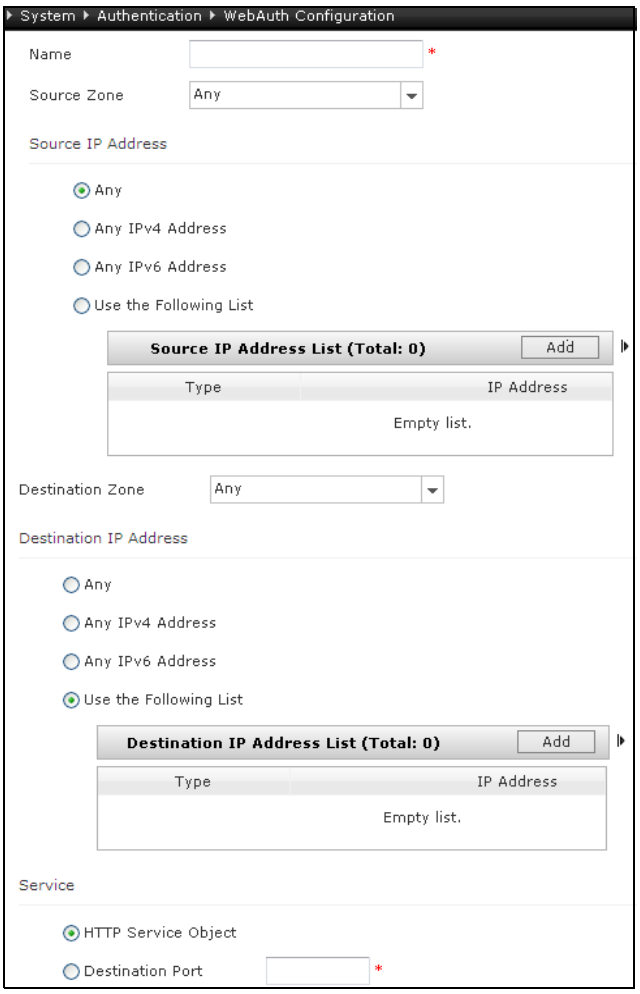


2. Set WebAuth banner and port number.

3. View and delete WebAuth automatic redirection polices.



4. Create and edit WebAuth automatic redirection polices.



Configuration Notes

- Each Vsys supports a maximum of WebAuth automatic redirection policies.
- Each policy supports up to 4,096 source IP address entries and 4,096 destination IP address entries.

Table 56 WebAuth Authentication Commands

webauth banner	Sets WebAuth banner.
webauth auth-port	Sets WebAuth port number.
webauth on,off	Enables or disables WebAuth authentication.
webauth policy	Creates WebAuth automatic redirection policies.
unset webauth policy	Deletes WebAuth automatic redirection policies.

3.16.3 Parameters

.

Table 57 Parameters of WebAuth Automatic Redirection Policies

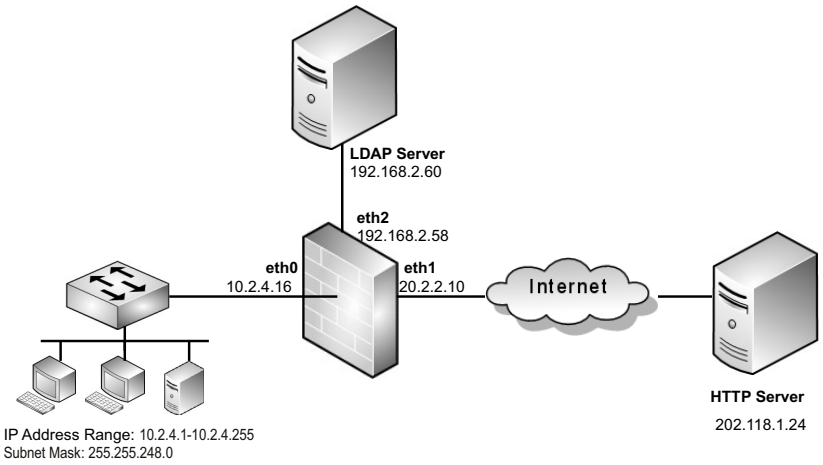
Parameter	Description
Name	Automatic redirection policy name. 1-63 UTF-8 characters except spaces and ? , " ' \ < > & #. Policy names must be unique and they cannot be modified.
Src Zone	The zone from which packets are sent.
Dst Zone	The zone to which packets are sent.
Src IP	The IP address or IP address list (v4 or v6) from which packets are sent.
Dst IP	The IP address or IP address list (v4 or v6) to which packets are sent.
Service	The port number used for passive authentication. It can be an HTTP service object (destination port number: 80) or a destination port (port number: 1-65535).

Table 58 Parameters of WebAuth Configuration

Parameter	Description
WebAuth Banner	Banners displayed to users after WebAuth authentication. 1-220 UTF-8 characters except ? " ' \ < > &.
WebAuth Port Number	The port number for WebAuth authentication. 1-65535. 4325 by default.
Interface	The interface on which WebAuth authentication can be enabled. Can be all Layer 3 interfaces except loopback and tunnel interfaces.
WebAuth	Enables or disables WebAuth authentication on a Layer 3 interface.

3.16.4 Example: User Authentication

In this example, a user named “testuser” needs to pass the authentication through an LDAP server before he can access an HTTP server.



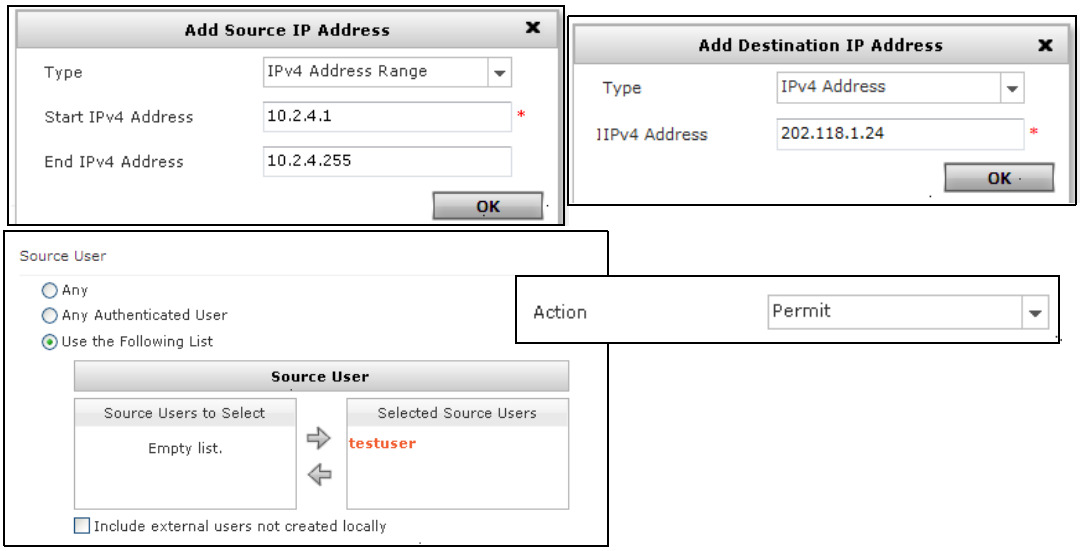
Configuration steps are listed below:

- 3.16.4.1 Configure an LDAP Server
- 3.16.4.2 Set the LDAP Server on FGX
- 3.16.4.3 Specify User Authentication Server
- 3.16.4.4 Enable WebAuth for the Interface
- 3.16.4.5 Enable WebAuth for the User
- 3.16.4.6 Create a WebAuth (Automatic Redirection) Policy

The user then:

- 3.16.4.7 User enters destination IP
- 3.16.4.8 User enters authentication IP

Note: You must have an access policy that allows the user access.



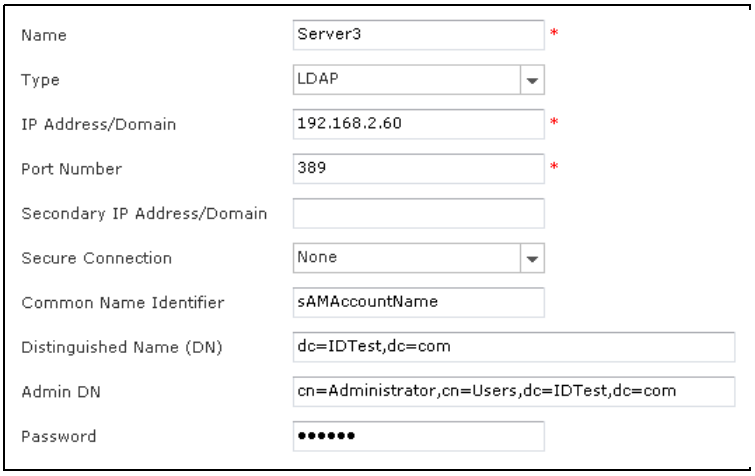
3.16.4.1 Configure an LDAP Server

1. Install the Active Directory service on Windows Server 2003.
2. Add the user information on the Server. User Name: testuser; Password: test.12

3.16.4.2 Set the LDAP Server on FGX

Note: The server configuration should be the same as that of the LDAP server configured above.

1. Choose **System** > **Authentication** > **Authentication Servers**.
2. Click **New** to set the LDAP server. Enter the following LDAP server information:
   Common Name Identifier: sAMAccountName
   Distinguished Name (DN): dc=IDTest,dc=com
   Admin DN: cn=Administrator,cn=Users,dc=IDTest,dc=com
   Password: 123456 (LDAP server administrator password)



3. Click **OK**.

CLI

```
FGX@root> configure mode override
FGX@root-system] ldap server Server3 ip/domain 192.168.2.60 port 389
Secure_Connection none
FGX@root-system] ldap server Server3 Admin_DN
cn=Administrator,cn=Users,dc=IDTest,dc=com
FGX@root-system] ldap server Server3 Common_Name_Identifier
sAMAccountName
FGX@root-system] ldap server Server3 Distinguished_Name
dc=IDTest,dc=com
FGX@root-system] end
FGX@root> save config
```

3.16.4.3 Specify User Authentication Server

1. Choose **System** > **Authentication** > **Authentication Configuration**.
2. Specify the new LDAP server "Server3"as the user authentication server.

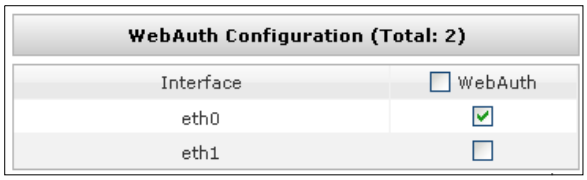
3. Click **OK**.

CLI

```
FGX@root> configure mode override
FGX@root-system] server authentication type authuser Server3
iFGX@root-system] end
FGX@root> save config
```

3.16.4.4 Enable WebAuth for the Interface

1. Choose **System > Authentication > WebAuth Configuration**. Enable WebAuth authentication on eth0.



2. Click OK.

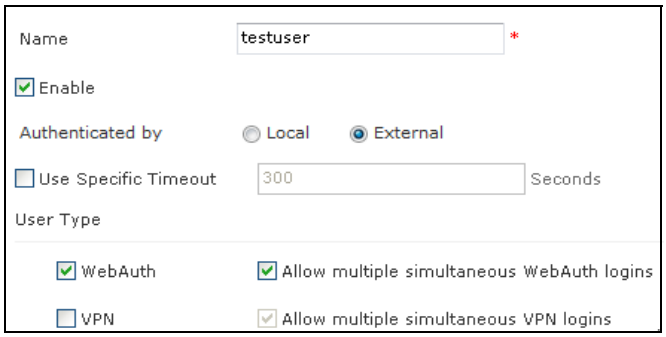
CLI

```
FGX@root> configure mode override
FGX@FGX@root-system] webauth ethernet eth0 on
FGX@root-system] end
FGX@root> save config
```

3.16.4.5 Enable WebAuth for the User

1. Choose **System > Authentication > Users**.
2. Click **New** to create a WebAuth user.

   User name: testuser; Authentication type: External. Check **WebAuth**.



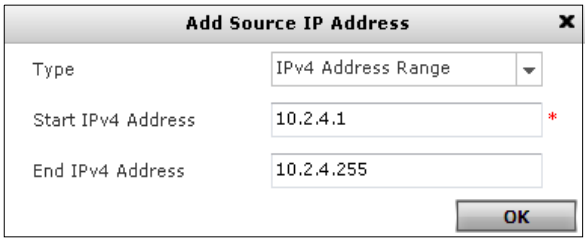
3. Click **OK**.

CLI

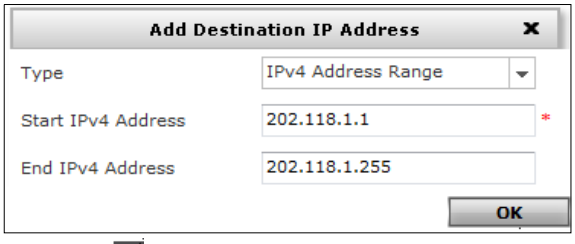
```
FGX@root> configure mode override
FGX@root-system] user authuser testuser authtype external enable
FGX@root-system] user authuser testuser auth
FGX@root-system] user authuser testuser auth multipoint enable
FGX@root-system] end
FGX@root> save config
```

3.16.4.6 Create a WebAuth (Automatic Redirection) Policy

1. In the **WebAuth Automatic Redirection Policies** list, click **New** to create "policy2."
2. In the **Source IP Address** section, set source IP address range as 10.2.4.1-10.2.4.255.



3. In the **Destination IP Address** section, set destination IP address range as 202.118.1.1-202.118.1.255.



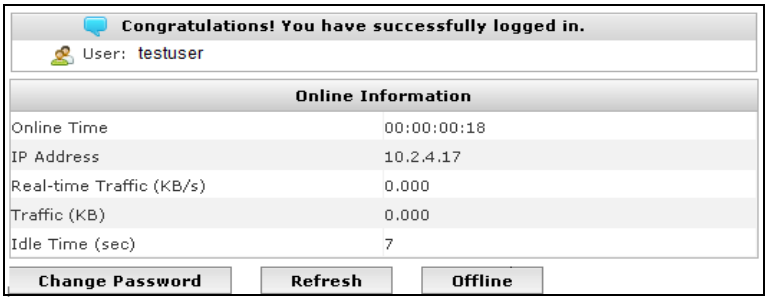
4. Click  .

CLI

```
FGX@root> configure mode override
FGX@root-system] webauth policy policy2 any 10.2.4.1-10.2.4.255 any
202.118.1.1-202.118.1.255 service http
FGX@root-system] end
FGX@root> save config
```

3.16.4.7 User enters destination IP

Normally the user does not know the authentication address https://10.2.4.16:4325. The user enters http://202.118.1.24, and the WebAuth authentication login page appears. The user enters user name and password. The WebAuth banner appears. The user can now access http://202.118.1.24.



3.16.4.8 User enters authentication IP

The user can also directly enter https://10.2.4.16:4325. The WebAuth authentication login page appears. The user enters user name and password. The user enters http://202.118.1.24 to open the destination after the successful authentication.

3.17 Backup and Restore

- 3.17.1 Overview
- 3.17.2 Basic Configuration Steps

3.17.1 Overview

You can back up system configuration files except system logs, diagnostic files, and licenses.

- Backing up the system

  It is recommended to periodically back up system configurations.

- Managing backup files

  You can view, delete, and download backup files. You can copy system backup files to the local storage medium, but this can be done only in the CLI. The backup files of one Vsys cannot be copied to another Vsys.

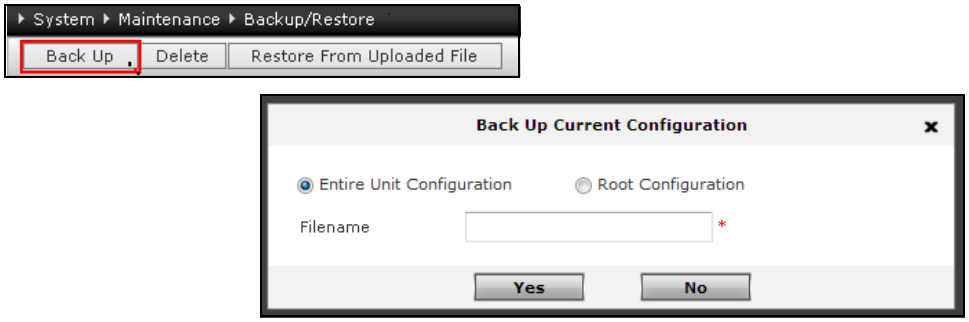
- Restoring the system

  System restoration can be done by using both local and remote backup files. In a remote restoration, the remote backup files will be uploaded to the system. They will be deleted automatically when the restoration is done.

3.17.2 Basic Configuration Steps

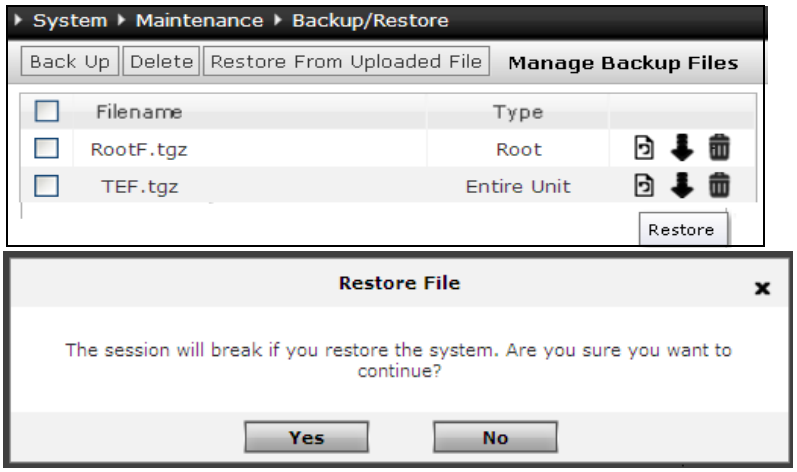
Choose **System > Maintenance > Backup/Restore**.

1. Back up the root or entire unit configuration.

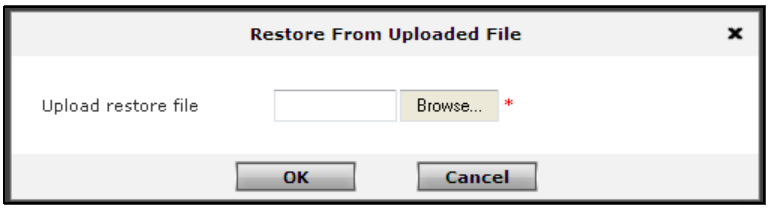


2. Download and delete backup files.

3. Restore the system using local backup files.



4. Restore the system using uploaded files.



Configuration Notes

- The backup filename can be 1-128 letters, digits, and underscores and cannot begin with an underscore. Backup filenames must be unique.
- The root system supports a maximum of five entire-unit configuration backup files and five root configuration backup files, and each Vsys supports a maximum of five Vsys configuration backup files.
- Administrators are allowed to back up the configuration of the root system and that of the whole system. Vsys administrators are allowed to back up only the configuration of their own Vsys.

Table 59 Backup and Restore Commands

backup	Backs up the system.
copy backup	Downloads backup files.
delete backup	Deletes backup files.
restore from internal	Restores the system locally.
restore from	Restores the system using uploaded files.

3.18 Technical Support

- 3.18.1 Overview
- 3.18.2 Basic Configuration Steps

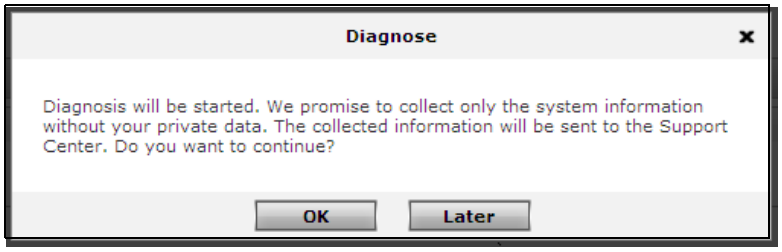
3.18.1 Overview

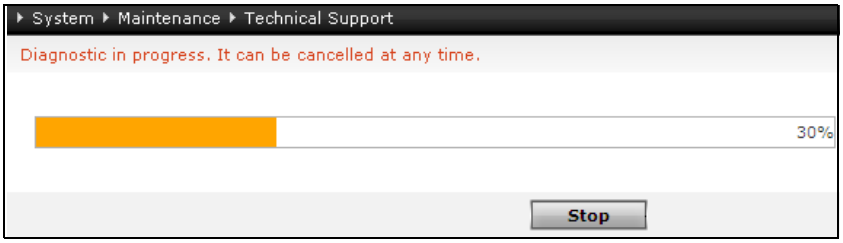
Through the one-touch operation, you can conveniently send diagnostic files to Technical Support Center. Diagnostic information includes information about configuration files, system status, or logs. Diagnostic files are saved on FGX. You can view, delete, or download diagnostic files. When a new diagnostic file is generated, it will replace the old one.

3.18.2 Basic Configuration Steps

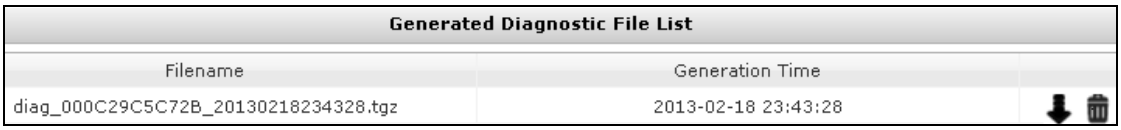
Choose **System > Maintenance > Technical Support**.

1. Diagnose the system.





2. View, delete, and download generated diagnostic files.



3.19 Centralized Management

- 3.19.1 Overview
- 3.19.2 Basic Configuration Steps

3.19.1 Overview

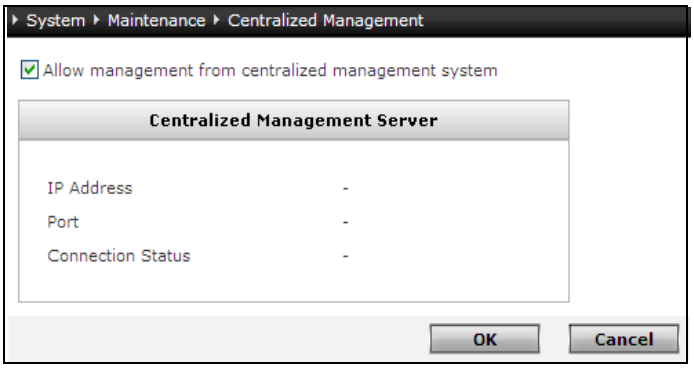
Centralized management is designed for network security devices, providing management functions such as alerts, monitoring, logging, and reporting. FGX supports centralized management, but it can be managed by only one centralized management system at a time.

Centralized management can be used even when there is no license imported.

When centralized management is enabled, FGX performs authentication on all servers that send centralized management requests to it, and only the server that pass the authentication can manage FGX. To configure the system, the centralized management server needs to temporarily get the configuration lock, and it will release the lock automatically after the configuration is done.

3.19.2 Basic Configuration Steps

Choose **System > Maintenance > Centralized Management**. Enable centralized management.



3.20 Diagnosis Tools

FGX provides the following diagnostic tools:

- 3.20.1 Ping. Test the connectivity between FGX and remote hosts.
- 3.20.2 Traceroute. Trace packet transmission.
- 3.20.3 Debug. Listen to packets and sessions.

3.20.1 Ping

Use **`ping`** to test network reachablity.

Table 60 Ping Commands

ping {*host_name* | *ipv4_address*} [*num*] **ping6** {*host_name* | *ipv6_address* [**interface** *interface_name*]} [*num*]	Ping the connectivity between FGX and a destination IP.

3.20.2 Traceroute

Use **`traceroute`** to trace transmission path to a destination host for connection status.

Traceroute learns routes in the following process:

1. Sends a packet with a TTL value of 1 to a destination host. When the packet reaches the first router, the TTL value is reduced to 0. The router drops the packet and sends back an ICMP timeout packet with the IP address of the first router and the time the packet reaches it.
2. Sends a packet with a TTL value of 2 to find out the IP address of the second router and the transmission time.
3. Keeps sending packets with different TTL values until gets the complete path to the destination host.

Each router in the path will be traced three times. The output format is:

```
Sequence number IP address/Domain name Tracing time 1 Tracing time 2 Tracing
time 3
```

- **Sequence Number**—The sequence of a router in the path a packet passes through.
- **IP Address**—The IPv4 address or domain name of the router or server a packet passes throgh.
- **Tracing Time 1, 2, 3**—The time a packet spends reaching and returning from the current router during the first, second and third tracing, in milliseconds.

Table 61 Traceroute Command

traceroute {*ipv4_address* | *domain name*}	Trace the routing path to a destination router or server.

3.20.3 Debug

You can trace and listen to packets through debug.

- 3.20.3.1 General Debug
- 3.20.3.2 VPN Debug
- 3.20.3.3 PPPoE Debug

3.20.3.1 General Debug

The table below shows the general debug commands.

- basic debug commands (**`show debug`**... **`debug clear`**).
- **debug dump hook**—sets types of packets for listening.
- **debug match**—sets matching conditions to listen to specified packets.
- **debug dump**—sets output conditions.

Table 62 Debug Commands

show debug	Views debug configuration information.
debug start *time* [*file_name*]	Sets a monitoring period (3-14,400 seconds).
debug stop	Stops listening.
debug file remove [*file_name*]	Removes debug files.
debug file download	Downloads debug files.
debug clear	Stops dumping packets and resets match conditions.
debug dump hook all	Listens to all packets.
debug dump hook dnat	Listens to packets on which DNAT was performed.
debug dump hook error	Listens to packets with error during transmission.
debug dump hook input	Listens to packets received.
debug dump hook input_error	Listens to packets received and packets on which error occurs during transmission.
debug dump hook input_output	Listens to packets received and successfully sent.
debug dump hook output	Listens to packets successfully sent.
debug dump hook output_error	Listens to packets sent and packets on which error occurs during transmission.
debug dump hook policy	Listens to packets matching policies.
debug dump hook route	Listens to packets routed.
debug dump hook snat	Listens to packets on which SNAT was performed.
debug match bidir	Enables or disables bidirectional listening.
debug match input	Sets incoming interfaces, any, channel, Ethernet, local, PPPoE, or VLAN.
debug match ip	Sets source and destination IPv4 or IPv6 addresses.
debug match mac	Sets source and destination MAC addresses.
debug match output	Sets outgoing interfaces, any, channel, Ethernet, local, PPPoE, or VLAN.
debug match port	Sets source and destination ports.

Table 62 Debug Commands (*continued*)

debug match protocol	Sets protocols, any, ARP, ICMP, ICMPv6, TCP, or UDP.
debug match tunnel	Sets VPN tunnels.
debug dump bytes	Sets the maximum output byte of packets.
debug dump session	Sets whether to output session information.
debug dump complex	Sets whether to output the detailed information of the packet header.

3.20.3.2 VPN Debug

Debug a specified auto IKE tunnel or all auto IKE tunnels. VPN debug is disabled by default.

The output debug information includes:

- The negotiation result/status
- The tunnel being debugged
- Information about each field of a negotiation packet

Table 63 VPN Debug Commands

show debug vpn [**all-tty**]	Views VPN debug configuration.
unset debug vpn [**all-tty**]	Cancels printing VPN debug information.
debug vpn ipsec *timeout*	Prints IPSec debug information.
debug vpn isakmp {**error** | **basic** | **detail**}	Prints ISAKMP debug information in three levels: error, basic, and detail.
unset debug vpn isakmp [**tunnel** *tunnel_name*]	Cancels printing ISAKMP debug information.
debug vpn l2tp	Prints the Layer 2 Tunneling Protocol (L2TP) debug information for all tunnels.
unset debug vpn l2tp	Cancels printing L2TP debug information for all tunnels.
debug sslvpn {**on** | **off**}	Enables or disables printing SSL VPN debug information.

3.20.3.3 PPPoE Debug

Configure PPPoE debug and view the configuration.

Table 64 PPPoE Debug Commands

show debug pppoe [all-tty]	Views PPPoE debug configuration.
debug pppoe	Prints PPPoE debug information.
unset debug pppoe [**all-tty**]	Cancels printing PPPoE debug information.
show debug pppoev6 [**all-tty**]	Views PPPoEv6 debug configuration.
debug pppoev6	Prints PPPoEv6 debug information.
unset debug pppoev6 [**all-tty**]	Cancels printing PPPoEv6 debug information.

3.21 Alert Configuration

- 3.21.1 Overview
- 3.21.2 Basic Configuration Steps
- 3.21.3 Parameters

3.21.1 Overview

When an event occurs, if it matches an alert policy, logs will be generated in English or Simplified Chinese and sent to the corresponding server. Alert policies include:

- Local log alert policy

  There is a default local log alert policy named “internal.” You can view and edit the policy, but you cannot delete it.

- Syslog alert policies

  The system sends system logs to a remote syslog server.

- E-mail alert policies

  The system sends an alert to a specified e-mail address by using a mail server.

- SNMP trap alert policies

  The system can send system logs to the SNMP management station in the SNMP trap mode. It also supports to send logs to more than one SNMP trap server. SNMP trap has two versions, v1 and v2c.

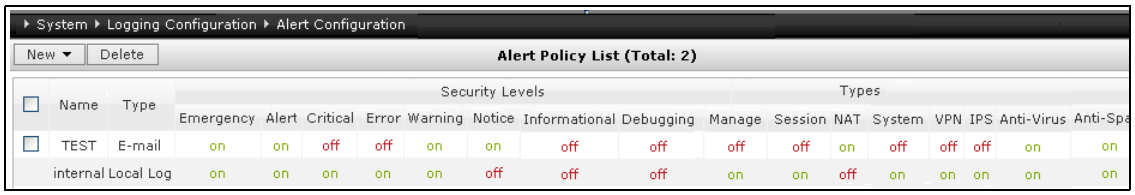
- Terminal print alert policies

Note: FGX supports 15 policies each for syslog, e-mail, and SNMP trap alerts.

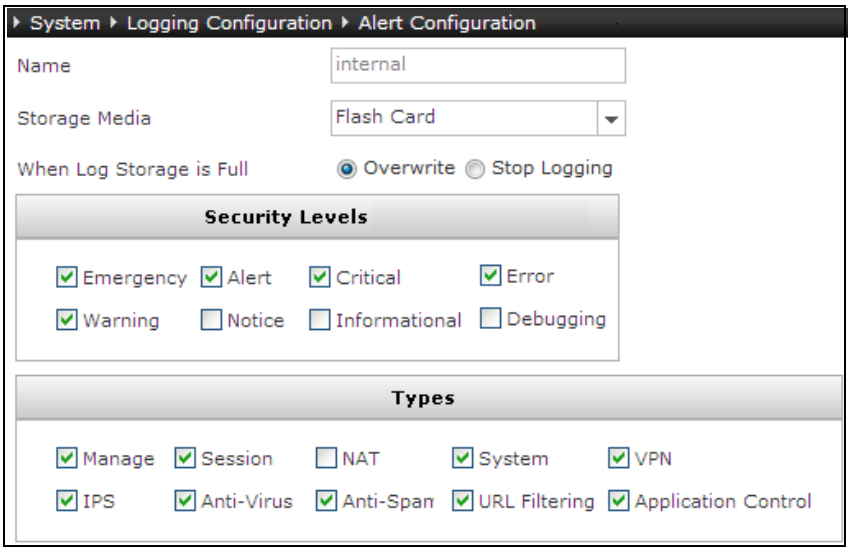
3.21.2 Basic Configuration Steps

Choose **System** > **Logging Configuration** > **Alert Configuration**.

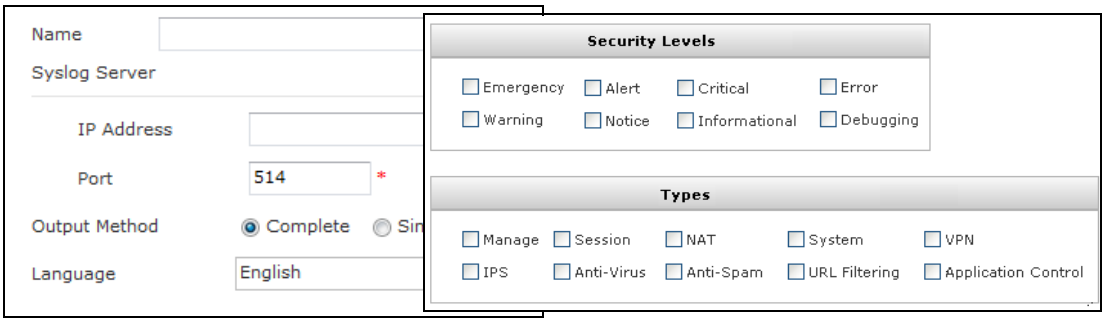
1. View and delete alert policies.



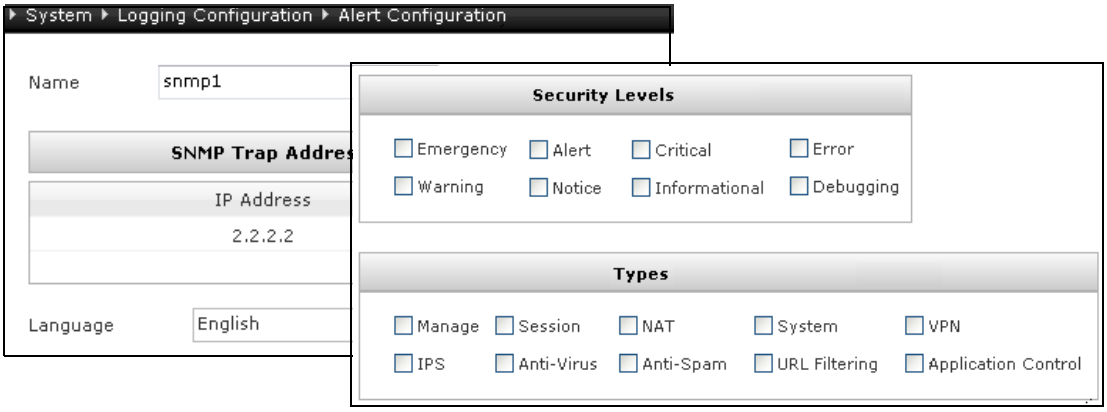
2. Edit the local log alert policy.



3. Create and edit:
   - Syslog alert policies.



- SNMP trap alert policies.



- E-mail alert policies.

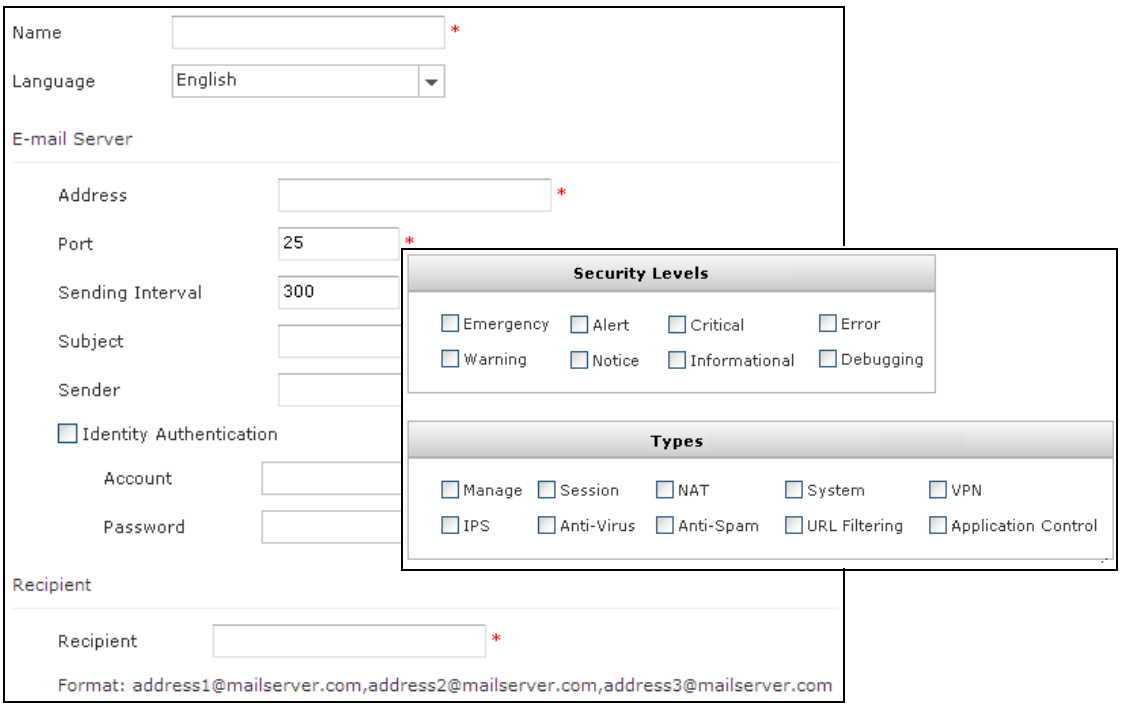


Table 65 Alert Policy Commands

show alert-config	Shows alert policies.
alert-config local-syslog	Edits the local log alert policy.
alert-config syslog	Creates syslog alert policies.
alert-config snmp-trap	Creates SNMP trap alert policies.
alert-config mail	Creates e-mail alert policies.
unset alert-config syslog	Deletes syslog alert policies.
unset alert-config snmp-trap	Deletes SNMP trap alert policies.
unset alert-config mail	Deletes e-mail alert policies.

3.21.3 Parameters

Table 66 Parameters of the Local Log Alert Policy

Parameter	Description
Name	Local log alert policy name. 1-63 UTF-8 characters except spaces and ? , " ' \ < > & #.
Storage Media	Log storage media, Flash Card and Hard Disk.
When Log Storage is Full	Sets log storage policies, Overwrite and Stop Logging.
Security Levels	FGX generates logs for different security levels of events, Emergency, Alert, Critical, Error, Warning, Notice, Informational, and Debugging.
Types	System log sources, Manage, Session, NAT, System, VPN, IPS, Anti-Virus, Anti-Spam, URL Filtering, and Application Control.

Table 67 Parameters of Syslog Alert Policies

Parameter	Description
Name	Syslog alert policy name. 1-63 UTF-8 characters except spaces and ? , " ' \ < > & #.
Syslog Server	Sets Syslog server IP address and port number: • **IP Address—**[0-223].[0-255].[0-255].[0-255]. • **Port—**1-65535. 514 by default.
Output Method	Methods in which system logs are output to the Syslog server: • **Complete—**outputs system logs completely, including message header and message body. The output format is: **<pri> Month** + **Date** + **Time** + **Host Name: Vsys Name** + **Event Library Version** - **Language ID** - **Module ID** - **Event ID** + **Security Level** + **Module Type** + **User Name** + **rep = Number of Times** | **Message** • **Simplified—**outputs part of a system log. The output format is: **<pri> Month** + **Date** + **Time** + **Host Name: Vsys Name** + **Event Library Version** - **Language ID** - **Module ID** - **Event ID** + **Security Level** + **Module Type** The default output method is Complete.
Language	Languages to output logs, English or Simplified Chinese.
Security Levels	Security levels of events in system logs.
Types	Sources of system logs.

Table 68 Parameters of E-mail Alert Policies

Parameter	Description
Name	E-mail alert policy name. 1-63 UTF-8 characters except spaces and ? , " ' \ < > & #.
Language	Languages to output logs, English or Simplified Chinese.
E-mail Server	Sets e-mail server that receives e-mail messages: • **Address—**an IP address or a domain name. IP address range [0-255].[0-255].[0-255].[0-255]. Domain name length 2-255 characters. • **Port—**1-65535. 25 by default. • **Sending Interval—**1-2,678,400 seconds. 300 by default. • **Subject—**0-64 UTF-8 characters except spaces and ? ' \. When sending an e-mail message, the serial number of the product is automatically appended to the e-mail subject. • **Sender—**e-mail address used to send e-mail messages. • **Identity Authentication—** when identity authentication is enabled, account and password are required. 1-255 characters.
Recipient	E-mail address for receiving alerts. A maximum of 10 e-mail addresses separated by commas.
Security Levels	Security levels of events in system logs.
Types	Sources of system logs.

Table 69 Parameters of SNMP Trap Alert Policies

Parameter	Description
Name	SNMP trap alert policy name. 1-63 UTF-8 characters except spaces and ? , " ' \ < > & #.
SNMP Trap Address	Sets SNMP Trap addresses: • **IP Address—**the IP address of an SNMP server that receives system logs in the SNMP trap mode. IP address range [0-223].[0-255].[0-255].[0-255]. • **Version—**versions of SNMP received by SNMP servers, v1 or v2c.
Language	Languages to output logs, English or Simplified Chinese.
Security Levels	Security levels of events in system logs.
Types	Sources of system logs.

3.22 Log Maintenance

- 3.22.1 Overview
- 3.22.2 Basic Configuration Steps
- 3.22.3 Parameters

3.22.1 Overview

Logs are generated to show the real-time running of the system. Logs are stored on local storage media. When the log file size exceeds the maximum storage space, the system will overwrite the oldest log files or stop logging.

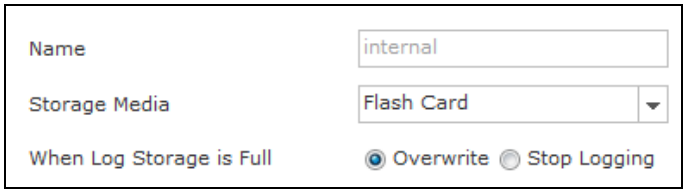
Events that match different alert policy types have different log output formats.

Table 70 System Log Output Formats

Policy Type	Log Output Format
Local log	**<pri> YYYY-MM-DD hh:mm:ss hostname:vsysname ver-lid-mid-evid Level Type username rep=xx | Message** Example: <165>2013-03-18 11:01:32 FGX:root 03-02-275-0000 Notice Manage root rep=1 | Administrative user root logged in through web from 10.2.1.153 successfully.
Syslog	Syslog alerts have two output formats: • **Complete**—outputs system log completely in the following format: **<pri> YYYY-MM-DD hh:mm:ss hostname:vsysname ver-lid-mid-evid Level Type username rep=xx | Message** Example: <165>2013-03-18 11:01:32 FGX:root 03-02-275-0000 Notice Manage root rep=1 | Administrative user root logged in through web from 10.2.1.153 successfully. • **Simplified**—outputs an abbreviated system log in the following format: **<pri> YYYY-MM-DD hh:mm:ss hostname:vsysname ver-lid-mid-evid Level Type** Example: <165>2013-03-18 11:01:32 FGX:root 03-02-275-0000 Notice Manage
E-mail	**<pri> YYYY-MM-DD hh:mm:ss hostname:vsysname ver-lid-mid-evid Level Type username rep=xx | Message** Example: <165>2013-03-18 11:01:32 FGX:root 03-02-275-0000 Notice Manage root rep=1 | Administrative user root logged in through web from 10.2.1.153 successfully. The subject of an alert e-mail message is: **[syslog] + MAC Address + Subject** When FGX which has a MAC address “000C29FB8FF0” sends an e-mail message of system logs with a customized subject “test”, the subject of the e-mail message is: [syslog]000C29FB8FF0test.
SNMP Trap	**<pri> YYYY-MM-DD hh:mm:ss hostname:vsysname ver-lid-mid-evid Level Type username rep=xx | Message** Example: <165>2013-03-18 11:01:32 FGX:root 03-02-275-0000 Notice Manage root rep=1 | Administrative user root logged in through web from 10.2.1.153 successfully.

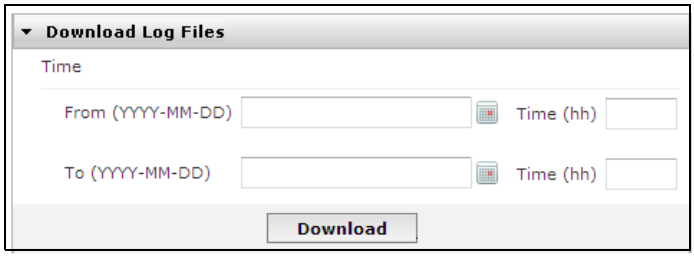
3.22.2 Basic Configuration Steps

Choose **System > Logging Configuration > Alert Configuration**. Click corresponding to the default local log alert policy “internal” and set log storage media and policies.



Choose **System > Logging Configuration > Log Maintenance**.

1. Download logs.



2. Delete all logs or logs generated within a specified period.

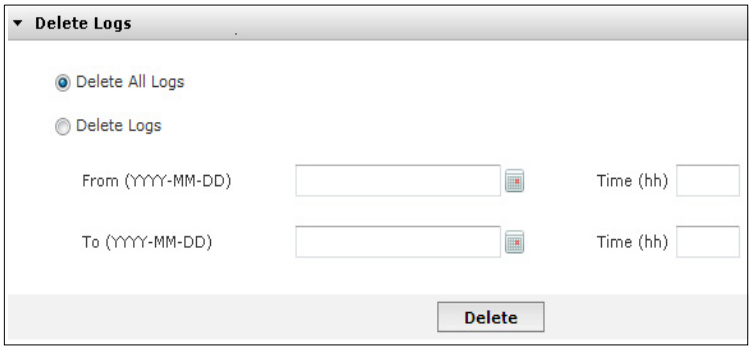


Table 71 Log Commands

logging media	Sets log storage media.
logging policy	Sets log storage policies.
delete log all,time	Deletes logs.

3.22.3 Parameters

Table 72 Parameters of System Logs

Parameter	Description
Priority	The first part of a system log message. The PRI part starts with a leading less-than character, followed by a number, which is followed by a greater-than character. The number contained within these angle brackets is a decimal known as the Priority value and represents both the Facility and Severity (Facility*8 + Severity). The Facilities and Severities of the messages are numerically coded with decimal values. For details, see **RFC 3164**. (FGX facility is 20.)
Date and Time	Indicates the date and time a system log was generated. The format is **YYYY-MM-DD hh:mm:ss**. For example, 2013-03-18 02:34:45.
Host and Vsys	Names of the host and the Vsys that generate system logs. The format is **hostname:vsysname**. For example, if the host name is henry and the Vsys name is root, the host is shown as henry:root.
Basic Information	Shows event base version, language ID, module ID, and event ID. The format is **ver-lid-mid-evid**. • Event base version is a two-byte integer. The current event base version is 03. • Language ID is a two-byte integer. 01 indicates Simplified Chinese and 02 indicates English. • Module ID is a two-byte integer. • Event ID is a four-byte integer.
Security Levels	Eight security levels include: • **Emergency—**memory shortage or hardware anomalies, such as power or CPU anomalies. This level ID is 0. • **Alert—**events that require immediate response, such as an attack. This level ID is 1. • **Critical—**conditions in which the device performance is affected, such as the plugging in or unplugging of a cable and the enabling or disabling of an NIC. This level ID is 2. • **Error—**all failed operations such as adding, deleting, and modification, as well as failure of packet reassemble and policy matching. This level ID is 3. • **Warning—**conditions that might affect system performance, such as mail server connection failure and authentication failure or timeout. This level ID is 4. • **Notice—**common events, such as successful addition, deletion, or modification. This level ID is 5. • **Informational—**general information about system operations. This level ID is 6. • **Debugging—**information related to debugging. This level ID is 7.
Types	Type of the module where a system log was generated. Module types Include Manage, System, Session, NAT, VPN, IPS, Anti-Virus, Anti-Spam, URL Filtering, and Application Control.

Table 72 Parameters of System Logs (*continued*)

Parameter	Description
User	The name of the user who triggered the log message generation, including administrative users, users, and the system. • Most log messages of the Manage type are triggered by administration operations, so the user name is the current administrator's name. • Log messages on sessions and forwarding data are related to source users, so the user name is the authenticated user who initiated the session or who sent the data. If the source user is not authenticated, the user name is displayed as "N/A". • Log messages generated by the system (scheduled tasks, such as DHCP and SAC) display the user name as "N/A". • For log messages generated in other cases, the user name is "N/A".
Repeat Times	Repeat times of a system log message. Duplicate system logs within a set period of time can be merged.
Message	The body of a system log message. A message describes events that occurred and includes parameters related to the events.

3.23 Certificates

- 3.23.1 Overview
- 3.23.2 Basic Configuration Steps
- 3.23.3 Example: Generate Certificates
- 3.23.4 Parameters / Local certificates
- 3.23.5 Parameters / CA certificates

3.23.1 Overview

Digital certificates are issued and managed by CA and can be used to authenticate identity in IKE negotiation. FGX supports identity authentication, but it does not support certificate issuance. FGX achieves certificate authentication through CA.

- Local Certificates

  To get a local certificate, you need to generate a local certificate request file first.

  Local certificates can be enrolled manually or automatically. Save a certificate request file to local for getting a certificate from CAmanually.

  FGX supports automatic certificate enrollment and renewal using the Simple Certificate Enrollment Protocol (SCEP). It sends the CA server a certificate renewal request within a specified time before the certificate expires.

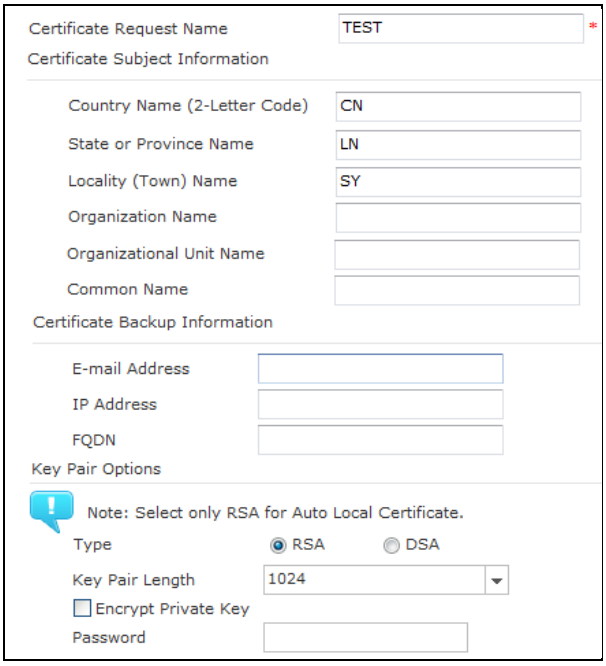
- CA Certificates

  CA certificates are used to verify the certificates issued by CA. FGX supports two ways of verifying certificates: OCSP and CRL. CRL is used by default. FGX CRL list contains all invalid or expired local certificates issued by CA. When using OCSP, FGX acts as an OCSP client and sends a verification request to an OCSP server. The OCSP server then checks the certificate status.

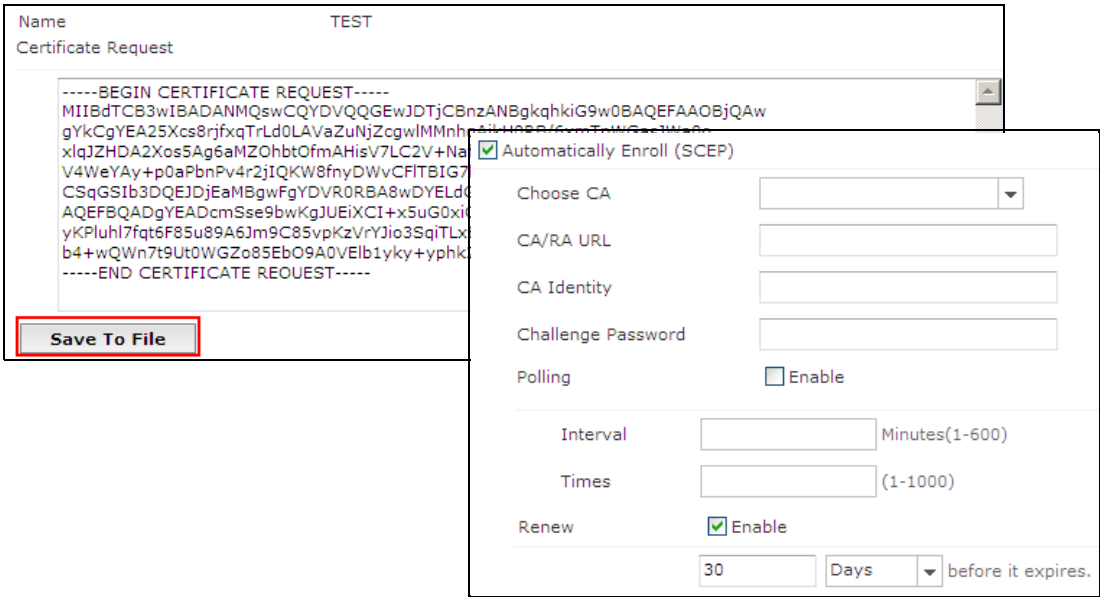
3.23.2 Basic Configuration Steps

Choose **System** > **Certificates** > **Local Certificates**.

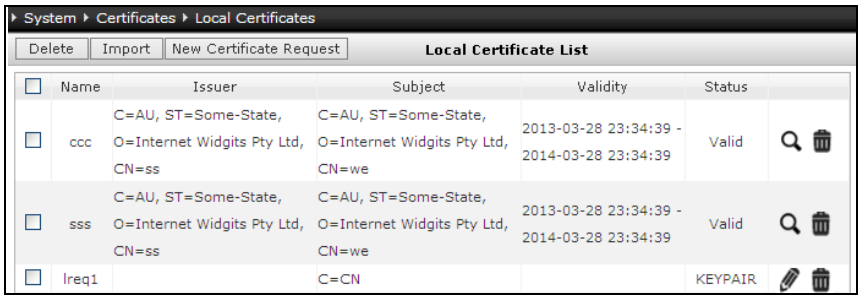
1. Generate local certificate requests.



2. Save the local certificate request to local for manual generation or enable automatic enrollment.

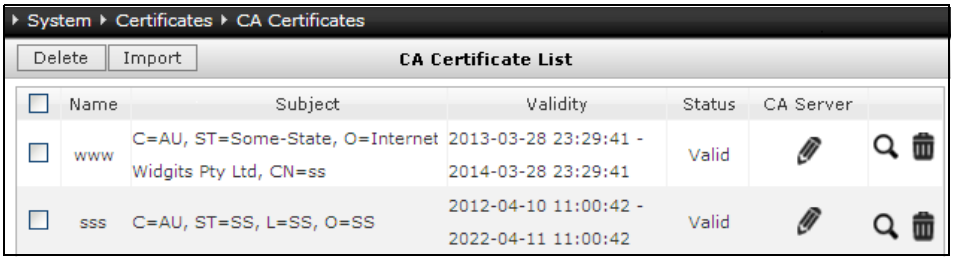


3. View, delete, and import local certificates.

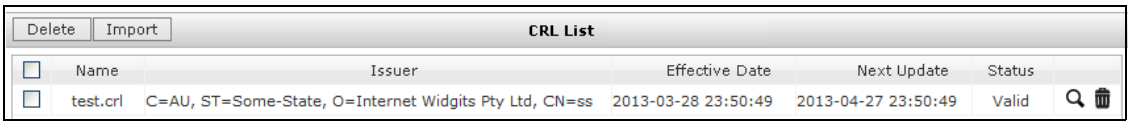


Choose **System** > **Certificates** > **CA Certificates**.

1. View, delete, and import CA certificates.



2. Import certificates to the CRL list or delete certificates from the CRL list.



Configuration Notes

- The first time you apply for a certificate from the CA server, the system will prompt you to verify the fingerprint of the CA certificate. Only when the fingerprint is verified can you continue the certificate enrollment.
- Certificate objects must be imported in the order of CA certificate, CRL, and local certificate, because both the CA certificate and CRL are required to verify whether the local certificate is issued by a CA and whether it is valid.
- You can import CRL, CA, or local certificates that are to be valid, but you cannot import expired ones.
- Local certificates being used by IPSec VPN tunnels cannot be deleted.

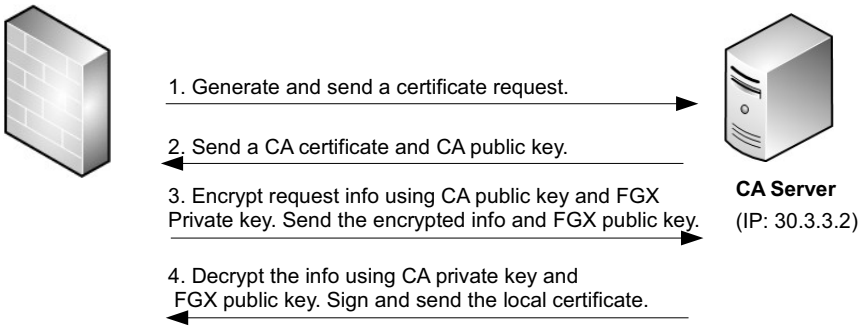
Table 73 Certificate Commands

generate certificate-request	Generates local certificate requests.
enroll request ca	Sends a local certificate request to a CA.
enroll request accept-ca-certificate	Accepts or denies a CA certificate fingerprint.
ca certificate checkmethod	Specifies a method for checking local certificates.
delete certificate req	Deletes local certificate requests.
delete certificate ca, crl, local	Deletes CA certificates, CRLs, or local certificates.
import certificate	Imports a local or a CA certificate.
import certificate crl	Imports a CRL.

3.23.3 Example: Generate Certificates

This example shows how to generate a local certificate automatically through a CA server. Figure 7 shows certificate enrollment process.

Figure 7 Certificate Enrollment

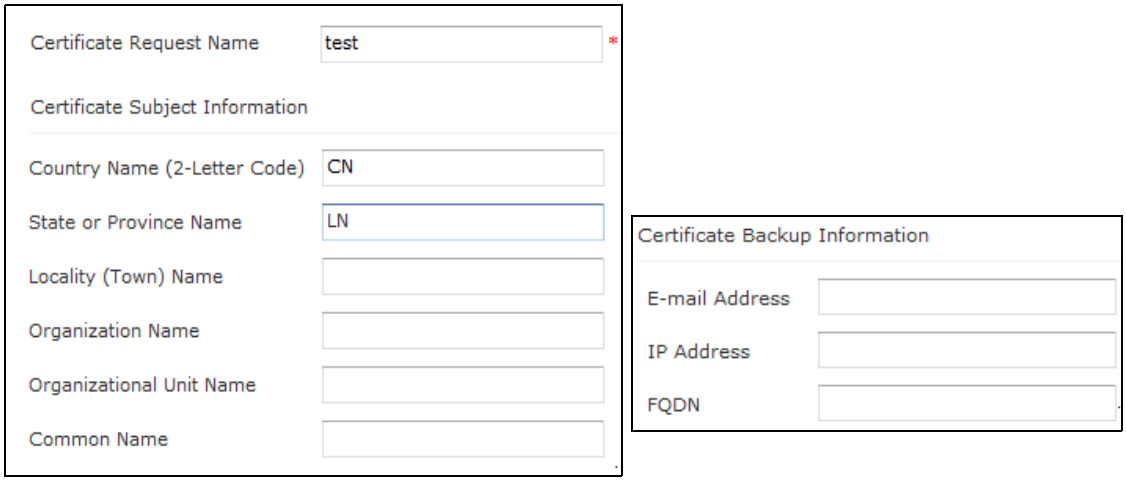


Configuration steps are listed below:

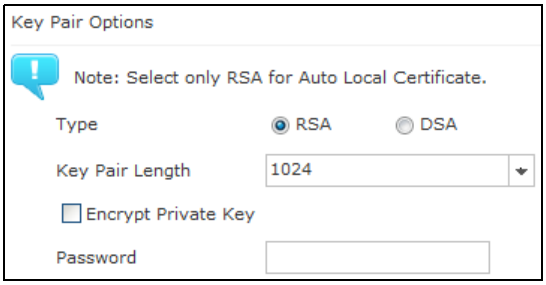
- 3.23.3.1 Create a Certificate Request
- 3.23.3.2 Enroll Certificate Automatically

3.23.3.1 Create a Certificate Request

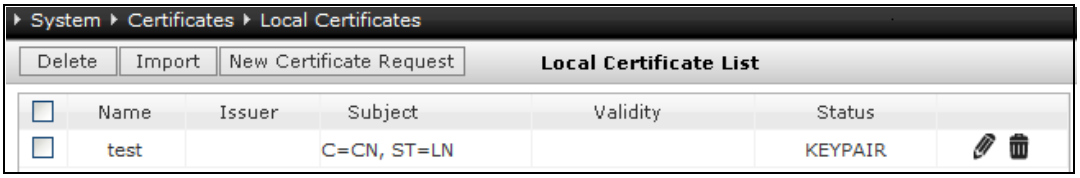
1. Choose **System** > **Certificates** > **Local Certificates**.
2. Click **New Certificate Reuquest**. Enter certificate request name and certificate subject and backup information.



3. Specify key information in the Key Pair Options section.



4. Click **OK**.
5. View the generated certificate request in **Local Certificate List**.



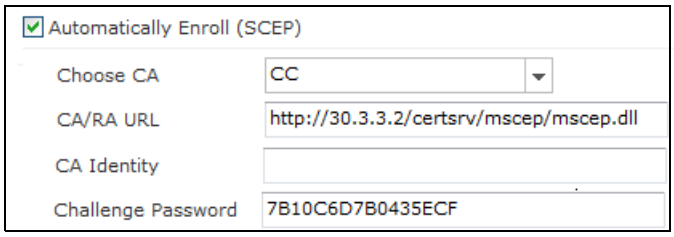
CLI

```
FGX@root> configure mode override
FGX@root-system] generate certificate-request test country CN state-or-province LN locality none organization none organizational-unit none common-name none ip-address none email-address none dns none rsa 1024
FGX@root-system] end
FGX@root> save config
```

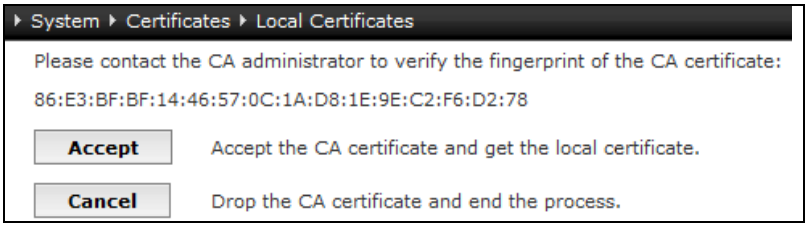
3.23.3.2 Enroll Certificate Automatically

1. Click corresponding to the generated certificate request.
2. Check Automatically Enroll (SCEP) and enter the CA certificate name, CA/RA URL, CA identity, and challenge password below.

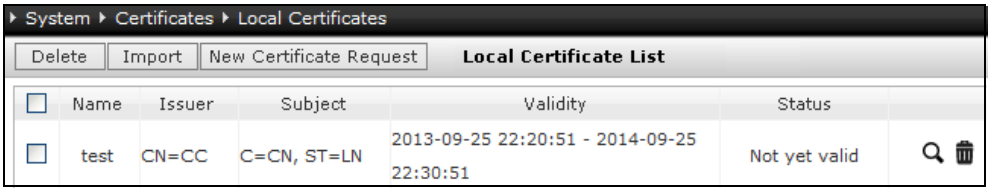
Note: The challenge password and the fingerprint are given by the CA server.



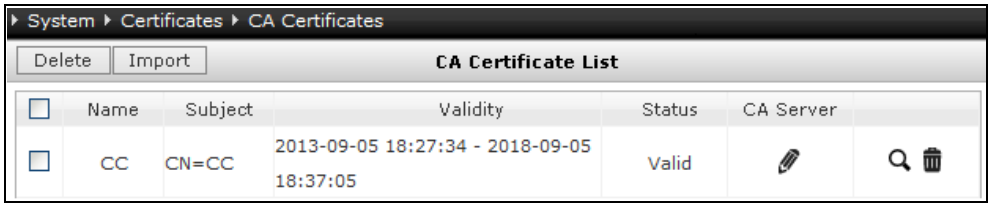
3. Click **OK** and verify the fingerprint of the CA certificate. Click **Accept** if it is correct.



4. New certificates are generated. Click **Return** to view the generated local certificate in **Local Certificate List**.



5. View the generated CA certificate in **CA Certificate List**.



CLI

```
FGX@root> configure mode override
FGX@root-system] enroll request test ca CC url http://30.3.3.2/
certsrv/mscep/mscep.dll ident none challenge 7B10C5D7B0435ECF
polling disable
% Please contact the CA administrator to verify the finger print of CA
certificate:
        86:E3:BF:BF:14:46:57:0C:1A:D8:1E:9E:C2:F6:D2:78
FGX@root-system] enroll request test accept-ca-certificate accept
% You have successfully generated the certificate.
Please check the certificates in the certificate list.
FGX@root-system] end
FGX@root> save config
```

3.23.4 Parameters / Local certificates

Table 74 Parameters of Local Certificate Requests

Parameters	Description
Certificate Request Name	Certificate request file name. 1-63 UTF-8 characters except spaces and ? , " ' \ < > & #.
Certificate Subject Information	Certificate subject information includes: • **Country Name (2-Letter Code)—**the name of the country where FGX locates. • **State or Province Name—**the name of the state or province where FGX locates. 0-127 UTF-8 characters except spaces and ` ? , " ' \ < > &. • **Locality (Town) Name—**the name of the locality where FGX locates. 0-127 UTF-8 characters except spaces and ` ? , " ' \ < > &. • **Organization Name—**the organization which FGX belongs to. 0-64 UTF-8 characters except spaces and ` ? , " ' \ < > &. • **Organization Unit Name—**the department in which FGX is applied. 0-64 UTF-8 characters except spaces and ` ? , " ' \ < > &. • **Common Name—**certificate subject name. 0-64 UTF-8 characters except spaces and ` ? , " ' \ < > &.
Certificate Backup Information	Certificate backup information includes: • **E-mail Address—**the e-mail address of the person who is responsible for the certificate. The length range is 5-64 characters. • **IP Address—**the IP address of the FGX device using the certificate. The maximum length is 64 characters • **FQDN—**the fully qualified domain name of the FGX device which uses the certificate. The length range is 2-64 characters. It can also be a domain name without dots. Specify at least one item in the **Certificate Subject Information** and **Certificate Backup Information** sections.
Key Pair Options	Key pair options include: • **Type—**the public key algorithm, RSA and DSA. RSA is used when you want to apply for a certificate automatically. • **Key Pair Length—**the longer the key, the more secure the communication, but the slower the speed of encryption and decryption. The key length can be 768,1024,1536, and 2048. 1024 by default. • **Encrypt Private Key—**encrypt the private key of the certificate. Disabled by default. • **Password—**the private key. 0-127 characters.

Table 75 Parameters of Automatic Certificate Enrollment and Renewal

Parameters	Description
Automatically Enroll (SCEP)	Enrolls certificates automatically. Disabled by default.
Choose CA	CA certificate name. This certificate is given by the CA server.

Table 75 Parameters of Automatic Certificate Enrollment and Renewal (*continued*)

Parameters	Description
CA/RA URL	The URL of the CA or RA (Register Authority) server that will issue the certificate. 2-255 characters.
CA Identity	The ID of the CA certificate to be generated. CA identities are used to uniquely identify CA certificates. Maximum length 255 characters.
Challenge Password	When the CA server uses a preshared key in ID authentication, the challenge password is used to verify the identity of the certificate requestor. Maximum length127 characters.
Polling	If the polling function is enabled, when waiting for the CA server to verify the certificate request, the system will keep sending polling messages until the number of messages reaches the limit or the CA server returns a status identifier. Disabled by default.
Interval	The interval between two consecutive polling messages sent by the system. 1-600 minutes.
Times	The maximum number of times that the system can send polling messages. 1-1,000.

Table 76 Parameters of Local Certificates

Parameter	Description
Name	Local certificate name. 1-63 UTF-8 charactersexcept spaces and ? , " ' \ < > & #.
Issuer	The organization that issues, manages, and revokes a local certificate.
Subject	The subject information of a local certificate.
Validity	The valid time of a local certificate.
Status	The status of a digital certificate during the enrollment: • **Valid—**the local certificate is valid. • **Pending—**the certificate is in the polling state, which happens when the CA server uses manual authentication. • **Keypair—**the object is a certificate request. • **Expired—**the certificate has expired. • **Not yet valid—**the certificate is not valid.

3.23.5 Parameters / CA certificates

Table 77 Parameters of Certificate Verification

Parameters	Description
Checking Methods	Certificate revocation checking method, CRL, OCSP, and None. Different CA certificates can use different checking methods and OCSP servers.
Strict Check	It is disabled by default. When using OCSP to check certificate status, if the connection between FGX and the OCSP server fails or the OCSP server returns “Unknown,” the certificate is considered invalid when strict check is enabled and valid when disabled.
OCSP URL	The URL address of the OCSP server is required when using OCSP as checking method. For example, http://ocsp.test.com. If necessary, you can also set the port number simultaneously, for example, http://ocsp.test.com:8080. FGX supports the following OCSP servers: Entrust, Microsoft, RSA Keon, and Verisign.

Table 78 Parameters of CA Certificates

Parameter	Description
Name	CA certificate name. Cannot be “any” (any is not case sensitive).
Subject	The subject information of a CA certificate.
Validity	The valid time of a CA certificate.
Status	CA certificate states during the enrollment: • **Valid—**the digital certificate is valid. • **Expired—**the certificate has expired. • **Not yet valid—**the certificate has not been valid yet.
CA Server	CA server configuration.

3.24 Objects

Policies on FGX can use IP address objects, IP address object groups, service objects, and service object groups.

- 3.24.1 IP Addresses
- 3.24.2 Services

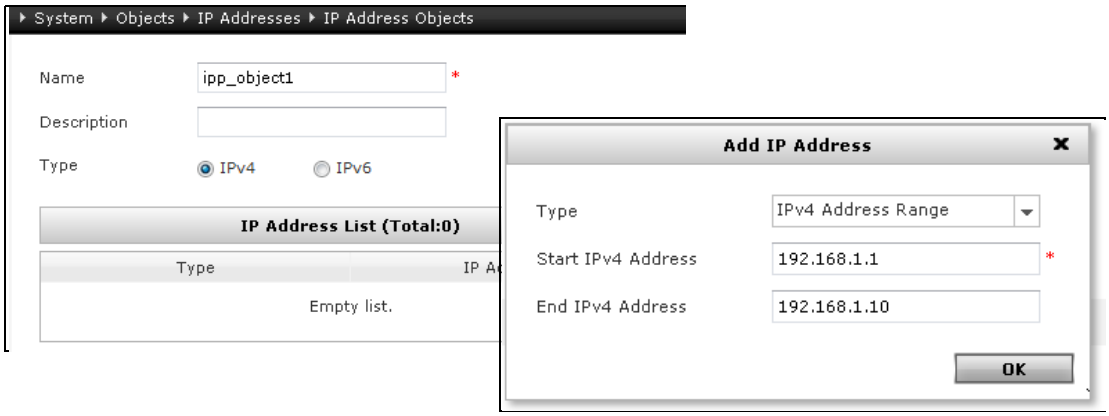
3.24.1 IP Addresses

You can define one or more IP addresses as an object. You can also add IP address objects of the same type to an IP address object group to facilitate configuration.

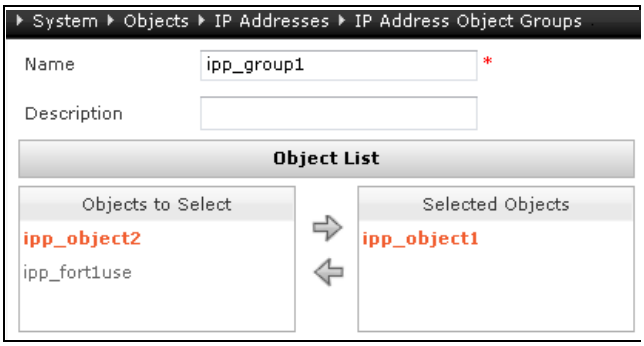
- 3.24.1.1 Basic Configuration Steps
- 3.24.1.2 IP Address Object Parameters
- 3.24.1.3 IP Address Object Group Parameters

3.24.1.1 Basic Configuration Steps

1. Choose **System** > **Objects** > **IP Addresses** > **IP Address Objects**.
2. Click **New** to create an IP address object. Click **Add** to edit IP addresses the object includes.



3. Choose **System** > **Objects** > **IP Addresses** > **IP Address Object Groups**.
4. Click **New** to create an IP address object group. Add objects from **Objects to Select** to the group.



Configuration Notes

- IP address objects being used by policies cannot be deleted.
- FGX supports up to 1,024 IP address objects, and each IP address object supports up to 128 IP address entries.
- FGX supports up to 1,024 IP address object groups, and each IP address object group supports up to 128 IP address objects. An IP address object group cannot have the same name with members within it.

Table 79 IP Address Objects/IP Address Group Objects Commands

object ipaddr *object_name* **description** *string*	Sets desription for an IP address object.
object group *group_name* **type ipaddr** [**object** *object_list*]	Adds an IP address object group or add IP address objects to the specified object group
object group *group_name* **type ipaddr description** *string*	Set description for an IP address object group.
object ipaddr *object_name* [*ipv4_list* | *ipv6_list*]	Adds an IP address object or add IP addresses to the specified IP address object.
unset object ipaddr [*object_name*]	Deletes IP address objects.
unset object group type ipaddr [*group_name*]	Deletes IP address object groups.
unset object group type ipaddr *group_name* **object** *object_name*	Deletes the specified object from an IP address object group.
unset object ipaddr *object_name* {*ipv4_list* | *ipv6_list*}	Deletes IP addresses from an IP address object.

3.24.1.2 IP Address Object Parameters

Table 80 Parameters of IP Address Objects

Parameter	Description
Name	IP address object name. 1-63 UTF-8 characters except ? , " ' \ < > & # and spaces.
Description	Description about an IP address object. 0-255 UTF-8 characters except ? " ' \ < > &.
Type	IP address type, IPv4 or IPv6.
IP Address	The IP addresses an IP address object can include, IPv4/IPv6 address, IPv4/IPv6 address range, IPv4 address and mask, or IPv6 address and prefix.
In Use	Shows the list of policies using an IP address object.

3.24.1.3 IP Address Object Group Parameters

Table 81 Parameters of IP Address Object Groups

Parameter	Description
Name	IP address object group name. 1-63 UTF-8 characters except ? , " ' \ < > & # and spaces.
Description	Description about an IP address object group. 0-255 UTF-8 characters except ? " ' \ < > &.
Included Objects	Objects included in an IP address object group.
In Use	Shows the list of policies using an IP address object group.

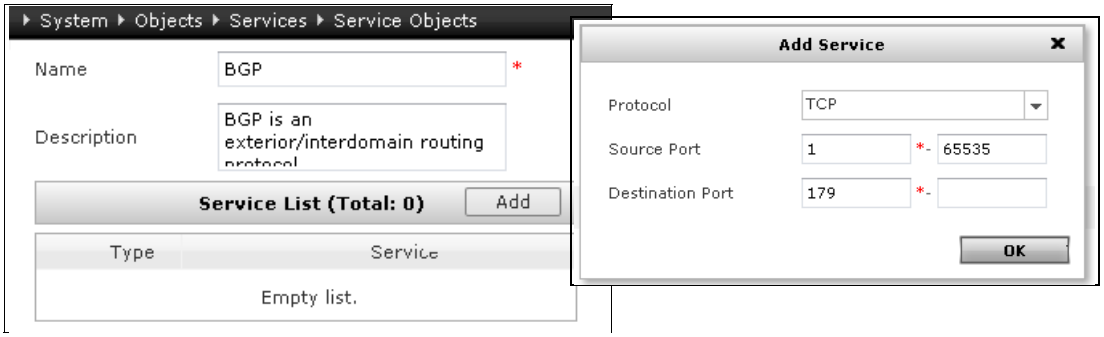
3.24.2 Services

You can define one or more services as an object. You can also add service objects to a service object group to facilitate configuration.

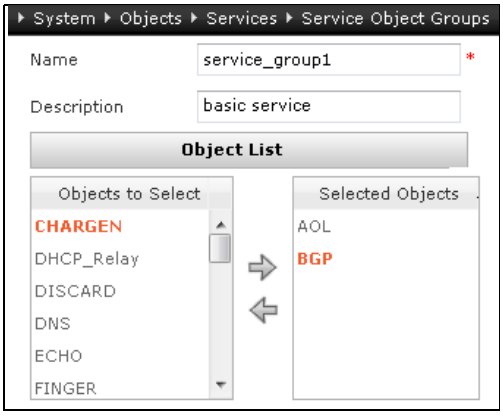
- 3.24.2.1 Basic Configuration Steps
- 3.24.2.2 Service Object Parameters
- 3.24.2.3 Service Object Group Parameters

3.24.2.1 Basic Configuration Steps

1. Choose **System** > **Objects** > **Services** > **Service Objects**.
2. Click **New** to create a service object. Click **Add** to edit services the object includes.



3. Choose **System** > **Objects** > **Services** > **Service Object Groups**.
4. Click **New** to create a service object group. Add objects from **Objects to Select** to the group.



Configuration Notes

- Service objects being used by policies cannot be deleted.
- FGX supports up to 1,024 service objects, and each service object supports up to 128 service entries.
- FGX supports up to 1,024 service object groups, and each service object group supports up to 128 service objects. A service object group cannot have the same name with members within it.

Table 82 Service Object/Service Object Group Commands

object service *object_name* **description** *string*	Sets description for a service object.
object group *group_name* **type service** [**object** *object_list*]	Adds a service object group or add service objects to the specified object group.
object group *group_name* **type service description** *string*	Sets description for a service object group.
object service *object_name* [{**tcp | udp**} {*src_port* | *src_port_range*} {*dst_port* **|** *dst_port_range*} | **icmp** {*icmp_type* | *icmp_list* | **Any** } | **icmpv6** {*icmpv6_type* | *icmpv6_list* | **Any**} | **other** *protocol_num*]	Adds a service object or add services to a service object group.
unset object service [*object_name*]	Deletes service objects.
unset object group type service [*group_name*]	Deletes service object groups.
unset object group type service *group_name* **object** *object_name*	Deletes a service object from a service object group.
unset object service *object_name* {{**tcp | udp**} {*src_port* | *src_port_range*} {*dst_port* **|** *dst_port_range*} | **icmp** {*icmp_type* | *icmp_list* | **Any**} | **icmpv6** {*icmpv6_type* | *icmpv6_list* | **Any**} | **other** *protocol_num*}	Deletes services from a service object.

3.24.2.2 Service Object Parameters

Table 83 Parameters of Service Objects

Parameter	Description
Name	Service object name. 1-63 UTF-8 characters except ? , " ' \ < > & # and spaces.
Description	Description about a service object. 0-255 UTF-8 characters except ? " ' \ < > &.
Service	The protocol and the corresponding protocol type, port numbers, or protocol numbers. Protocols include ICMP, ICMPv6, TCP, UDP, and Other.
In Use	Shows the list of policies using a service object.

3.24.2.3 Service Object Group Parameters

Table 84 Parameters of Service Object Groups

Parameter	Description
Group Name	Service object group name. 1-63 UTF-8 characters except ? , " ' \ < > & # and spaces.
Description	Description about a service object group. 0-255 UTF-8 characters except ? " ' \ < > &.
Included Objects	Service objects included in a service object group.
In Use	Shows the list of policies using a service object group.

4 Network Configuration

This section describes network configuration.

- Interfaces
  - 4.1 Interfaces Overview.
  - 4.2 Ethernet Interface.
  - 4.3 Ethernet Channel.
  - 4.4 Redundant Interface.
  - 4.5 Virtual Interface.
  - 4.6 VLAN Interface.
  - 4.7 Loopback Interface.
  - 4.8 PPPoE Interface.
  - 4.9 Tunnel Interface.
- ARP/CAM
  - 4.10 ARP.
  - 4.11 CAM.
- 4.12 Zones.
- DNS
  - 4.13 DNS Host.
  - 4.14 DNS Proxy.
  - 4.15 DNS Cache.
- DHCP
  - 4.16 DHCP Servers.
  - 4.17 DHCP Server Subnets.
  - 4.18 DHCPv6.
- STP, Neighbor discovery
  - 4.19 STP.
  - 4.20 Neighbor Discovery.

4.1 Interfaces Overview

- 4.1.1 Working Modes
- 4.1.2 Interface Attributes

4.1.1 Working Modes

Interfaces are classified as Layer 2 interfaces or Layer 3 interfaces. Layer 2 interfaces (except for virtual interfaces) have the following two working modes:

- Access (default)

  Interfaces are switching ports responsible for Layer 2 data switching and normally used as access ports to connect terminal devices. An interface in access mode belongs to only one VLAN.

- Trunk

  By setting Layer 2 interfaces to work in trunk mode (trunk ports), multiplexing can be implemented through a single link to forward data among multiple VLANs. You can configure a trunk port to permit certain VLANs so that the trunk port can automatically forward data sent from or to those VLANs.

  - FGX trunk ports use the IEEE 802.1Q protocol to encapsulate packets;
  - Configure a native VLAN on a trunk port to receive packets without IEEE 802.1Q encapsulation. The trunk port drops any unencapsulated packet if no native VLAN has been defined.

  Trunk mode normally applies in scenarios where there are not adequate interfaces connecting to the intranet. For more information, see Example 2: Multi-Vsys Based on Trunk Interface.

4.1.2 Interface Attributes

On FGX, you can view, create, delete, and edit interfaces with IPv4 or IPv6 configurations. Choose **Network > Interfaces** to open the **Interfaces** page and configure related settings.

- You can delete inactive interfaces but cannot manually create or delete Ethernet interfaces and tunnel interfaces.
- An interface in use cannot be deleted. You should dereference the interface before deleting it.
- Tunnel interfaces do not support IPv6 configurations.
- FGX currently does not support IPv6 anycast addresses.

All interfaces have common attributes, such as name and link state. Layer 2 and Layer 3 interfaces have their own specific attributes.

- 4.1.2.1 Common Attributes
- 4.1.2.2 Layer 2 Specific Attributes
- 4.1.2.3 Layer 3 Specific Attributes

4.1.2.1 Common Attributes

Table 85 Common Interface Attributes

Parameter	Description
Interface	The name of an interface. Each type of interface has its corresponding naming convention: eth1 is the name of an Ethernet interface; ch1, a channel interface; vlan1, a VLAN interface; tunnel1, a tunnel interface; rint2, a redundant interface; veth3, a virtual interface; lo2, a loopback interface; and ppp2, a PPPoE interface. You cannot modify the interface name.
Link	The physical status of an interface. The status is maintained automatically by the system. • **Green icon (Up)—**connected and link negotiation was successful. • **Red icon (Down)—**disconnected. The link status is always up for loopback interfaces and tunnel interfaces.
Active	The active state of an interface. The state is normally administratively maintained except for the tunnel interface. • **Green icon (On)—**enabled. • **Red icon (Off)—**disabled. The active state of a tunnel interface is determined by that of its corresponding tunnel.
Mode	The mode of a Layer 2 interface. Modes include Layer 2, Layer 3, and Shared Layer 3. You can make advanced settings to specify a Layer 2 interface to work in access mode or trunk mode. You can set Ethernet interfaces, Ethernet channels, and redundant interfaces to work in shared Layer 3 mode. By default, shared Layer 3 interfaces do not belong to any Vsys (including the root system). One shared Layer 3 interface can be assigned to and used by different Vsys. Shared Layer 3 normally applies in scenarios where there are not adequate interfaces connecting to the Internet. For more information, see Example 1: Multi-Vsys Based on Shared Layer 3 Interface.
MAC Address	The MAC address of an interface. Tunnel interfaces, loopback interfaces, and PPPoE interfaces do not have MAC addresses.
In Use	The list of entries using an interface.
NIC Mode	It has three attributes. Only Ethernet interfaces have NIC mode. • **Link Speed—**the data rate of an interface. 10 Mbps, 100 Mbps, 1000 Mbps, and Auto. In Auto mode, FGX automatically controls its link speed depending on the network environment. • **Duplex—**the duplex mode of an interface. There are three duplex modes: •**Full—**allows FGX to send and receive data simultaneously. •**Half—**allows FGX either to send or to receive data at a given time. •**Auto—**allows FGX to automatically negotiate the duplex mode. • **Flow Control—**controls data flow on an interface. When an interface cannot receive packets because of congestion, FGX sends a message to notify the remote device of the situation. Upon receiving the message, the remote device does not forward packets to the interface until the congestion is eliminated. •**On—**enabled. •**Off—**disabled.

Table 85 Common Interface Attributes (*continued*)

Parameter	Description
Use Specific MAC Address	Check this check box to manually specify a MAC address. Loopback interfaces, tunnel interfaces, virtual interfaces, and PPPoE interfaces do not have this attribute. It is disabled by default.
Connect to Virtual Network	The virtual network with which virtual interfaces connect. Only virtual interfaces have this attribute.
Description	Description about an interface, 0-255 UTF-8 characters. Cannot contain ?'\"<>&.

4.1.2.2 Layer 2 Specific Attributes

Table 86 Layer 2 Specific Attributes

Parameter	Description
Belongs to	The VLAN or channel to which a Layer 2 interface belongs.
Layer 2 Interface List	Assign interfaces to an Ethernet channel. The **Interfaces to Select** list displays all Ethernet interfaces that are in Layer 2 access mode and not assigned to any VLAN.
Layer 2 Advanced Settings	Set the working mode for a Layer 2 interface. Modes include Access (default) and Trunk. • If an interface is configured to work in access mode, you can choose whether or not to assign it to a VLAN. • If an interface is configured to work in trunk mode, you can configure the VLANs allowed by the trunk in **VLAN List** and configure its native VLAN.

4.1.2.3 Layer 3 Specific Attributes

Table 87 Layer 3 Specific Attributes

Parameter	Description
MTU	The maximum transmission unit. The MTU of Layer 3 interfaces only limits packets on outgoing interfaces. If a packet is larger than the outgoing interface MTU, the packet will be fragmented into smaller pieces. The MTU range is listed as below: • In IPv4, the MTU range of loopback interfaces is 68-65,535 bytes; PPPoE interfaces, 68-1,492 bytes; and other Layer 3 interfaces 68-1,500 bytes. • In IPv6, the MTU range of loopback interfaces is 1,280-65,535 bytes; PPPoE interfaces, 1,280-1,492 bytes; and other Layer 3 interfaces 1,280-1,500 bytes. The default MTU of PPPoE interfaces is 1,454 bytes; and other Layer 3 interfaces, 1,500 bytes.
Layer 2 Interface List	Assign Ethernet interfaces, Ethernet channels, redundant interfaces, and virtual interfaces in Layer 2 access mode to a VLAN or assign Layer 2 Ethernet interfaces to an Ethernet channel. The Layer 2 Interface List area comprises two list boxes, Interfaces to Select and Selected Interfaces. VLAN interfaces and Ethernet channels have this attribute.
IP Tracking	Track IP addresses. • Tracking types: **•IPv4 track type—**None, Ping, ARP Ping. **•IPv6 track type—**None, Ping, and NS Ping. **•Wait Time—**the length of time before a redundant interface recovers from failure. Only redundant interfaces have this attribute.
IPv4 Address Configuration	Methods of obtaining IPv4 addresses, including: • **Static IP—**Manually configure static IP addresses for Layer 3 interfaces. You need to configure related settings in IP Address List. • **DHCP—**obtains IP addresses assigned dynamically by a DHCP server. You can set whether to enable DNS proxy. When it is enabled, the system automatically adds DNS proxy according to the DNS information obtained through DHCP interfaces.
IPv4 Address List	Includes the following parameters: Primary, IP Address, and Mask Length. You can add up to 32 IPv4 addresses to the list. Primary indicates the primary IP address used by the interface.
IPv6 Address Configuration	Includes configuration of link-local addresses and ULA/global unicast addresses. • **Link-local address—**can be automatically generated (default) or manually configured. •When you check **Auto Config Link-Local**, it indicates automatically generating the address. FGX will automatically generate a link-local address for the interface based on the link-local prefix and the MAC address of that interface. •When you uncheck **Auto Config Link-Local,** it indicates manually configuring the address. • **ULA/Global unicast address—**can be automatically configured in a stateless manner and manually configured (default). You can choose either or both. •Check **Stateless Auto Config**, FGX will perform a stateless address autoconfiguration. •Uncheck **Stateless Auto Config** and you need to manually configure IPv6 addresses in IP Address List.
IPv6 Address List	Includes the following parameters: IP Address, Prefix Length, Type, and Status. You can manually add up to 31 IPv6 global unicast addresses to the list. • **Type—**the types of ULA or global unicast addresses that you manually configure. Types include: **•Manual—**manually generate an address without using the EUI-64 format interface identifier. **•EUI-64—**use EUI-64 format interface identifier to generate an address. • **Status—**indicates the status of IPv6 addresses, including: TENTATIVE, DUPLICATE, PREFERRED, DEPRECATED, and INVALID.

4.2 Ethernet Interface

- 4.2.1 Overview
- 4.2.2 Basic configuration steps
- 4.2.3 Example: Ethernet Interface

4.2.1 Overview

FGX supports up to 32 Ethernet interfaces.

- Name

  The name of an onboard interface “eth” followed by a number. FGX provides several expansion slots for network interface cards (NICs). Each NIC supports up to four expansion interfaces. The name of an expansion interface begins with “eth” followed by a hyphen, a slot number, and a port number. For example, eth-s1p1 and eth-s2p4. By default, there is only eth0 in Layer 3 mode. The IP address is 192.168.1.100/24. All other Ethernet interfaces work in Layer 2 access mode. For more information, see 4.1.1 Working Modes.

- Vsys

  You can assign a Layer 3 Ethernet interface to a single Vsys. For more information, see Chapter 13, “Virtual Systems.”

- Management interface

  You can set a Layer 3 Ethernet interface as a dedicated management interface (M). The management interface cannot be assigned to any zone. When the working mode or the Vsys of the interface changes, the system automatically changes the interface to a normal interface. The management interface can be used to:

  - Configure Telnet, SSH, Web, and Ping access settings;
  - Configure SNMP, interface WebAuth authentication, external server authentication, and NTP synchronization;
  - Perform system upgrade;
  - Send syslog, e-mail, and SNMP trap alerts.

- Access control

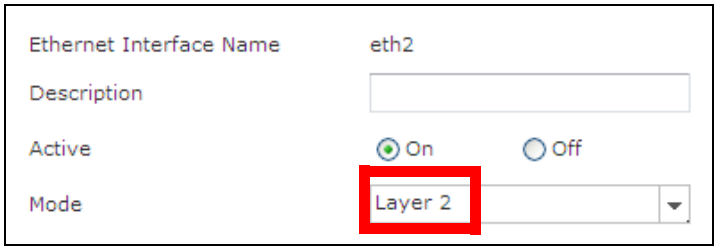
  Login to FGX through the management interface is controlled by access control policies. For more information, see 3.11 Access Services.

4.2.2 Basic configuration steps

- 4.2.2.1 Layer 2.
- 4.2.2.2 Layer 3.
- 4.2.2.3 Shared Layer 3.

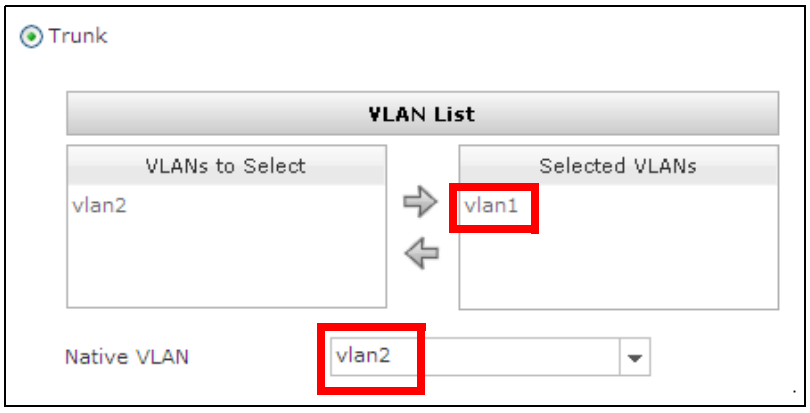
4.2.2.1 Layer 2

1. Choose **Network > Interfaces.**
2. Click corresponding to the Ethernet interface and set the work mode as Layer 2:



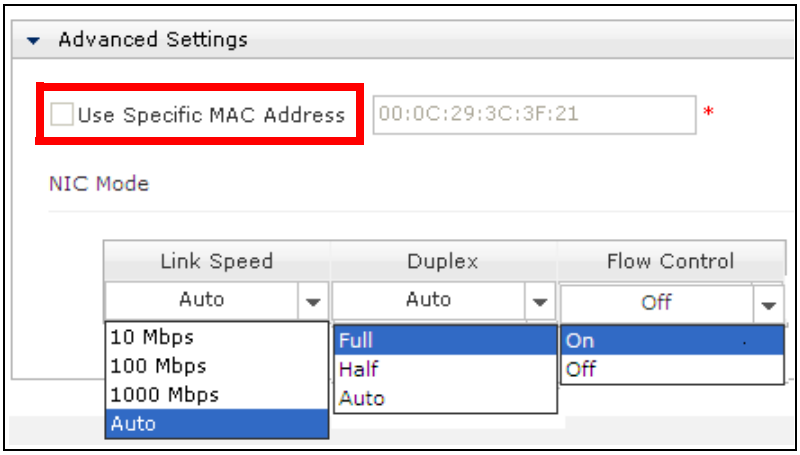
   a. Set the interface to work in access mode and assign it to a VLAN.

   b. Set the interface to work in trunk mode.



   The VLANs you select from **VLAN List** cannot be the same as the native VLAN.

3. In **Advanced Settings**, configure as follows:



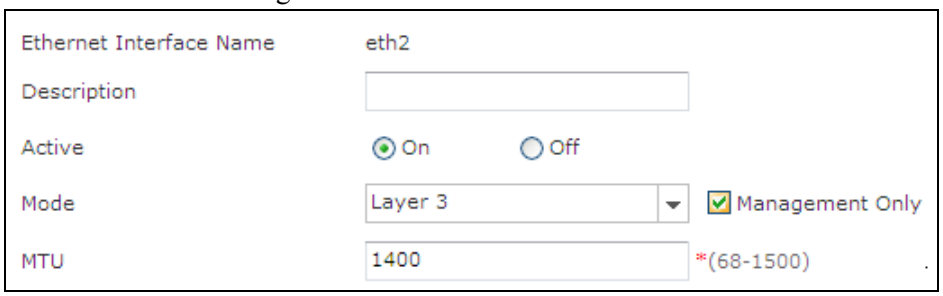
You cannot use a specific MAC address for a Layer 2 interface.

Table 88 Layer 2 Ethernet Interface Commands

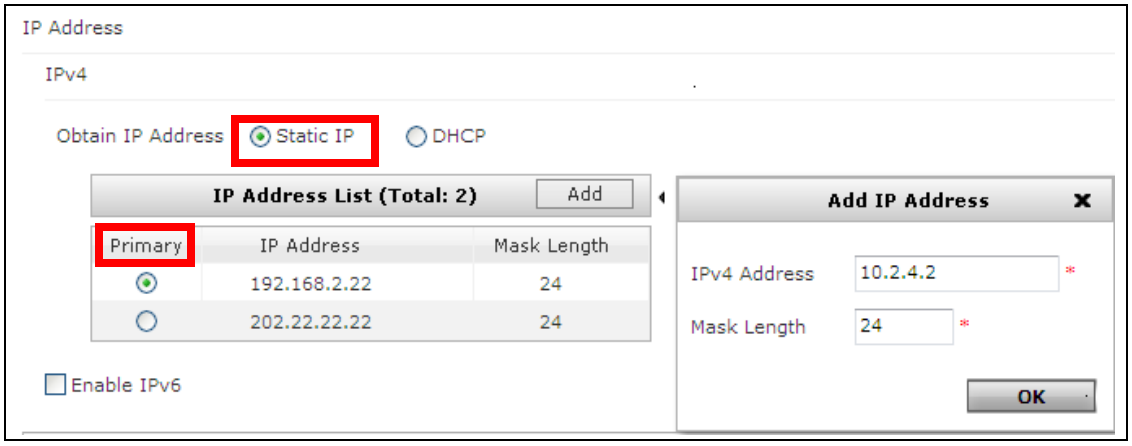
interface ethernet *interface_id*	Enter a specified Ethernet interface configuration mode.
working-type layer2-interface	Set an interface to work in Layer 2 mode.
shutdown	Disable an interface.
unset shutdown	Enable an interface.
port mode {**access** | **trunk**}	Set the working mode for Layer 2 interfaces except virtual interfaces.
port access vlan *vlan_id*	Assign a Layer 2 interface to a specified VLAN.
unset port access vlan	Delete a VLAN to which a Layer 2 interface belongs.
port trunk allowed vlan	Set VLANs which are allowed by a specified trunk port. Data in allowed VLANs will be encapsulated through 802.1Q.
unset port trunk allowed vlan	Delete VLANs which are allowed by a specified trunk port.
port trunk native vlan *vlan_id*	Set a native VLAN which is allowed by a specified trunk port. Data in this VLAN will not be encapsulated through 802.1Q.
unset port trunk native	Delete the native VLAN which is allowed by a specified trunk port.
hold ethernet *interface_id*	Assign Layer 2 Ethernet interfaces to an Ethernet channel.
unset hold ethernet *interface_id*	Delete a Layer 2 Ethernet interface from an Ethernet channel.
speed {**10** | **100** | **1000** | **auto**} **duplex** {**half** | **full** | **auto**}	Set link speed and duplex mode for Ethernet interfaces.
flow control {**on** | **off**}	Enable or disable flow control for an Ethernet interface.
show interface [**brief**]	Display the information about all interfaces.
show interface ethernet [*interface_id* | **brief**]	Display information about Ethernet interfaces.

4.2.2.2 Layer 3

1. Choose **Network > Interfaces**.
2. Click corresponding to the Ethernet interface. Set its work mode, MTU value, and set the interface as a management interface.



3. Configure IPv4 address (Static IP):

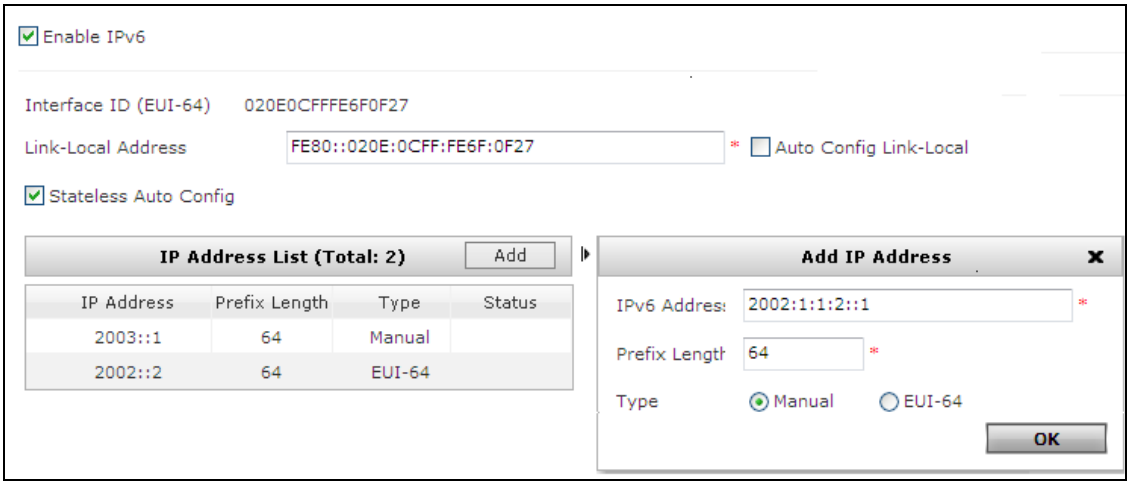


Primary indicates the IP address is preferably used as primary IP address.

4. Configure IPv4 address (DHCP):

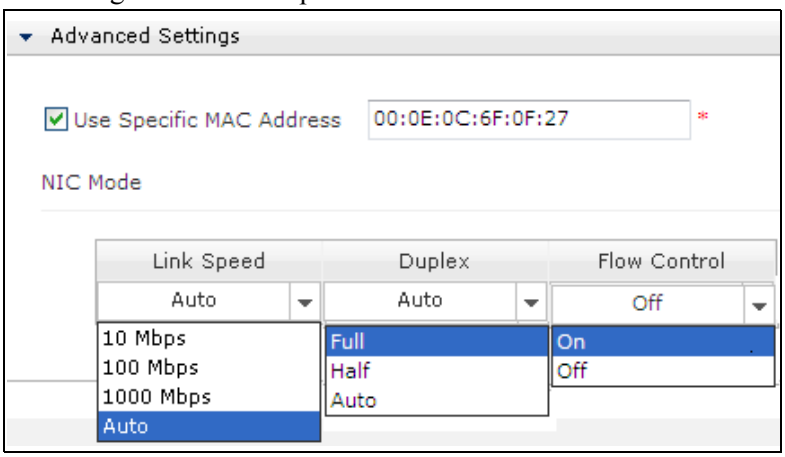
- Check **Enable DNS Proxy** to automatically add DNS proxy for a DHCP client interface.
- An interface allows up to 32 IPv4 addresses.

5. Configure IPv6 address:



- Link-local address is generated automatically by default. When you uncheck **Auto Config Link Local**, you can specify a link-local address in the corresponding text box.
- Check **Stateless Auto Config**, the IPv6 address is automatically generated through stateless address autoconfiguration.
- You can manually configure IPv6 addresses in **IP Address List**.
- FGX supports both autoconfiguration and manual configuration of IPv6 addresses at the same time.
- An interface allows up to 32 IPv6 addresses (including one link-local address and 31 global unicast addresses).
- Link-local addresses and addresses automatically configured in a stateless way cannot be used as primary IP addresses.

6. In **Advanced Settings**, check **Use Specific MAC Address** to change the MAC address and configure NIC mode parameters.



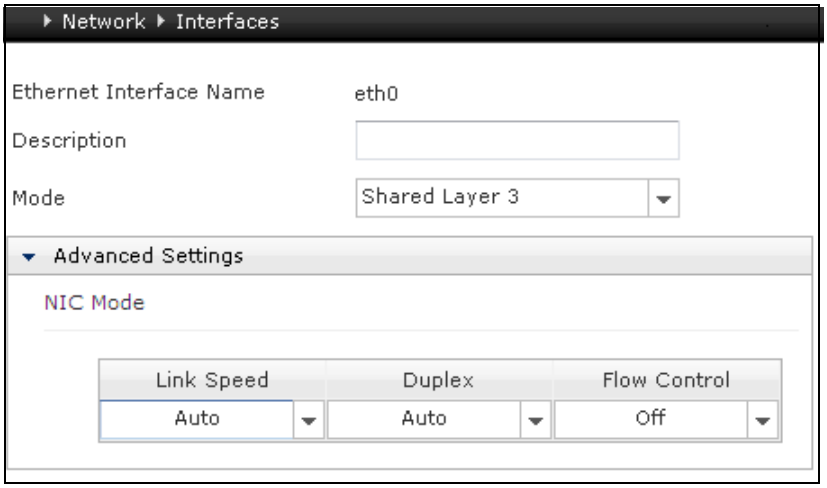
- By default, the system provides a specific MAC address.
- Only Ethernet interfaces have the NIC mode.

Table 89 Layer 3 Ethernet Interface Commands

working-type layer3-interface	Set an interface to work in Layer 3 mode.
management-only	Set a Layer 3 Ethernet interface as the dedicated management interface.
unset management-only	Unset the management function of a Layer 3 Ethernet interface.
mtu {*mtu_value* | **default**}	Set the MTU of a Layer 3 interface or shared Layer 3 interface.
ip address *ipv4 netmask* [**secondary**]	Assign an IPv4 address to a specified Layer 3 interface or shared Layer 3 interface.
unset ip address [*ipv4*]	Delete the IPv4 addresses from a specified Layer 3 interface or shared Layer 3 interface.
dhcp client	Set a Layer 3 or shared Layer 3 interface as the DHCP client. The interface can then automatically obtain an IP address dynamically assigned by the DHCP server.
unset dhcp client	Delete DHCP client configuration.
dhcp update ip address	Obtain a new dynamically assigned IP address.
dhcp enable-dns-proxy	Enable the function of automatically adding DNS proxy for a DHCP client interface working in IPv4 mode.
unset dhcp enable-dns-proxy	Disable the function of automatically adding DNS proxy for a DHCP client interface working in IPv4 mode.
ipv6 enable	Enable IPv6 on a specified Layer 3 interface or shared Layer 3 interface.
unset ipv6 enable	Disable IPv6 on a specified Layer 3 interface or shared Layer 3 interface.
ipv6 address {*ipv6* | **auto**} **link-local**	Set a link-local address for a specified Layer 3 interface or shared Layer 3 interface.
ipv6 address autoconfig	Enable the stateless address autoconfiguration for a specified Layer 3 interface or shared Layer 3 interface.
unset ipv6 address autoconfig	Disable the function of stateless address autoconfiguration for a specified Layer 3 interface or shared Layer 3 interface.
ipv6 address {*ipv6* | *ipv6/prefix*} [**eui-64**]	Manually add ULAs (Unique Local Addresses)/global unicast addresses for a specified Layer 3 interface or shared Layer 3 interface.
unset ipv6 address	Delete ULAs/global unicast addresses from a specified Layer 3 interface or shared Layer 3 interface.
default mac	Obtain the default MAC address of an Ethernet interface, an Ethernet channel, a VLAN, or a redundant interface.
mac address *mac_address*	Change the MAC address of an Ethernet interface, an Ethernet channel, a VLAN, or a redundant interface.

4.2.2.3 Shared Layer 3

1. Choose **Network > Interfaces**.
2. Click corresponding to the Ethernet interface and configure as follows:



- Ethernet interfaces, Ethernet channels, and redundant interfaces can work in shared Layer 3 mode.
- Before you add an address for a shared Layer 3 interface, you need to assign the interface to a Vsys first.

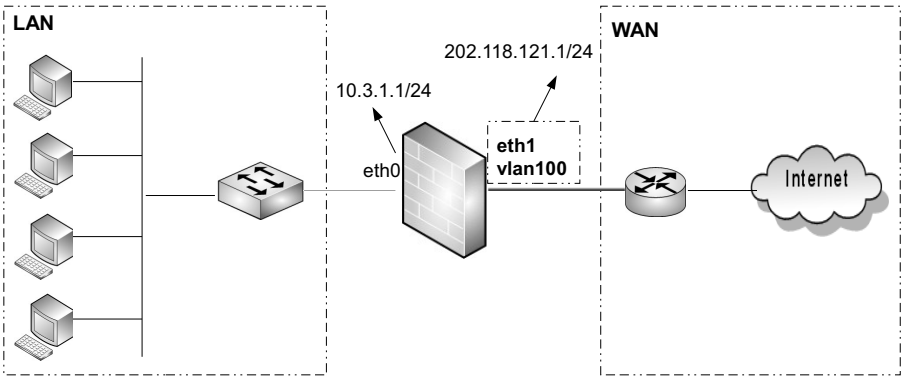
Table 90 Shared Layer 3 Ethernet Interface Commands

working-type layer3-shared-interface	Set an interface to work in shared Layer 3 mode.
speed {**10** | **100** | **1000** | **auto**} **duplex** {**half** | **full** | **auto**}	Set link speed and duplex mode for Ethernet interfaces.
flow control {**on** | **off**}	Enable or disable flow control for an Ethernet interface.

4.2.3 Example: Ethernet Interface

A company needs to access the Internet through FGX.

Figure 8 Interface Configuration

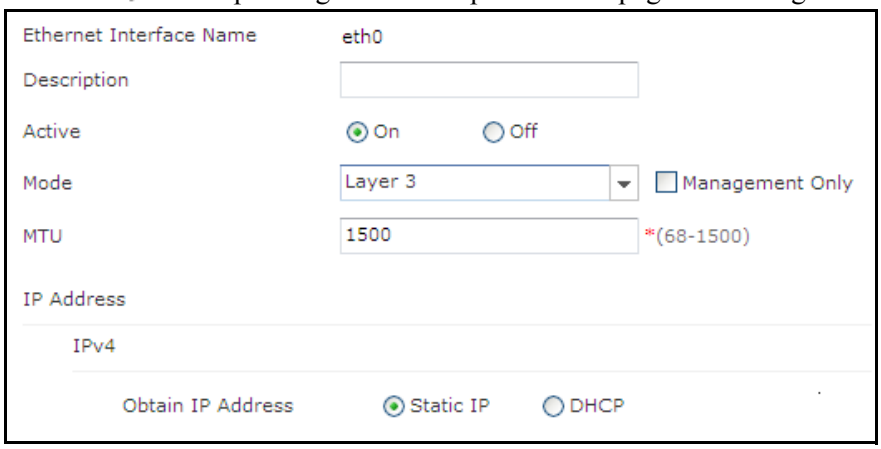


This example shows how to:

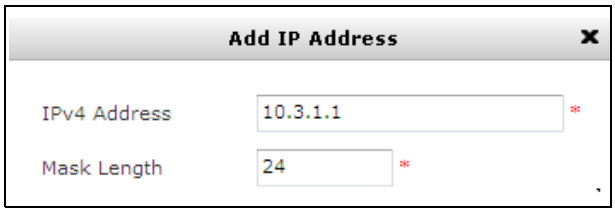
- Configure eth0 to work in Layer 3 mode and configure its IP address 10.3.1.1/24.
- Create vlan100 comprising the Layer 2 interface eth1 and configure its IP address 202.118.121.1/24.

WebUI

1. Choose **Network > Interfaces**.
2. Click corresponding to eth0 to open the Edit page and configure as follows:

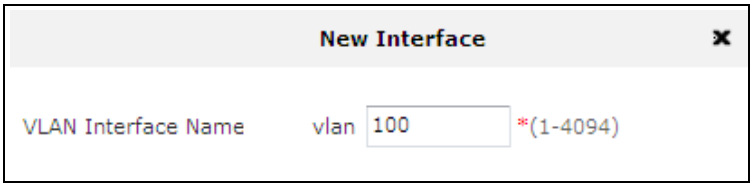


3. In **IP Address List**, click **Add** to add an IP address.

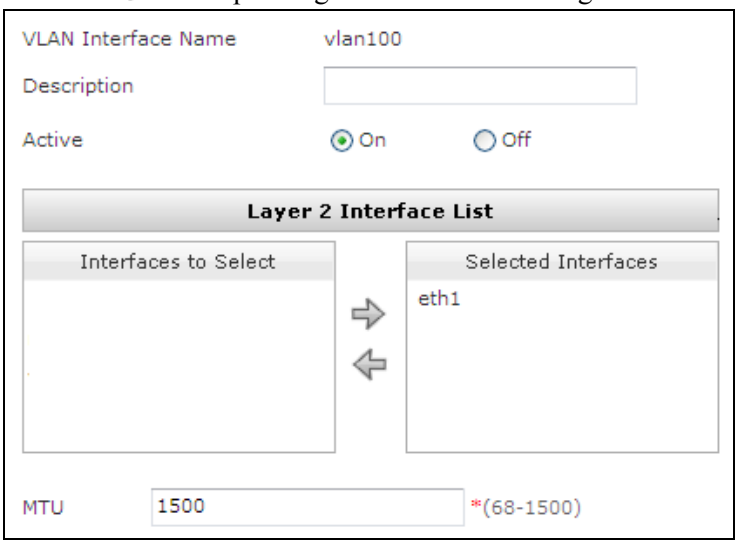


4. Click **OK**.

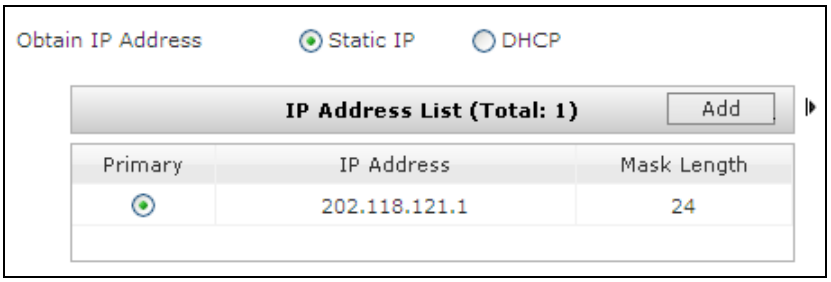
5. Click **New** and choose **VLAN** to create a VLAN interface.



6. Click corresponding to vlan100 and configure as follows:



7. Click **Add** in **IP Address List** to configure the IP address.



8. Click **OK**.
9. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] working-type layer3-interface
FGX@root-system-if-eth0] ip address 10.3.1.1 255.255.255.0
FGX@root-system-if-eth0] exit
FGX@root-system] vlan 100
FGX@root-system-vlan100] hold ethernet 1
FGX@root-system-vlan100] ip address 202.118.121.1 255.255.255.0
FGX@root-system-vlan100] end
FGX@root> save config
```

4.3 Ethernet Channel

- 4.3.1 Overview
- 4.3.2 Basic configuration steps

4.3.1 Overview

An Ethernet channel (or a channel interface) is a logical aggregation of two or more Ethernet interfaces. Using channels increases bandwidth and improves fault tolerance. FGX supports up to eight Ethernet channels.

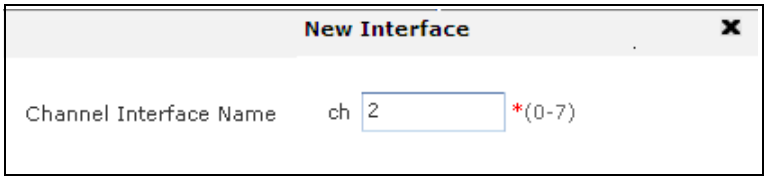
- These Ethernet interfaces share the same MAC address and function as one interface.
- The data rate of a channel is the total rate of all the Ethernet interfaces within the channel.
- When one interface fails, other Ethernet interfaces in a channel can take over the work.
- You can assign a Layer 3 Ethernet channel to a single Vsys.

4.3.2 Basic configuration steps

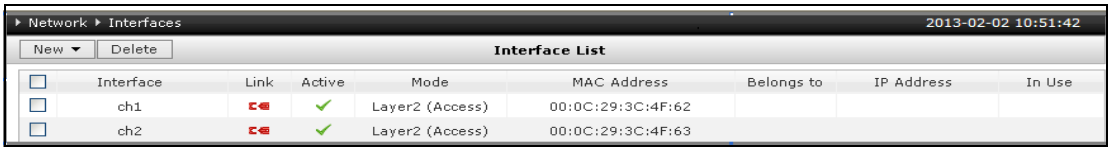
- 4.3.2.1 Layer 2.
- 4.3.2.2 Layer 3.
- 4.3.2.3 Shared Layer 3.

4.3.2.1 Layer 2

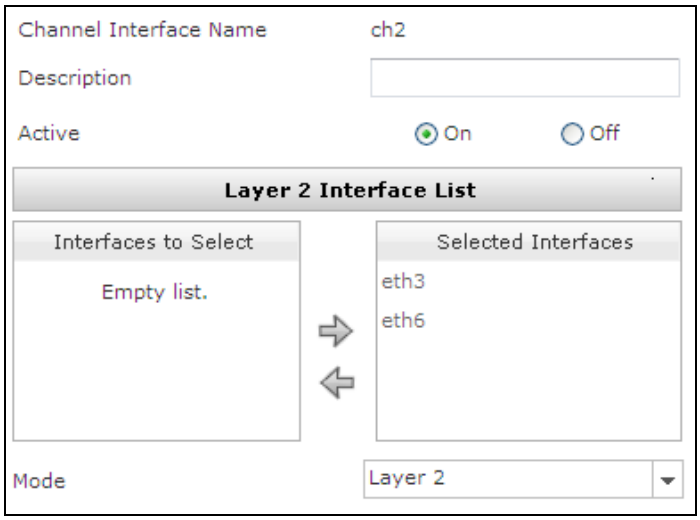
1. Choose **Network > Interfaces**.
2. Click **New**.



3. View the Ethernet channel.



4. Click corresponding to the Ethernet channel and assign unused Layer 2 Ethernet interfaces to it:



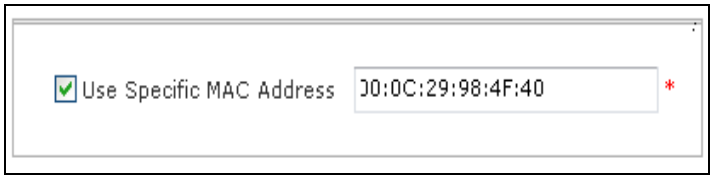
5. Layer 2 advanced settings (access and trunk mode) and MAC address setting are the same as Ethernet interfaces. Go to 4.2.2.1 Layer 2 for steps 2-3.

Table 91 Layer 2 Channel Interface Commands

channel *channel_id*	Create an Ethernet channel or enter the configuration mode of a specified Ethernet channel.
unset channel *channel_id*	Delete a specified Ethernet channel.
show interface channel [*channel_id* | **brief**]	Display information about Ethernet channels.
shutdown	Disable an interface.
unset shutdown	Enable an interface.
hold ethernet *interface_id*	Assign Layer 2 Ethernet interfaces to an Ethernet channel.
unset hold ethernet *interface_id*	Delete a Layer 2 Ethernet interface from an Ethernet channel.
working-type layer2-interface	Set an interface to work in Layer 2 mode.

4.3.2.2 Layer 3

1. Choose **Network > Interfaces**.
2. Click corresponding to the Ethernet channel. Configure IPv4 address (Static IP and DHCP) and IPv6 address the same as for Ethernet interfaces. Go to 4.2.2.2 Layer 3 for steps 3-5.
3. In **Advanced Settings**, specify a MAC address instead of using the default address:



For IPv4 and IPv6 CLI configurations, see Layer 3 Ethernet Interface Commands.

4.3.2.3 Shared Layer 3

1. Choose **Network > Interfaces**.
2. Click corresponding to the Ethernet channel. Assign unused Layer 2 Ethernet interfaces to it and set the work mode:

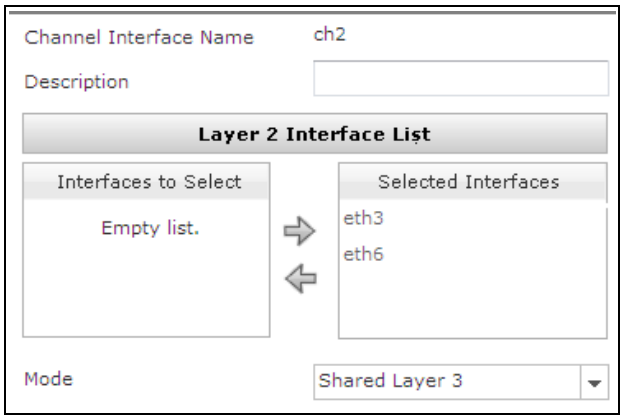


Table 92 Shared Layer 3 Ethernet Channel Commands

hold ethernet *interface_id*	Assign Layer 2 Ethernet interfaces to an Ethernet channel.
unset hold ethernet *interface_id*	Delete a Layer 2 Ethernet interface from an Ethernet channel.
working-type layer3-shared-interface	Set an interface to work in shared Layer 3 mode.

4.4 Redundant Interface

- 4.4.1 Overview
- 4.4.2 Basic configuration steps

4.4.1 Overview

A redundant interface is a logical interface formed by binding two Ethernet interfaces together to achieve redundancy and high reliability at the interface level. FGX supports up to four redundant interfaces.

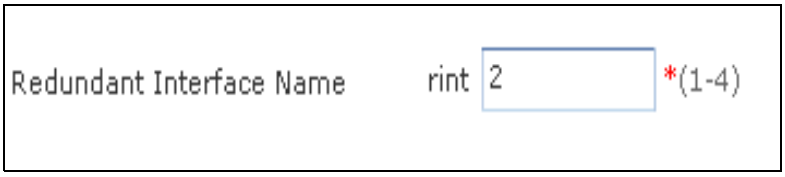
- One Ethernet interface acts as the primary interface, and the other as the backup.
- No data passes through the backup interface.
- When the primary one fails, the backup one becomes the primary interface. A failover is performed automatically.
- When one Ethernet interface is deleted, the other one is deleted simultaneously.
- You can assign a Layer 3 redundant interface to a single Vsys.

4.4.2 Basic configuration steps

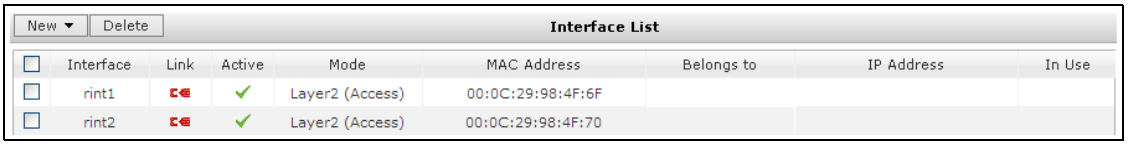
- 4.4.2.1 Layer 2.
- 4.4.2.2 Layer 3.
- 4.4.2.3 Shared Layer 3.

4.4.2.1 Layer 2

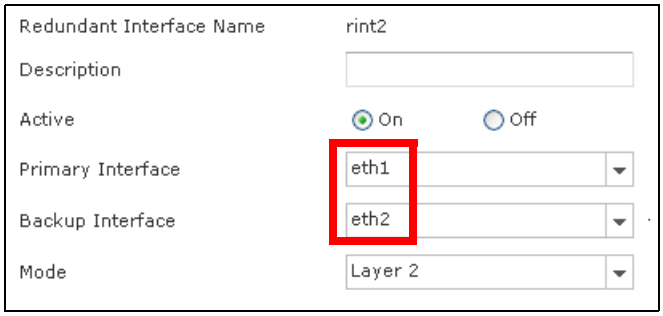
1. Choose **Network > Interfaces**.
2. Click **New**.



3. View the redundant interface.

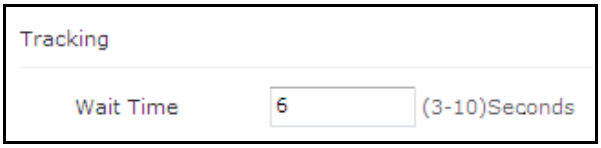


4. Click corresponding to the redundant interface. Assign it with two unused Layer 2 Ethernet interfaces as primary and backup and set the work mode as Layer 2.



You must select both Ethernet interfaces or none.

5. Set the wait time, the length of time before a redundant interface recovers from failure.



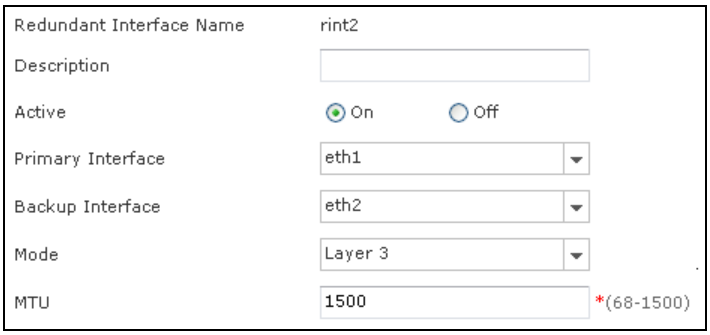
6. Other Layer 2 advanced settings (access and trunk mode) and MAC address setting are the same as Ethernet interfaces. Go to 4.2.2.1 Layer 2 for steps 2-3.

Table 93 Layer 2 Redundant Interface Commands

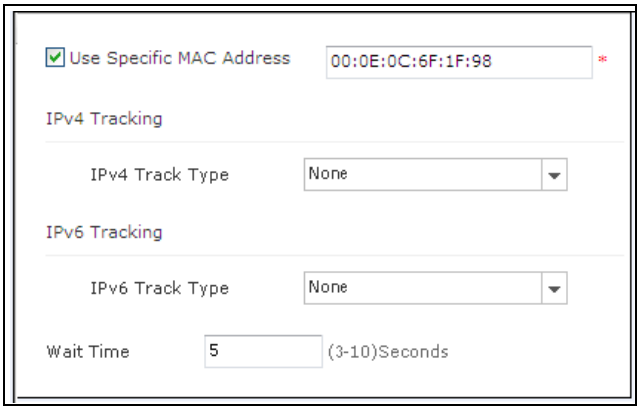
rint *rint_id*	Create a redundant interface or enter the configuration mode of a specified redundant interface.
unset rint *rint_id*	Delete a specified redundant interface.
show interface rint [*rint_id* | **brief**]	Display information about redundant interfaces.
shutdown	Disable an interface.
unset shutdown	Enable an interface.
hold ethernet primary *interface_id* **secondary** *interface_id*	Set a primary and a backup Ethernet interface for a redundant interface.
unset ethernet	Delete the primary and backup interfaces of a redundant interface.
switch	Switch the primary and backup interfaces of a redundant interface.
working-type layer2-interface	Set an interface to work in Layer 2 mode.
wait-time *wait_time*	Set the wait time for failure recovery of a redundant interface.

4.4.2.2 Layer 3

1. Choose **Network > Interfaces.**
2. Click corresponding to the redundant interface. Assign primary and backup interfaces to it and set the work mode and MTU value.



3. Configure IPv4 address (Static IP and DHCP) and IPv6 address the same as for Ethernet interfaces. Go to 4.2.2.2 Layer 3 for steps 3-5.
4. In **Advanced Settings**, change the MAC address and configure tracking:



Before specifying an IPv6 track type, you need to enable IPv6 on the redundant interface by checking **Enable IPv6**.

Table 94 Layer 3 Redundant Interface Commands

hold ethernet primary *interface_id* **secondary** *interface_id*	Set a primary and a backup Ethernet interface for a redundant interface.
unset ethernet	Delete the primary and backup interfaces of a redundant interface.
working-type layer3-interface	Set an interface to work in Layer 3 mode.
mtu {*mtu_value* | **default**}	Set the MTU of a Layer 3 interface or shared Layer 3 interface.
default mac	Obtain the default MAC address of an Ethernet interface, an Ethernet channel, a VLAN, or a redundant interface.

Table 94 Layer 3 Redundant Interface Commands (*continued*)

mac address *mac_address*	Change the MAC address of an Ethernet interface, an Ethernet channel, a VLAN, or a redundant interface.
monitor type	Set an IPv4 track type for a specified Layer 3 or shared Layer 3 redundant interface.
unset monitor type	Delete the IPv4 track type of a specified Layer 3 or shared Layer 3 redundant interface.
monitor typev6	Set the IPv6 track type for a specified Layer 3 or shared Layer 3 redundant interface.
unset monitor typev6	Delete the IPv6 track type of a specified Layer 3 or shared Layer 3 redundant interface.
wait-time *wait_time*	Set the wait time for failure recovery of a redundant interface.

For IPv4 and IPv6 CLI configurations, see Layer 3 Ethernet Interface Commands.

4.4.2.3 Shared Layer 3

1. Choose **Network > Interfaces**.
2. Click corresponding to the redundant interface. Assign unused Layer 2 Ethernet interfaces to it and set the work mode:

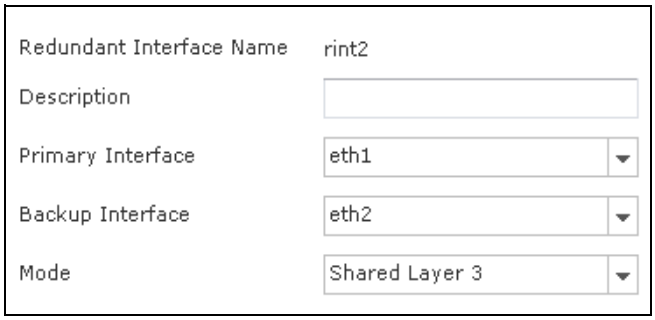


Table 95 Shared Layer 3 Redundant Interface Commands

hold ethernet primary *interface_id* **secondary** *interface_id*	Set a primary and a backup Ethernet interface for a redundant interface.
unset ethernet	Delete the primary and backup interfaces of a redundant interface.
working-type layer3-shared-interface	Set an interface to work in shared Layer 3 mode.

4.5 Virtual Interface

- 4.5.1 Overview
- 4.5.2 Basic configuration steps

4.5.1 Overview

Virtual interfaces connect to virtual networks, enabling different Vsys to communicate with each other independently of Ethernet interfaces. For more information, see 13.1.2. Vnet. FGX supports up to 1,023 virtual interfaces. You can assign a Layer 3 virtual interface to a single Vsys. Virtual interfaces are used in the way similar to Ethernet interfaces, but they cannot be:

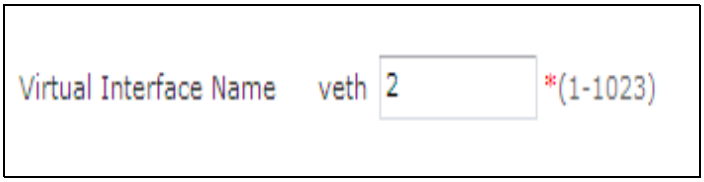
- Assigned to an Ethernet channel or redundant interface;
- Used as HA synchronization interfaces;
- Set in Trunk mode.

4.5.2 Basic configuration steps

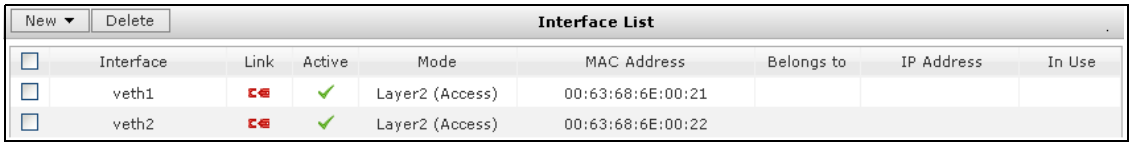
- 4.5.2.1 Layer 2.
- 4.5.2.2 Layer 3.

4.5.2.1 Layer 2

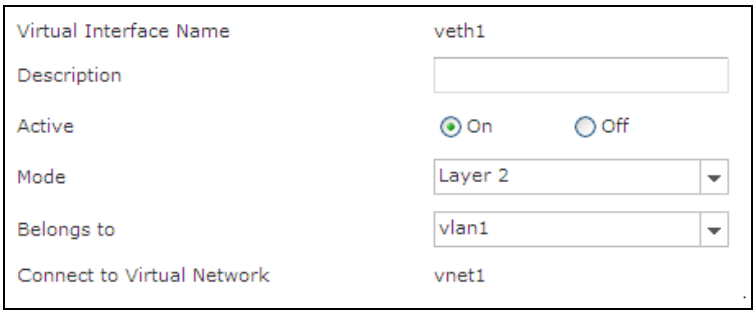
1. Choose **Network > Interfaces.**
2. Click **New**.



3. View the Layer 2 virtual interface.



4. Click corresponding to the virtual interface. Set the work mode and specify the VLAN it belongs to:



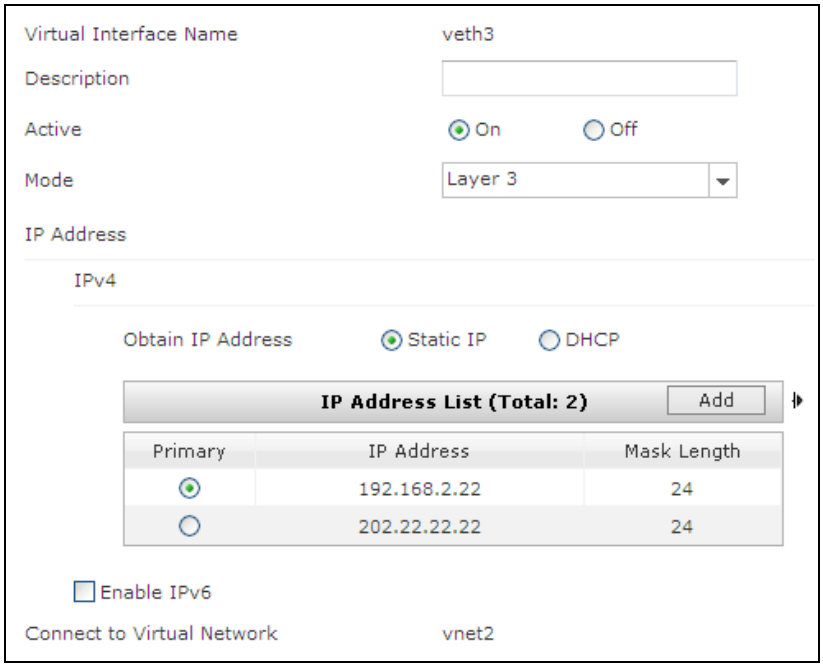
When you choose **System > Virtual Systems > Virtual Networks** and assign veth1 to the virtual network vnet1, the system automatically displays the result shown as above.

Table 96 Layer 2 Virtual Interface Commands

veth *veth_id*	Create a virtual interface or enter the configuration mode of a specified virtual interface.
unset veth *veth_id*	Delete a specified virtual interface.
show interface veth [*veth_id* | **brief**]	Display information about virtual interfaces.
shutdown	Disable an interface.
unset shutdown	Enable an interface.
working-type layer2-interface	Set an interface to work in Layer 2 mode.
port access vlan *vlan_id*	Assign a Layer 2 interface to a specified VLAN.
unset port access vlan	Delete a VLAN to which a Layer 2 interface belongs.

4.5.2.2 Layer 3

1. Choose **Network > Interfaces**.
2. Click corresponding to the virtual interface and configure as follows:



- A virtual interface cannot work in shared Layer 3 mode.
- A virtual interface has no MTU value.
- Configuration of IPv4 address (Static IP and DHCP) and IPv6 address is the same as Ethernet interfaces. Go to 4.2.2.2 Layer 3 for steps 3-5.
- For CLI configurations, see Layer 3 Ethernet Interface Commands.

4.6 VLAN Interface

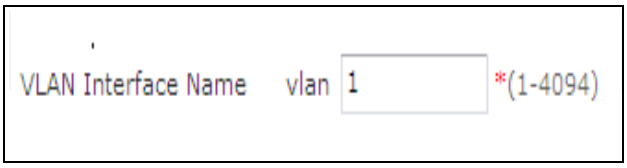
- 4.6.1 Overview
- 4.6.2 Basic configuration steps
- 4.6.3 Example: VLAN Interface

4.6.1 Overview

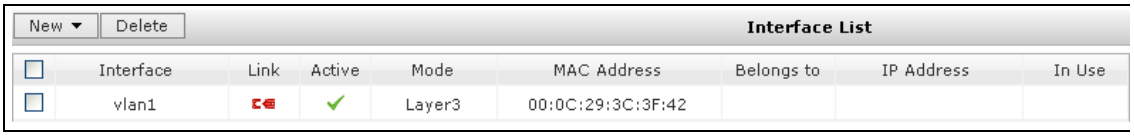
A VLAN groups hosts into a broadcast domain regardless of the physical locations of the hosts. A VLAN interface acts as a VLAN holding Layer 2 interfaces. Members within a VLAN communicate with each other in Layer 2 switching mode, and members in different VLANs communicate in Layer 3 routing mode. FGX supports up to 4,094 VLAN interfaces.

4.6.2 Basic configuration steps

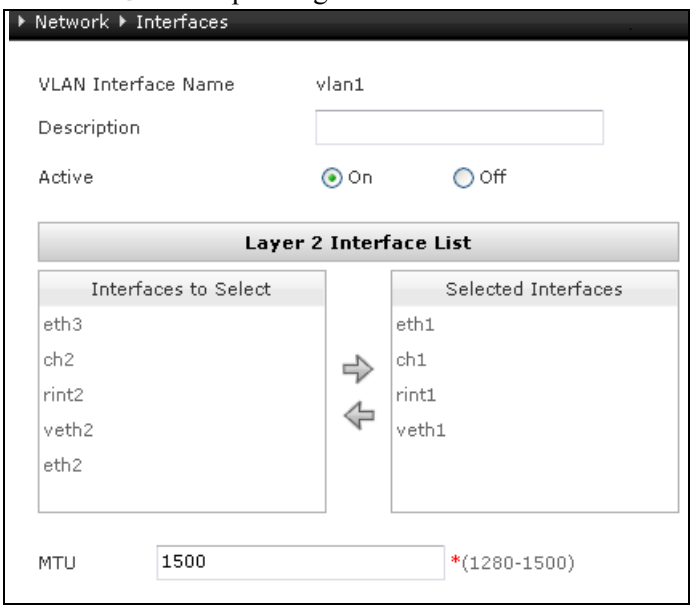
1. Choose **Network > Interfaces.**
2. Click **New**.



3. View the VLAN interface.



4. Click corresponding to the VLAN interface and assign unused Layer 2 interfaces to it:



- A VLAN interface can hold the following Layer 2 interfaces: Ethernet interfaces, Ethernet channels, redundant interfaces, and virtual interfaces.
- A VLAN interface works as a Layer 3 interface.

5. Configuration of IPv4 address (Static IP and DHCP) and IPv6 address is the same as Ethernet interfaces. Go to 4.2.2.2 Layer 3 for steps 3-5.
6. In **Advanced Settings**, specify a MAC address instead of using the default address:

Table 97 VLAN Interface Commands

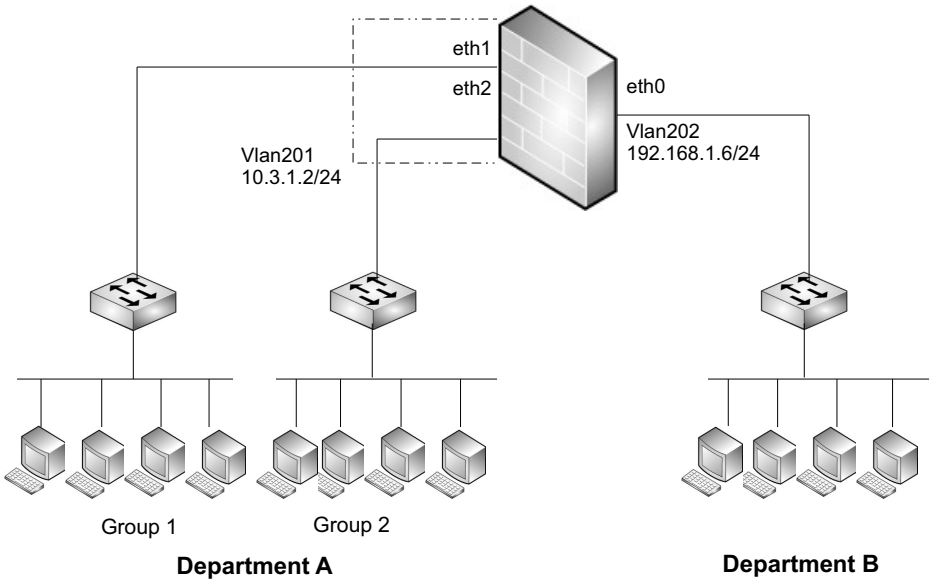
vlan *vlan_id*	Create a VLAN or enter the configuration mode of a specified VLAN.
unset vlan *vlan_id*	Delete a specified VLAN.
show interface vlan [*vlan_id* | **brief**]	Display information about VLANs.
shutdown	Disable an interface.
unset shutdown	Enable an interface.
hold ethernet, channel, rint, veth	Assign Layer 2 interfaces to a VLAN.
unset hold ethernet, channel, rint, veth	Delete a Layer 2 interface from a VLAN.
mtu {*mtu_value* | **default**}	Set the MTU of a Layer 3 interface or shared Layer 3 interface.
default mac	Obtain the default MAC address of an Ethernet interface, an Ethernet channel, a VLAN, or a redundant interface.
mac address *mac_address*	Change the MAC address of an Ethernet interface, an Ethernet channel, a VLAN, or a redundant interface.

For IPv4 and IPv6 CLI configurations, see Layer 3 Ethernet Interface Commands.

4.6.3 Example: VLAN Interface

There are two departments in a company, Department A and Department B. Department A is subdivided into two groups, Group 1 and Group 2. By dividing VLANs, employees within the same department can communicate with each other in Layer 2 switching mode, and those in different departments can communicate in Layer 3 routing mode.

Figure 9 VLAN Application



You need to set up a topology on FGX for the following configurations:

- Create vlan201 and vlan202.
- Allocate eth1 and eth2 to vlan201.
- Allocate eth0 to vlan202.
- Set 10.3.1.2/24 as the IP address for vlan201.
- Set 192.168.1.6/24 as the IP address for vlan202.

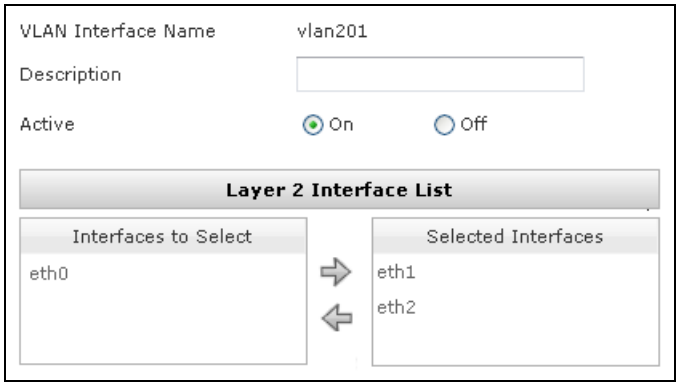
This example shows how to:

- 1. Configure vlan201
- 2. Configure vlan202

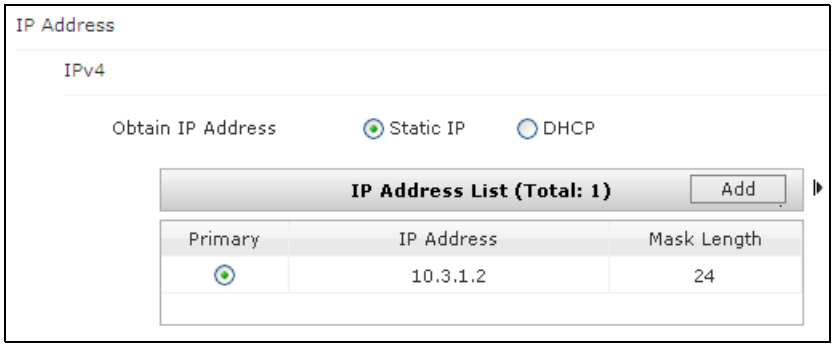
1. Configure vlan201

1. Choose **Network > Interfaces**.
2. Click **New**.

3. Click corresponding to vlan201 and configure as follows:



4. Configure the IP address:



5. Click **OK**.
6. Click .

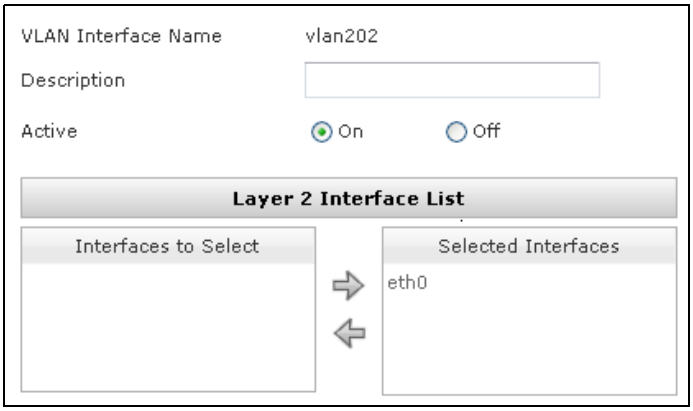
CLI

```
FGX@root> configure mode
FGX@root-system] vlan 201
FGX@root-system-vlan201] hold ethernet 1,2
FGX@root-system-vlan201] ip address 10.3.1.2 255.255.255.0
FGX@root-system-vlan201] exit
FGX@root-system-vlan201] end
FGX@root> save config
```

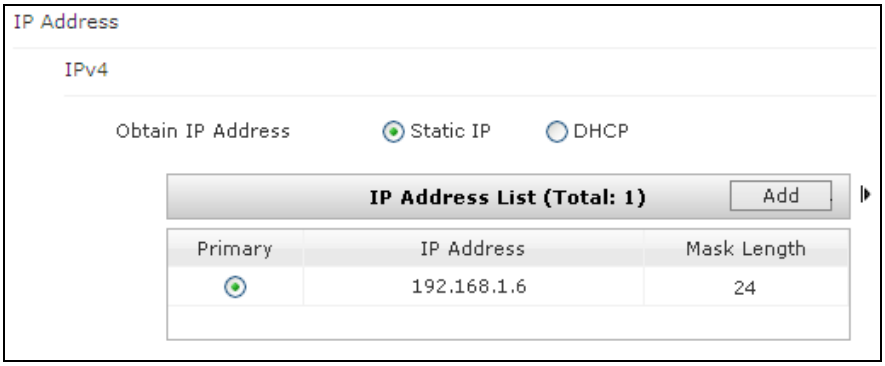
2. Configure vlan202

1. Choose **Network > Interfaces**.
2. Click **New**.

3. Click corresponding to vlan202 and configure as follows:



4. Configure the IP address:



5. Click **OK**.
6. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] vlan 202
FGX@root-system-vlan202] hold ethernet 0
FGX@root-system-vlan202] ip address 192.168.1.6 255.255.255.0
FGX@root-system-vlan202] exit
FGX@root-system-vlan202] end
FGX@root> save config
```

4.7 Loopback Interface

- 4.7.1 Overview
- 4.7.2 Basic configuration steps

4.7.1 Overview

A loopback interface is a logical Layer 3 interface. FGX supports up to 1,023 loopback interfaces.

The link state of a loopback interface always stays up unless the interface is disabled or the device to which the interface belongs goes down.

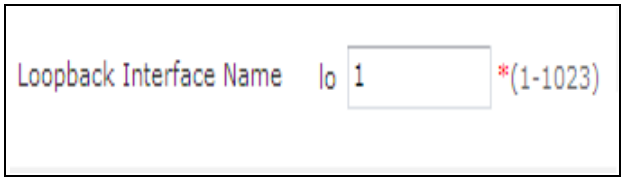
- You can keep track of the state of a device by monitoring the state of its loopback interfaces. For example, a network manager can use the SNMP protocol to obtain FGX state and monitoring information. For more information, see 3.12 SNMP.
- You can manage FGX using the loopback interface configured with an IP address and required routing.
- Access through loopback interfaces is controlled by access control policies.

Note the following when applying loopback interfaces in Vsys:

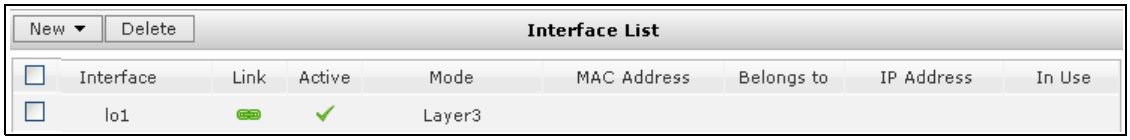
- Vsys administrators are able to create and configure loopback interfaces in their own Vsys.
- Loopback interfaces in different Vsys can have the same name.
- When a Vsys is deleted, its loopback interfaces are deleted simultaneously.
- Loopback interfaces created in one Vsys cannot be assigned to another Vsys.

4.7.2 Basic configuration steps

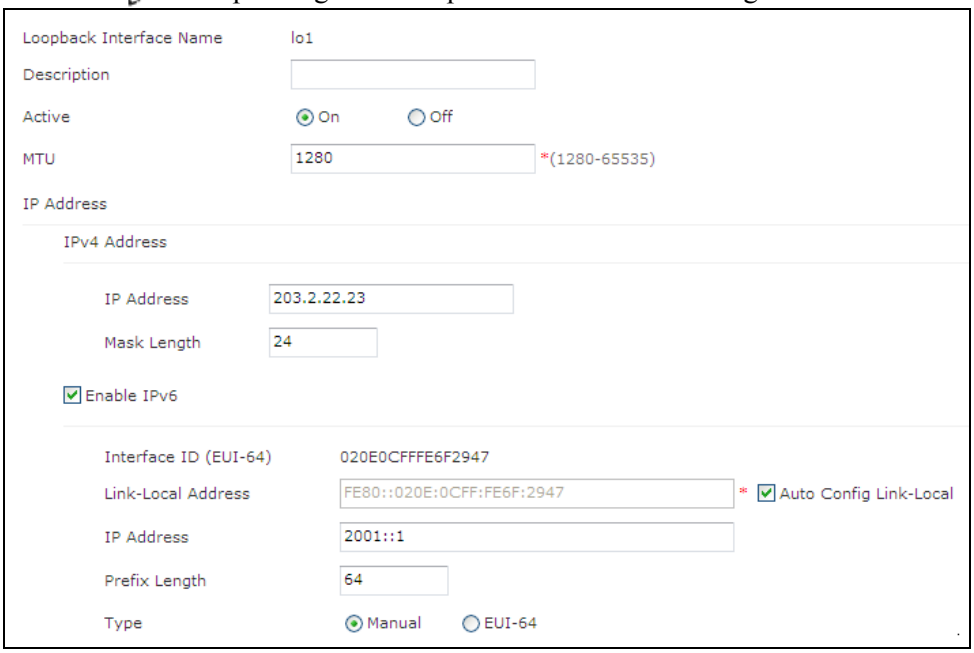
1. Choose **Network > Interfaces**.
2. Click **New**.



3. View the loopback interfaces.



4. Click corresponding to the loopback interface and configure as follows:



- You can configure only one IPv4 address and only one IPv6 address for a loopback interface.
- The format of the IPv4 address is [1-223].[0-225].[0-225].[0-225]. You cannot enter 127.0.0.0-127.255.255.255 or 192.168.255.254.
- A loopback interface does not support IPv6 address autoconfiguration except for the link-local address.

Table 98 Loopback Interface Commands

loopback *lo_id*	Create a loopback interface or enter the configuration mode of a specified loopback interface.
unset loopback *lo_id*	Delete a specified loopback interface.
show interface loopback [*lo_id* | **brief**]	Display information about loopback interfaces.
shutdown	Disable an interface.
unset shutdown	Enable an interface.
mtu {*mtu_value* | **default**}	Set the MTU of a Layer 3 interface or shared Layer 3 interface.

For IPv4 and IPv6 CLI configurations, see Layer 3 Ethernet Interface Commands.

4.8 PPPoE Interface

- 4.8.1 Overview
- 4.8.2 Basic configuration steps
- 4.8.3 Parameter reference

4.8.1 Overview

A PPPoE interface is a logical Layer 3 interface. FGX supports up to eight PPPoE interfaces.

- A PPPoE interface binds a Layer 2 Ethernet or redundant interface to it;
- One PPPoE interface can use only one Layer 2 Ethernet or redundant interface;
- Multiple PPPoE interfaces can use the same Layer 2 Ethernet or redundant interface.

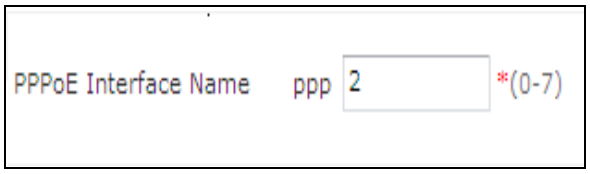
FGX can work as a PPPoE client to establish a PPP connection with the ISP through PPPoE dial-up. The FGX PPPoE interface can obtain local and remote IP addresses as well as DNS server IP addresses.

FGX supports IPv4-based PPPoE (PPPoEv4) and IPv6-based PPPoE (PPPoEv6).

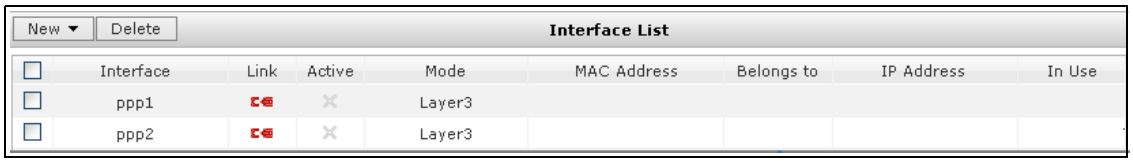
- A PPPoE interface can work as a PPPoEv6 client obtaining prefix information through DHCPv6 prefix delegation to form IPv6 addresses.
- One Layer 2 Ethernet interface or redundant interface can be configured for both PPPoEv4 and PPPoEv6 client interfaces simultaneously. For more information, see Table 100 PPPoE Interface Attributes.

4.8.2 Basic configuration steps

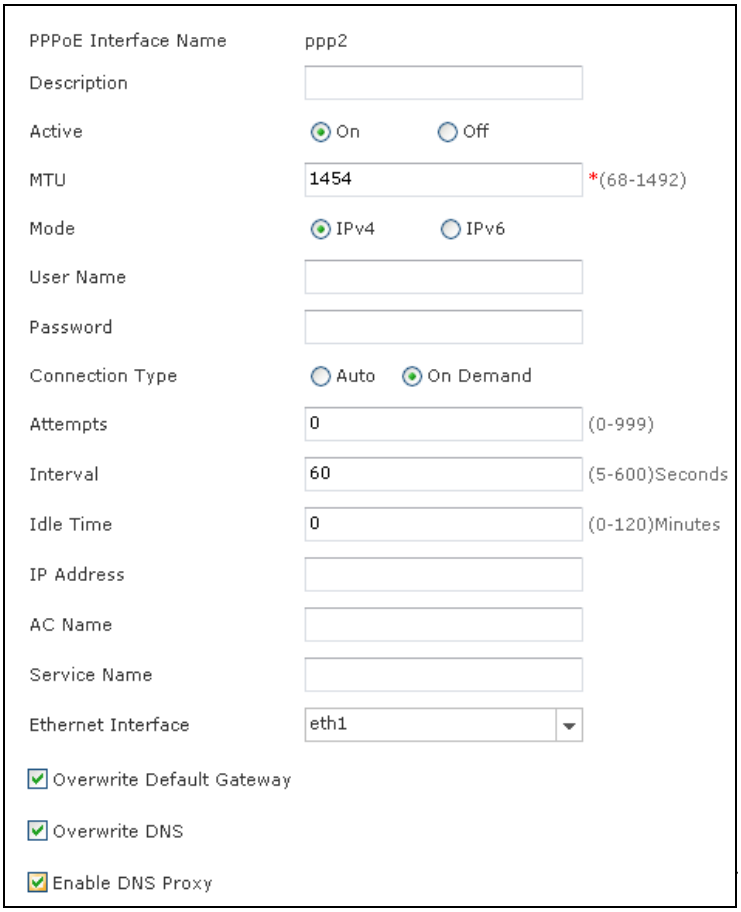
1. Choose **Network > Interfaces**.
2. Click **New**.



3. View the PPPoE interface.



4. Click corresponding to the PPPoE interface and configure as follows:



A PPPoE interface obtains the IPv6 address only through DHCPv6.

Table 99 PPPoE Interface Commands

pppoe *pppoe_id*	Create a PPPoE interface or enter the configuration mode of a specified PPPoE interface.
unset pppoe *pppoe_id*	Delete a specified PPPoE interface.
show interface pppoe [*pppoe_id* | **brief**]	Display information about PPPoE interfaces.
active {**on** | **off**}	Enable or disable a PPPoE interface.
mtu {*mtu_value* | **default**}	Set the MTU of a Layer 3 or shared Layer 3 interface.
mode {**ipv4** | **ipv6**}	Set the working type of PPPoE interfaces.
username *user_name* **password** *passwd*	Configure a dialup user.
unset user	Delete a dialup user.
connection-type	Set the dialup connection types.
connection-type ondemand idle	Set the length of idle time (no data transmission) that will cause a disconnection.

Table 99 PPPoE Interface Commands (*continued*)

ip address *ipv4 netmask* [**secondary**]	Assign an IPv4 address to a specified Layer 3 or shared Layer 3 interface.
unset ip address [*ipv4*]	Delete the IPv4 addresses from a Layer 3 or shared Layer 3 interface.
interface-id *if_id*	Set an interface ID for a specified PPPoE interface.
unset interface-id	Delete the interface ID of a specified PPPoE interface.
acname *ac_name*	Set an AC name.
unset acname	Delete an AC name.
servicename *service_name*	Set a service name.
unset servicename	Delete a service name.
hold {**ethernet** *interface_id* | **rint** *rint_id*}	Assign a Layer 2 Ethernet interface or Layer 2 redundant interface to a PPPoE interface.
unset hold	Delete a Layer 2 interface from a PPPoE interface.
overwrite-default-gateway	Enable the function of overwriting the default gateway for a PPPoE interface.
unset overwrite-default-gateway	Disable the function of overwriting the default gateway for a PPPoE interface.
overwrite-dns	Enable the function of overwriting the system DNS for a PPPoE interface working in IPv4 mode.
unset overwrite-dns	Disable the function of overwriting the system DNS for a PPPoE interface working in IPv4 mode.
enable-dns-proxy	Enable the function of automatically adding DNS proxy for a PPPoE interface working in IPv4 mode.
unset enable-dns-proxy	Disable the function of automatically adding DNS proxy for a PPPoE interface working in IPv4 mode.
dhcp-prefix-delegate	Enable the function of automatically triggering DHCPv6 client requests for a PPPoE interface.
unset dhcp-prefix-delegate	Disable the function of automatically triggering DHCPv6 client requests for a PPPoE interface.

4.8.3 Parameter reference

Table 100 PPPoE Interface Attributes

Parameter	Description
Active	The active state of a PPPoE interface. • **On—**enabled. • **Off—**disabled (default).
MTU	The maximum transmission unit. • In IPv4, 68-1,492 bytes. • In IPv6, 1,280-1,492 bytes. The default MTU is 1,454 bytes.
Mode	The working modes, IPv4 (default) and IPv6.
User Name	The name of a PPPoE dial-up user, 0-127 characters. Can be digits, letters, and the following special characters: `~!@#$%^&*()_+-=[]{}|;:"<>,./?. It must begin with a digit or letter.
Password	The password, 0-127 UTF-8 characters except spaces.
Connection Type	Dial-up connection types: • **Auto (default)—**automatically connects to the ISP. When the connection is disconnected, FGX requires an auto reconnection. • **On Demand—**connects to the ISP only upon access request.
Attempts	Maximum number of consecutive failed dial-up connection attempts. 0-999. 0 = no limit (default).
Interval	The length of time between two dial-up connections. 5-600 seconds, default 60.
Idle Time	Length of idle time (no data transmission; 0-120 mins) that will cause a disconnect. 0 = permanent connection (default). Can be configured only when the connection type is On Demand.
IP Address	An IPv4 address configured on a PPPoE interface for PPPoE communication. The format is [1-223].[0-225].[0-225].[0-225]. You cannot enter 127.0.0.0-127.255.255.255 or 192.168.255.254. Only for IPv4 mode.
Interface ID	A 64-bit manually configured interface ID. You need to configure this parameter only when the interface ID cannot be obtained through automatic PPPoE negotiation. Only for IPv6 mode.
AC Name	The brand, model, or serial number of the ADSL modem provided by the ISP, 0-127 UTF-8 characters except spaces and question marks. Normally you do not need to configure it.
Service Name	The name of the ISP or that of the service provided by the ISP, 0-127 UTF-8 characters except spaces and question marks. Normally you do not need to configure it.
Ethernet Interface	The interface used for receiving and sending data for PPPoE communication. It must be a Layer 2 Ethernet interface or redundant interface.
Overwrite Default Gateway	Send packets that should be sent to the default gateway to the PPPoE interface after PPPoE dial-up. Disabled by default.
Overwrite DNS	Overwrite the DNS server information configured on FGX DNS Host with that obtained from the ISP. Only for IPv4 mode. Disabled by default.
Enable DNS Proxy	The system automatically adds DNS proxy according to the DNS information obtained through the PPPoE dial-up interface. Only for IPv4 mode. Disabled by default.
DHCP-Prefix Delegation	The PPPoE interface working as a DHCPv6 client will automatically request a DHCPv6 server to delegate prefixes and other configuration parameters after successful PPPoE negotiation. Only for IPv6 mode. Disabled by default.

4.9 Tunnel Interface

- 4.9.1 Overview
- 4.9.2 Basic configuration steps
- 4.9.3 Parameter reference

4.9.1 Overview

A VPN tunnel is used as a logical Layer 3 interface to establish VPN communication.

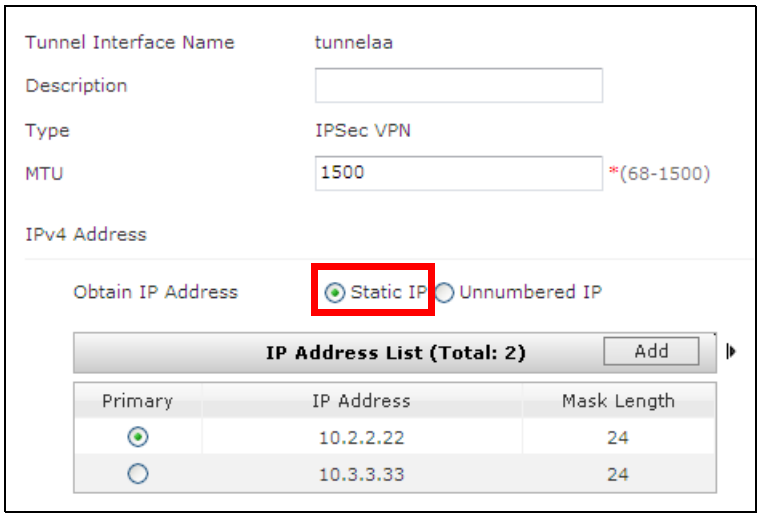
FGX does not support creating tunnel interfaces manually.

- When you create an IPSec VPN tunnel or SSL VPN tunnel, a tunnel interface is automatically created.
- When a tunnel is deleted, the corresponding interface is deleted as well.
- Tunnel interfaces cannot be deleted directly.
- When a tunnel interface is configured with a static IP address, the system automatically adds a directly connected route with the tunnel interface as the outgoing interface. The route can direct traffic into the corresponding IPSec or SSL VPN tunnel.

You can configure static IP addresses for tunnel interfaces or borrow IP addresses from other Layer 3 or shared Layer 3 interfaces. See Table 102 Tunnel Interface Attributes. With the IP borrowing mechanism, tunnel interfaces can perform routing without using up too many IP addresses. For more information, see Chapter 6, “Routing” and Chapter 11, “Virtual Private Network 2.”

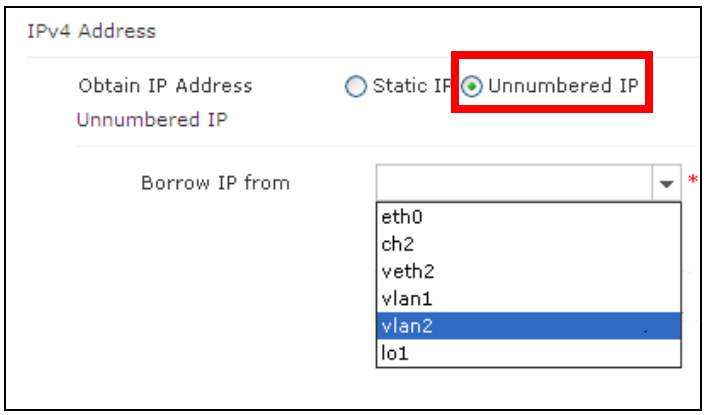
4.9.2 Basic configuration steps

1. Choose **Network > Interfaces**.
2. Click corresponding to the tunnel interface.
3. Configure IPv4 address (Static IP):



A tunnel interface does not support IPv6 address configurations.

4. Configure IPv4 address by borrowing IP addresses from other interfaces:



- A tunnel interface can borrow only one IP address at a time.
- When there are more than two IP addresses to borrow from one interface, the tunnel interface borrows the primary IP address. Fore more information, see Table 102 Tunnel Interface Attributes.

Table 101 Tunnel Interface Commands

tunnel *tunnel_id*	Enter the configuration mode of a specified VPN tunnel interface.
mtu {*mtu_value* | **default**}	Set the MTU of a Layer 3 interface or shared Layer 3 interface.
unnumbered *l3_interface_name*	Borrow IP addresses from other Layer 3 interfaces or shared Layer 3 interfaces except PPPoE interfaces.
unset unnumbered	Delete IP addresses which are borrowed from other Layer 3 interfaces or shared Layer 3 interfaces.
show interface tunnel [*tunnel_id* | **brief**]	Display information about VPN tunnel interfaces.

For IPv4 and IPv6 CLI configurations, see Layer 3 Ethernet Interface Commands.

4.9.3 Parameter reference

You can view and edit tunnel interfaces which are automatically generated when IPSec and SSL VPN tunnels are created.

Table 102 Tunnel Interface Attributes

Parameter	Description
Type	Tunnel interface type, including IPSec VPN and SSL VPN. You cannot change the type.
MTU	Maximum transmission unit. Tunnel interface MTU range is 68-1,500. The default MTU is 1,500.
Obtain IP Address	Methods of obtaining IP addresses, including: • **Static IP—**manually configure IP addresses for Layer 3 interfaces. You need to configure related settings in **IP Address List.** • **Unnumbered IP—**allows a tunnel interface to borrow an IP address from another Layer 3 interface to participate in routing. It can borrow from a VLAN interface, loopback interface, Layer 3 or shared Layer 3 Ethernet interface, Layer 3 or shared Layer 3 Ethernet channel, Layer 3 or shared Layer 3 redundant interface, and Layer 3 virtual interface.
IP Address List	Includes the following parameters: Primary, IP Address, and Mask Length. You can add up to 32 IPv4 addresses to the list. Primary indicates the primary IP address used by the interface.
In Use	Indicates a tunnel interface is being used by a manually configured route. You cannot delete a tunnel whose corresponding tunnel interface is being used by a manually configured route.

4.10 ARP

- 4.10.1 Overview
- 4.10.2 Basic configuration steps
- 4.10.3 Parameter reference

4.10.1 Overview

The Address Resolution Protocol (ARP) is used for resolving IP addresses at the network layer into MAC addresses at the data link layer. The ARP table on FGX is a cache table for Layer 3 data forwarding. It supports up to 32,768 ARP entries and the following types:

- Static ARP Entries—manually created and deleted.
- Dynamic ARP Entries—automatically created and deleted.
- Proxy ARP Entries—manually created and deleted.

4.10.2 Basic configuration steps

Table 103 ARP Commands

show arp [**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id* **|** *ipv4*]	View the ARP entries of the current system.
show arp static	View static ARP entries.
show arp dynamic	View dynamic ARP entries.
show arp timeout	View the timeouts of dynamic ARP entries.
show arp proxy	View proxy ARP entries.
arp {**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*} *ipv4 mac_address*	Create a static ARP entry.
arp proxy {**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*} *ipv4 mac_address*	Create a proxy ARP entry.
unset arp *ipv4*	Delete the ARP entries of a specified IPv4 address.
unset arp static [**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*]	Delete static ARP entries.
unset arp dynamic [**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*]	Delete dynamic ARP entries.
unset arp proxy [**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*]	Delete proxy ARP entries.
arp {**vlan** *vlan_id* **| ethernet** *interface_id* **| channel** *channel_id* **| rint** *rint_id* **| veth** *veth_id*} **timeout** {*timeout_value* **| default**}	Edit timeouts of dynamic ARP entries.

4.10.3 Parameter reference

You can monitor the ARP table in the WebUI and configure it in the CLI. For more information, see 14.6 ARP.

Table 104 Parameters of the ARP Table

Parameter	Description
IP Address	The IP address of a destination host. It cannot be a loopback address, multicast address, broadcast address of a subnet, or limited broadcast address. The IP address in a static or proxy ARP entry cannot be 0.0.0.0 or 255.255.255.255 or the same as that of the interface corresponding to the entry.
MAC Address	The MAC address corresponding to an IP address. It cannot be a broadcast or multicast MAC address.
Type	The type of ARP entry: Static, Dynamic, and Proxy.
State	The state of an ARP entry. • **INCOMPLETE—**an ARP request has already been sent, but no reply has been received. • **REACHABLE—**an entry is available. • **STALE—**an entry is available, but its lifetime is running out. The entry needs to be renewed. • **FAILED—**an entry is unavailable. This state cannot be seen.
Lifetime (s)	The lifetime of a dynamic ARP entry, in seconds.
Interface	The Layer 3 interface corresponding to an entry. Interfaces include Layer 3 Ethernet interfaces, Layer 3 Ethernet channels, VLAN interfaces, shared Layer 3 interfaces, Layer 3 virtual interfaces, and Layer 3 redundant interfaces.

4.11 CAM

- 4.11.1 Overview
- 4.11.2 Basic configuration steps
- 4.11.3 Parameter reference

4.11.1 Overview

Content Addressable Memory (CAM) is high-speed memory that facilitates addressing. A CAM table is an address table for Layer 2 switching, recording the mapping relationship between MAC addresses and Layer 2 interfaces.

FGX supports up to 16,384 CAM entries and the following types:

- Local CAM Entries. A local CAM entry corresponds to the MAC address of a Layer 3 interface on FGX. The entry is created or deleted when a Layer 3 interface is created or deleted.
- Static CAM Entries—manually created and deleted CAM entries. Static CAM entries will never time out unless you manually delete them.
- Dynamic CAM Entries—learned dynamically. You can set timeouts. A dynamic entry is deleted when it times out.
- Multicast CAM Entries—used when FGX sends multicast packets within a VLAN.

4.11.2 Basic configuration steps

Table 105 CAM Commands

show cam-table [**vlan** *vlan_id* | *mac_address*]	View CAM entries.
show cam-table timeout	View the timeouts of dynamic CAM entries.
cam-table vlan *vlan_id* {**channel** *channel_id* | **ethernet** *interface_id* **| rint** *rint_id* **| veth** *veth_id*} *mac_address*	Create CAM entries.
unset cam-table *mac_address*	Delete the CAM entries of a specified MAC address.
unset cam-table static vlan *vlan_id* [*mac_address*]	Delete static CAM entries.
unset cam-table dynamic [**vlan** *vlan_id*]	Delete dynamic CAM entries.
cam-table timeout [**vlan** *vlan_id*] {*timeout_value* | **default**}	Edit timeouts of dynamic CAM entries.

4.11.3 Parameter reference

You can monitor the CAM table in the WebUI and configure it in the CLI. For more information, see 14.7 CAM.

Table 106 Parameters of the CAM Table

Parameter	Description
Destination Address	The MAC address to which a packet is sent. It cannot be 00:00:00:00:00:00 or FF:FF:FF:FF:FF:FF.
Address Type	The type of CAM entry: Local, Static, Dynamic, and Multicast.
Layer 3 Information	The VLAN corresponding to an entry.
Destination Port	Layer 2 interfaces. Static and dynamic entries correspond to a Layer 2 interface. Multicast entries correspond to a list of Layer 2 interfaces through which multicast packets are forwarded.
Timeout (sec)	The timeout of a dynamic CAM entry. 10-30,000 seconds. It is 300 seconds by default.

4.12 Zones

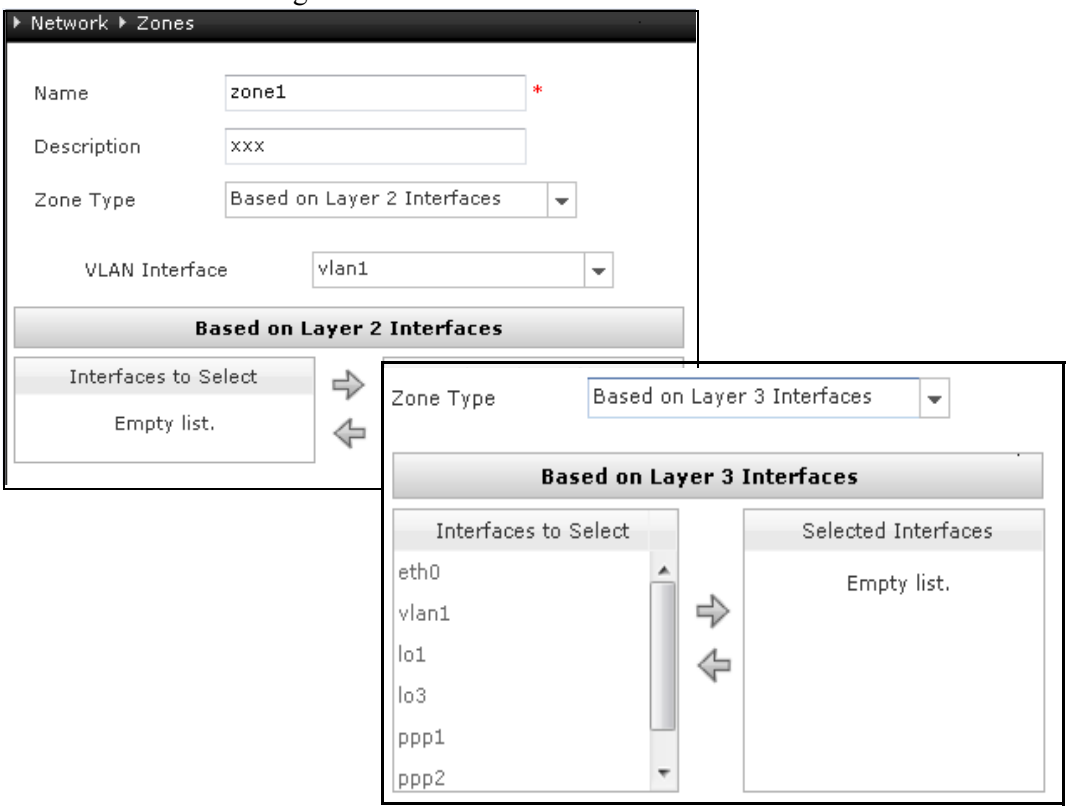
- 4.12.1 Overview
- 4.12.2 Basic configuration steps
- 4.12.3 Example: Zone Application
- 4.12.4 Parameter reference

4.12.1 Overview

A FGX device acts as a node connecting different networks for data communication, and each interface on FGX connects a different network. A zone is a collection of these interfaces, binding them together as a logical network so that uniform security control can be performed. Zones cannot communicate with each other unless access policies are configured. FGX provides no zones by default. You can create up to 30 zones.

4.12.2 Basic configuration steps

1. Choose **Network > Zones**.
2. Click **New** and configure as follows:



- Layer 3 (shared Layer 3) interfaces and Layer 2 interfaces cannot be assigned to the same zone.
- If a zone is based on Layer 2 interfaces, you can choose only one VLAN for it and assign one or more Layer 2 interfaces from this VLAN to the zone.
- If you remove all Layer 2 interfaces from this VLAN, the zone is still based on Layer 2 interfaces.
- If you delete the VLAN, the Layer 2-based zone will be automatically based on Layer 3 interfaces.

3. View the zone.

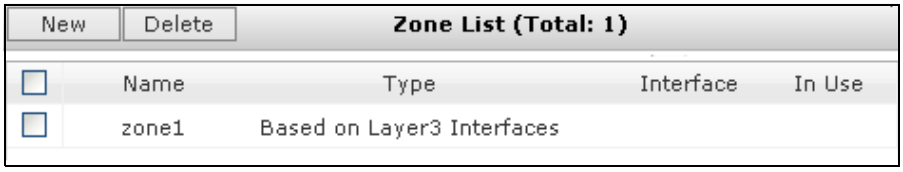


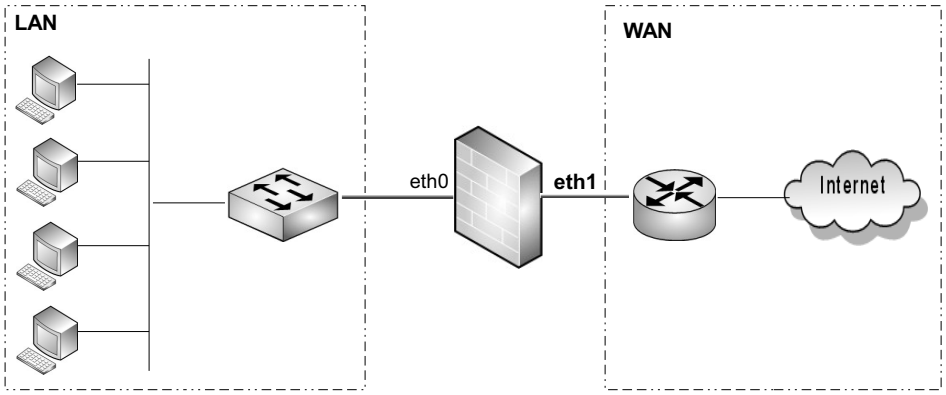
Table 107 Zone Commands

zone *zone_name*	Create a zone.
unset zone [*zone_name*]	Delete zones.
zone based-layer2	Configure a zone based on Layer 2 interfaces.
unset zone based-layer2	Delete a Layer 2 interface from a specified zone.
zone based-layer3	Configure a zone based on Layer 3 interfaces or shared Layer 3 interfaces.
unset zone based-layer3	Delete a Layer 3 interface or shared Layer 3 interface from a specified zone.
zone description	Set a comment for a specified zone.
show zone [*zone_name*]	Display zone information.

4.12.3 Example: Zone Application

A company needs to communicate with the Internet. The following figure shows the network topology.

Figure 10 Network Topology

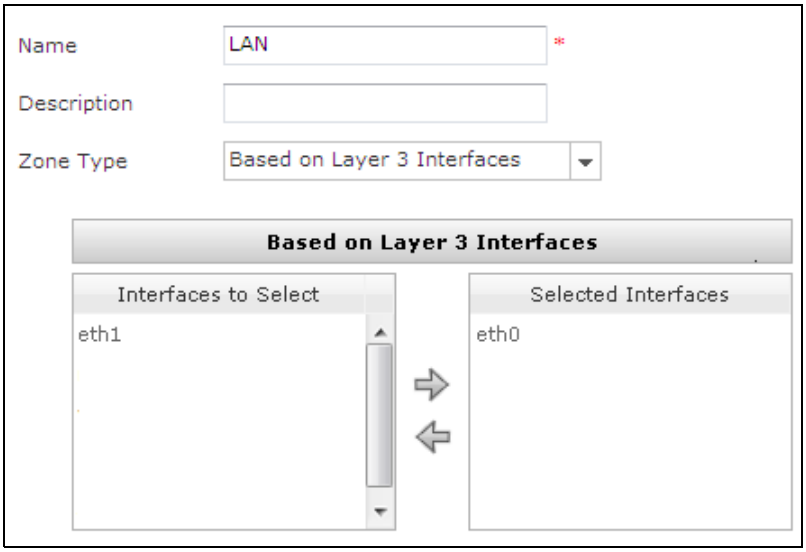


This example shows how to:

- Create a zone named LAN and allocate the Layer 3 interface eth0 to LAN.
- Create a zone named WAN and allocate the Layer 3 interface eth1 to WAN.
- Set the default action of the inter-zone policy as Permit.

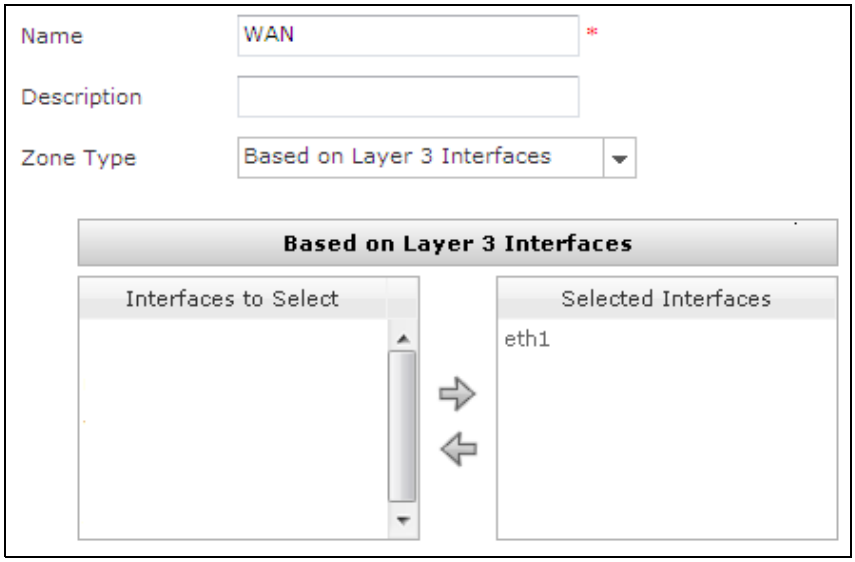
WebUI

1. Choose **Network > Zones**.
2. Click **New** to create a zone.



3. Click **OK**.

4. Click **New** to create another zone.



5. Click **OK**.
6. Choose **Firewall > Default Policy Settings**.
7. Click **Permit** in the **Configure Default Inter-Zone Policies** area.

8. Click **OK**.
9. Click  .

CLI

```
FGX@root> configure mode
FGX@root-system] zone LAN
FGX@root-system] zone LAN based-layer3 eth0
FGX@root-system] zone WAN
FGX@root-system] zone WAN based-layer3 eth1
FGX@root-system] policy default inter-zone access permit
FGX@root-system] exit
FGX@root> save config
```

4.12.4 Parameter reference

Table 108 Parameters of Zones

Parameter	Description
Name	The name of a zone, 1-63 UTF-8 characters. Cannot contain ?,'\"<>&# or spaces. The name cannot be Any or mgt-interface.
Type	The type of zone. Based on Layer 2 or Layer 3 interfaces (default).
Interface	Interfaces comprised in a zone. An interface can be assigned to one zone only.
In Use	The list of policies using a zone. Zones being used by policies cannot be deleted. To delete them, you need to dereference the zones first.
Description	Description about a zone, 0-255 UTF-8 characters. Cannot contain ?'\"<>&.

4.13 DNS Host

- 4.13.1 Overview
- 4.13.2 Basic configuration steps
- 4.13.3 Parameter reference

4.13.1 Overview

FGX can work as a DNS client to request domain name resolution services from DNS servers. You can set up to three IPv4 DNS servers and two IPv6 DNS servers to resolve domain names of system upgrade servers, UTM rule update servers, LDAP servers, and so on.

4.13.2 Basic configuration steps

1. Choose **Network > DNS > Host**.
2. Configure as follows:

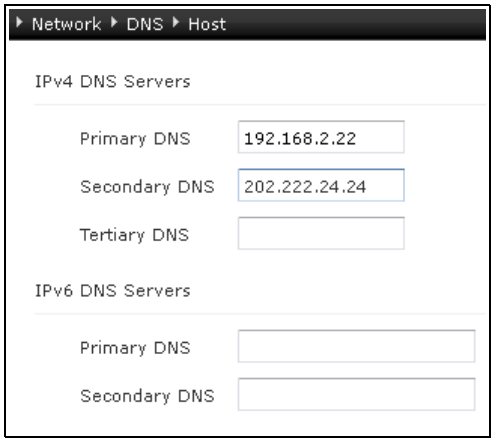


Table 109 DNS Host Commands

dns host	Configure a DNS server for FGX.
unset dns host	Delete DNS server configurations.
show dns host	Display DNS server configuration information.

4.13.3 Parameter reference

Table 110 Parameters of DNS Hosts

Parameter	Description
IPv4 DNS Servers	The IP addresses of IPv4 DNS servers, including Primary DNS, Secondary DNS, and Tertiary DNS. The IP address format is [1-223].[0-225].[0-225].[0-225]. You cannot enter 127.0.0.0-127.255.255.255 or 192.168.255.254.
IPv6 DNS Servers	The IP addresses of IPv6 DNS servers, including Primary DNS and Secondary DNS. You cannot configure the following types of IPv6 addresses for IPv6 DNS servers: loopback address (::1), multicast address (FF00/8-FFFF/8), unspecified address (::), and ::FFFF:0:0/96.

4.14 DNS Proxy

- 4.14.1 Overview
- 4.14.2 Basic configuration steps
- 4.14.3 Parameter reference

4.14.1 Overview

FGX DNS proxy has the following advantages:

- DNS proxy can make split DNS queries.
- DNS proxy allows you to send DNS queries to the DNS server through a tunnel interface.
- Using the cache on FGX improves DNS query speed.

DNS proxy provides transparent and non-transparent proxies. Both are disabled by default.

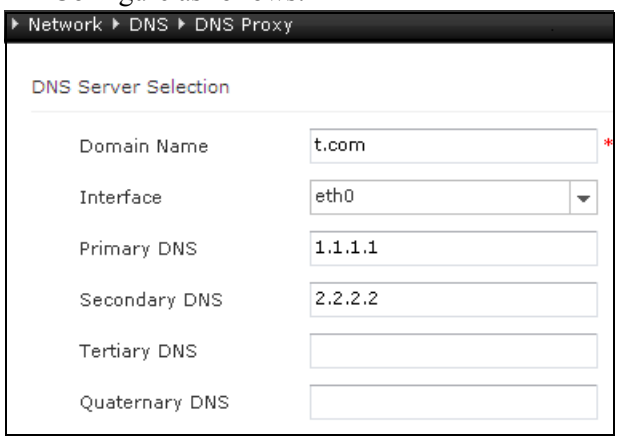
- Non-Transparent Proxy. When the DNS server address of a DNS client is directed to FGX, FGX functions as the DNS server for the client.

  When you configure a proxy DNS server or add a local static cache entry, non-transparent proxy is enabled. For more information, see 4.14.3 Parameter reference and 4.15.3 Parameter reference.
- Transparent Proxy. If the DNS client uses an actual DNS server address but sets FGX as its gateway, DNS proxy is completely transparent to users.

  When you configure an access policy and enable DNS proxy, transparent proxy is enabled. For more information, see 8.1.2 Access Policies.

4.14.2 Basic configuration steps

1. Choose **Network > DNS > DNS Proxy**.
2. Configure as follows:



- FGX supports up to 2,048 DNS proxy entries.
- You can configure IP addresses for both IPv4 and IPv6 DNS servers in the same DNS proxy entry.
- The format of IPv4 addresses for DNS servers is [1-223].[0-225].[0-225].[0-225]. You cannot enter 127.0.0.0-127.255.255.255 or 192.168.255.254. You cannot configure the following types of IPv6 addresses for DNS servers: loopback address (::1), multicast address (FF00/8-FFFF/8), unspecified address (::), and ::FFFF:0:0/96.

3. View the DNS proxy entry.

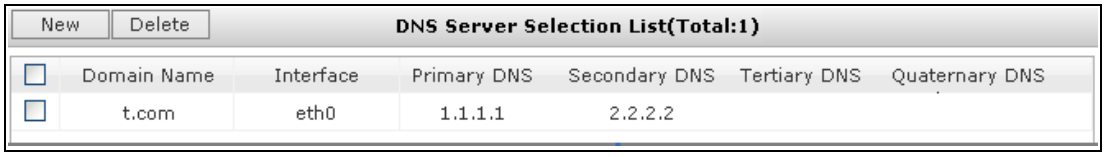


Table 111 DNS Proxy Commands

dns server-select	Add DNS proxy.
unset dns server-select	Delete DNS proxies.
show dns server-select	Display DNS proxy configuration information.

4.14.3 Parameter reference

Table 112 Parameters of DNS Proxy

Parameter	Description
Domain Name	The domain name that requires DNS proxy. A valid domain name or an asterisk (*), which means any domain name.
Interface	The Layer 3 interface (excluding loopback interfaces) used for forwarding domain name resolution requests. Any by default.
Primary DNS	The IPv4 or IPv6 address of the primary DNS server.
Secondary DNS	The IPv4 or IPv6 address of the secondary DNS server.
Tertiary DNS	The IPv4 or IPv6 address of the tertiary DNS server.
Quaternary DNS	The IPv4 or IPv6 address of the quaternary DNS server.

4.15 DNS Cache

- 4.15.1 Overview
- 4.15.2 Basic configuration steps
- 4.15.3 Parameter reference

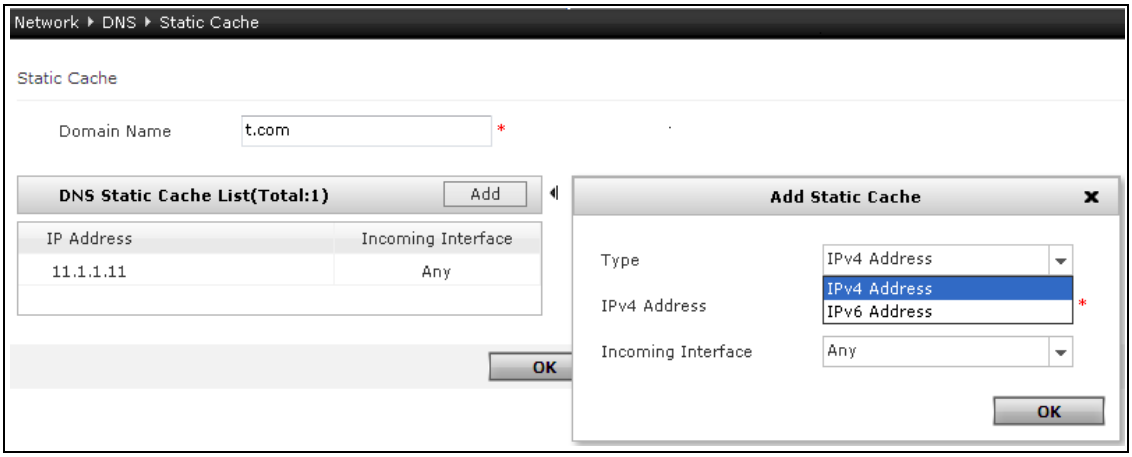
4.15.1 Overview

When a user uses FGX to perform a DNS query, FGX first searches for a matching entry in static caches. If no match is found, FGX will look it up in dynamic caches. If this fails, FGX will forward the request packet to other DNS servers through the proxy feature until the lookup succeeds, and the final entry will be added to dynamic caches.

- Dynamic Cache. Dynamically records domain names, corresponding IP addresses, and TTLs. The DNS cache table supports up to 1,024 dynamic cache entries.
- Static Cache. Manually configured and records IP addresses, corresponding domain names, and incoming interfaces. The DNS cache table supports up to 2,048 static cache entries.

4.15.2 Basic configuration steps

1. Choose **Network > DNS > Static Cache**.
2. Configure as follows:



- To make static DNS caching take effect, you need to enable this function by clicking Enable in the Static DNS Caching field.
- You can delete dynamic DNS cache entries using the **unset dns cache dynamic** [*domain_name*] command.

3. View the static cache entry.

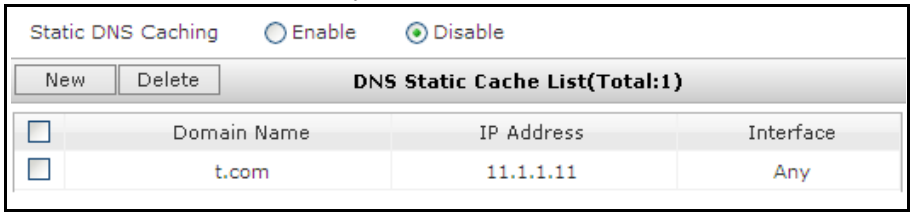


Table 113 DNS Cache Commands

dns cache	Add a static DNS cache.
dns cache-state {**on** | **off**}	Enable or disable the DNS static cache.
unset dns cache dynamic	Delete dynamic DNS cache entries.
unset dns cache static	Delete static DNS cache entries.
show dns cache	Display DNS cache information.
show dns cache-state	Display the state of the DNS static cache.

4.15.3 Parameter reference

Table 114 Parameters of Static DNS Cache

Parameter	Description
Domain Name	The domain name in a static cache entry.
IP Address	The IP address corresponding to a domain name in a static cache entry. You can configure both IPv4 and IPv6 addresses in the same static DNS cache entry. The format of the IPv4 address is [1-223].[0-225].[0-225].[0-225]. You cannot enter 127.0.0.0-127.255.255.255 or 192.168.255.254. A domain name can correspond to 32 IP addresses at most.
Interface	The Layer 3 interface (excluding loopback interfaces) on which domain name resolution requests are received.

4.16 DHCP Servers

- 4.16.1 Overview
- 4.16.2 Basic configuration steps
- 4.16.3 DHCP Examples
- 4.16.4 Parameter reference

4.16.1 Overview

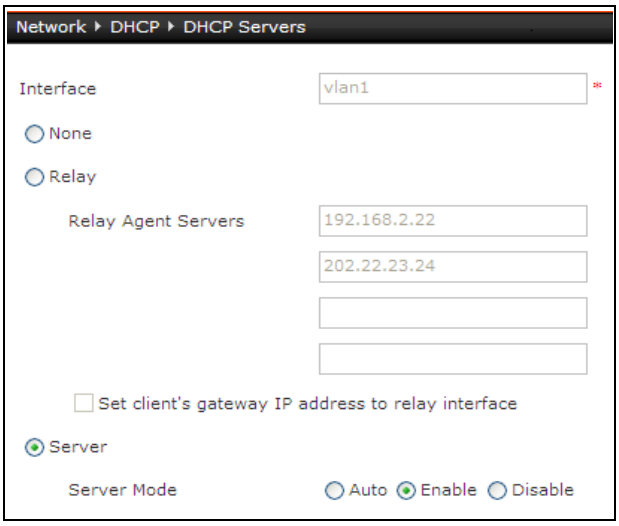
The Dynamic Host Configuration Protocol (DHCP) is used to dynamically assign IP addresses. FGX can function as a DHCP client, DHCP server, and DHCP relay agent simultaneously. Only one DHCP role can be set for each interface.

FGX supports the following three DHCP roles:

- **DHCP servers**—automatically assign IP addresses to the hosts (DHCP clients) on any interface in any zone.
- **DHCP relay agents**—receive DHCP messages from DHCP servers and send them to the hosts on any interface in any zone.
- **DHCP clients**—obtain dynamically assigned IP addresses. You should configure DHCP clients in Interfaces module. See 4.2.2.2 Layer 3 for step 4.

4.16.2 Basic configuration steps

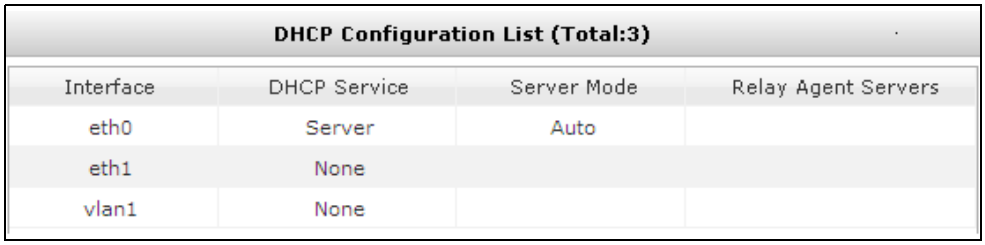
1. Choose **Network > DHCP > DHCP Servers**.
2. Configure as follows:



- Only interfaces with valid IP addresses can be configured as DHCP servers or relay agents.
- On the **DHCP Servers** page, you can click **DHCP IP Address Binding Status** to open the corresponding monitoring page and view the binding status information.

- If you have logged on to FGX through an interface and then configure this interface as a DHCP client, the original IP address of this interface will become invalid. You must log on to FGX again using a dynamically obtained IP address.
- If you check "**Set client's gateway IP address to relay interface**" for configuring DHCP relay agents, FGX will overwrite the Gateway field in the DHCP reply message with the IP address of the DHCP relay interface. If no Gateway field is specified in the reply message, the gateway will be automatically directed to the IP address of the relay interface.

3. View the DHCP configuration entry.



DHCP Configuration List (Total:3)

Interface	DHCP Service	Server Mode	Relay Agent Servers
eth0	Server	Auto	
eth1	None		
vlan1	None		

Table 115 DHCP Server Commands

dhcp interface none	Delete the DHCP role of a specified interface.
dhcp interface relay	Configure a specified interface as a DHCP relay agent.
unset dhcp interface relay	Delete the DHCP relay agent role of specified interface.
dhcp interface relay change-gateway	Set whether the DHCP relay agent on an interface will update the gateway.
dhcp interface server {**auto** | **enable** | **disable**}	Set a DHCP server mode for a specified interface.
unset dhcp interface all	Delete the DHCP configurations of all interfaces.
show dhcp interface [*interface_name*]	Display the configuration information of DHCP interfaces.
show dhcp server ip-binding	Display the IP address binding state for a DHCP server.

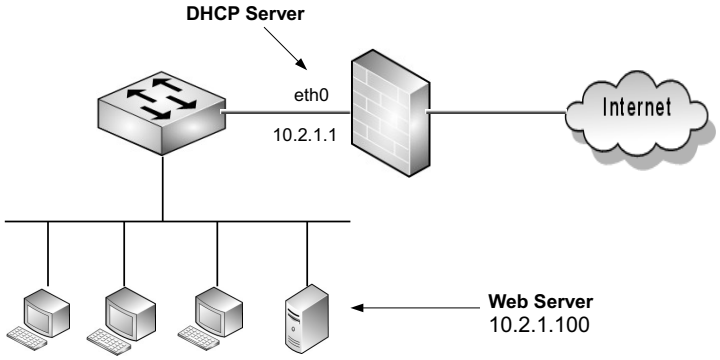
4.16.3 DHCP Examples

- Example 1: Configure DHCP Server
- Example 2: Configure DHCP Relay Agent

Example 1: Configure DHCP Server

The interface eth0 on FGX is configured as a DHCP server to dynamically assign IP addresses of the subnet 10.2.1.0/24 and other network parameters to DHCP clients in the intranet. A Web server whose MAC address is 44:37:E6:27:C5:D5 needs to have the reserved IP address 10.2.1.100.

Figure 11 Configuring DHCP Server

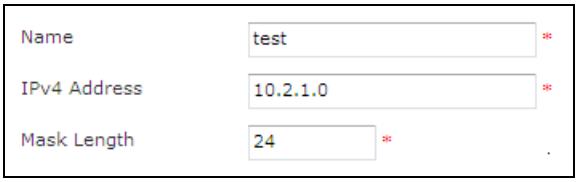


This example shows how to:

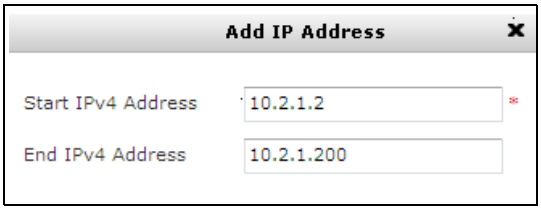
- Create a DHCP server subnet (10.2.1.0/24) named test.
- Set eth0 as the DHCP server.
- Create the reserved IP 10.2.1.100.

WebUI

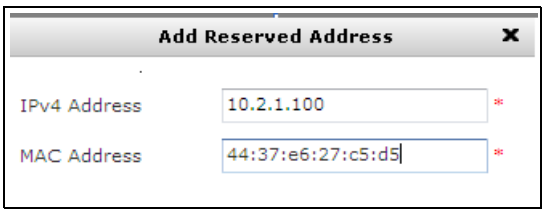
1. Choose **Network > DHCP > DHCP Server Subnets**.
2. Click **New** to create a DHCP server subnet.



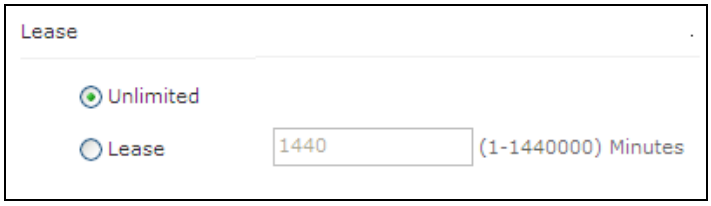
3. In **IP Pool List**, click **Add** to add an IP address range.



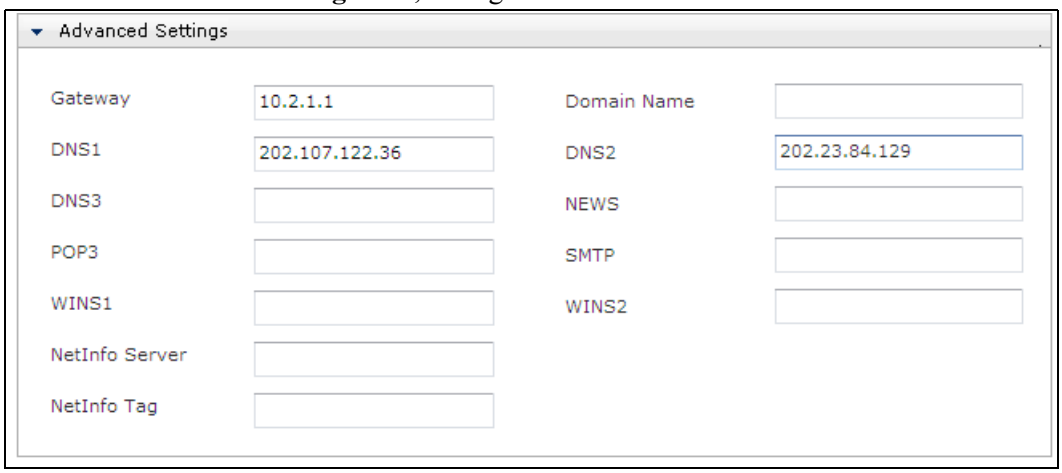
4. In **Reserved Address List**, click **Add** to add a reserved address.



5. In the **Lease** area, click **Unlimited** to keep the lease permanent.



6. In the **Advanced Settings** area, configure as follows:



7. Click **OK**.
8. Choose **Network > DHCP > DHCP Servers**.
9. In **DHCP Configuration List**, click corresponding to eth0 to open the Edit page.
10. In the **Server** area, click **Auto** to set the server to work in Auto mode.

11. Click **OK**.
12. Click .

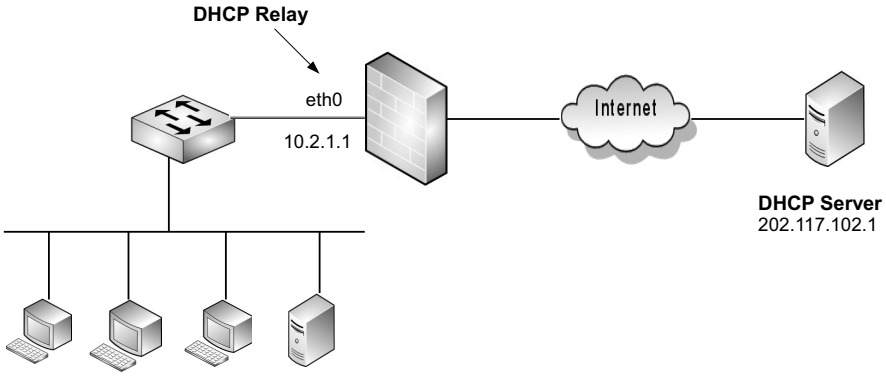
CLI

```
FGX@root> configure mode
FGX@root-system] dhcp subnet test 10.2.1.0 24
FGX@root-system] dhcp subnet test dynamic 10.2.1.2-10.2.1.200
FGX@root-system] dhcp subnet test reserve 10.2.1.100
44:37:E6:27:C5:D5
FGX@root-system] dhcp subnet test lease unlimited
FGX@root-system] dhcp subnet test gateway 10.2.1.1
FGX@root-system] dhcp subnet test dns 202.107.122.36
FGX@root-system] dhcp subnet test dns2 202.23.84.129
FGX@root-system] dhcp interface eth0 server auto
FGX@root-system] exit
FGX@root> save config
```

Example 2: Configure DHCP Relay Agent

The interface eth0 of FGX is configured as the DHCP relay agent forwarding DHCP messages from the DHCP server 202.117.102.1 to DHCP clients in the intranet.

Figure 12 Configuring DHCP Relay Agent



This example shows how to:

- Configure eth0 as the DHCP relay agent and configure the DHCP server with the IP address 202.117.102.1.
- Set the gateway address of the DHCP clients in the intranet to the IP address of eth0.

WebUI

1. Choose **Network > DHCP > DHCP Servers**.
2. In **DHCP Configuration List**, click corresponding to eth0 to open the Edit page and configure as follows:

3. Click **OK**.
4. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] dhcp interface eth0 relay 202.117.102.1 primary
FGX@root-system] dhcp interface eth0 relay change-gateway enable
FGX@root-system] exit
FGX@root> save config
```

4.16.4 Parameter reference

Table 116 Parameters of DHCP Services

Parameter	Description
Interface	Interface on which DHCP service is configured. Can be a Layer 3 or shared Layer 3 Ethernet interface, Layer 3 or shared Layer 3 channel interface, Layer 3 or shared Layer 3 redundant interface, VLAN interface, or virtual interface.
DHCP Service	DHCP services provided by FGX, including: • **None—**indicates DHCP is not enabled on a Layer 3 interface. • **Relay—**indicates a Layer 3 interface is working as a DHCP relay agent. • **Server—**indicates a Layer 3 interface is working as a DHCP server. • **Client—**indicates a Layer 3 interface is working as a DHCP client.
Server Mode	The working mode of a specified Layer 3 interface working as a DHCP server on FGX. • **Auto—**FGX automatically detects whether there is an external DHCP server already existing on the network. If there is, the DHCP server on FGX will stop working; otherwise, it will dynamically assign IP addresses to DHCP clients. • **Enable—**the DHCP server on FGX is always enabled. FGX does not perform detection of external servers but works as a DHCP server directly. • **Disable—**the DHCP server on FGX is disabled but it still keeps information already assigned, such as IP addresses.
Relay Agent Servers	The IPv4 addresses of the relay agent servers when specified Layer 3 interfaces are working as relay agents on FGX. The IP address format is [1-223].[0-225].[0-225].[0-225]. You cannot enter 127.0.0.0-127.255.255.255 or 192.168.255.254.

4.17 DHCP Server Subnets

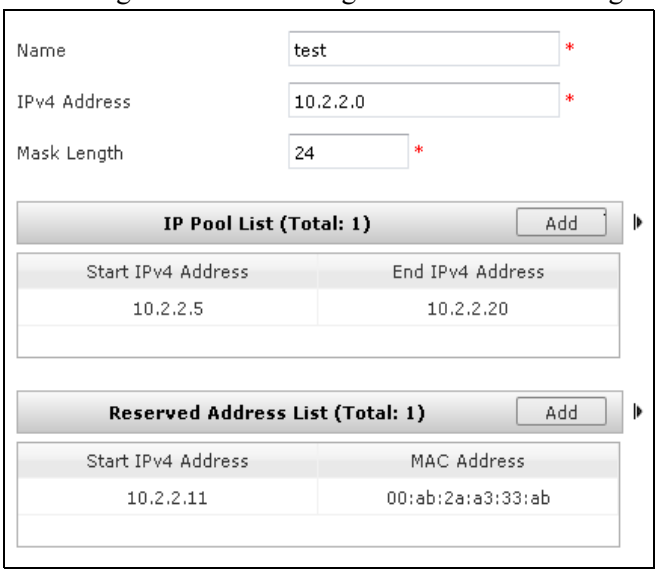
- 4.17.1 Overview
- 4.17.2 Basic configuration steps
- 4.17.3 Parameter reference

4.17.1 Overview

A DHCP server subnet functions to provide address pools for a DHCP server to assign IP addresses to DHCP clients. The role of DHCP server is assumed by a Layer 3 interface on FGX. FGX supports up to 256 DHCP server subnets.

4.17.2 Basic configuration steps

1. Choose **Network > DHCP > DHCP Server Subnets**.
2. Configure IP address range used for DHCP assignment and reserved IP address:



3. Configure lease time and advanced settings:

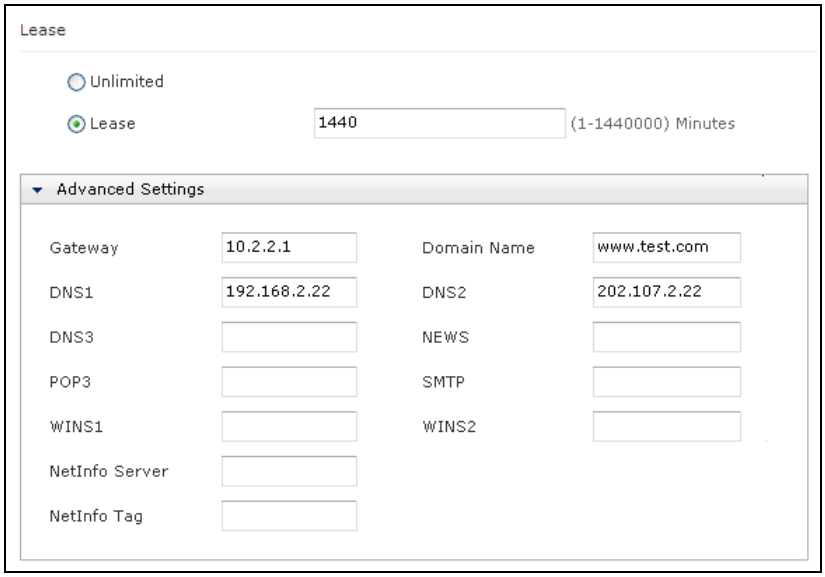


Table 117 DHCP Server Subnet Commands

dhcp subnet	Add a DHCP subnet.
unset dhcp subnet	Delete DHCP subnets.
dhcp subnet domain	Specify a domain name for a specified subnet.
unset dhcp subnet domain	Delete the domain name of a specified subnet.
dhcp subnet dynamic	Add an IP address pool for a specified subnet.
unset dhcp subnet dynamic	Delete the IP address pool from a specified subnet.
dhcp subnet reserve	Configure a reserved address for a specified subnet.
unset dhcp subnet reserve	Delete a specific reserved address from a specified subnet.
dhcp subnet gateway, wins, dns, smtp, pop3, news, nis	Configure IP addresses of the specified servers in a specified subnet.
unset dhcp subnet gateway, wins, dns, smtp, pop3, news, nis	Delete IP addresses of the specified servers in a specified subnet.
dhcp subnet nistag	Set a tag for the NetInfo server (NIS) in a specified subnet.
unset dhcp subnet nistag	Delete the tag of the NIS in a specified subnet.
dhcp subnet lease	Set a lease period for a specified subnet.
show dhcp server subnet	Display the configuration information of DHCP subnets.

4.17.3 Parameter reference

Table 118 Parameters of DHCP Server Subnets

Parameter	Description
Name	The name of a DHCP server subnet, 1-63 UTF-8 characters. Cannot contain ?,'\"<>&# or spaces. The name length range is 1-63 characters.
Network Address	The network address and mask length of a DHCP server subnet. It should be an IPv4 address. The format is [1-223].[0-225].[0-225].[0-225], and you cannot enter 127.0.0.0-127.255.255.255.
IP Pool	An IP address pool comprising dynamically assigned addresses. You can configure an IP address pool by setting start and end IP addresses or just a single IP address. The start IP address cannot be greater than the end IP address. When configuring IP addresses for a subnet, you must set all of the addresses in that subnet. IP Pool List allows up to 256 IP addresses.
Reserved IP Address	IP addresses with which DHCP clients are bound. These IP addresses are sent to specified DHCP clients through a DHCP server. Reserved Address List allows up to 256 IP addresses.
Lease (min)	The duration of IP address leases. Its range is 1-1,440,000 minutes. It is 1,440 minutes by default. You can set it as Unlimited. If you modify the lease duration when FGX is running, the new lease setting will not take effect until the client sends a DHCPREQUEST message to request a lease update.
Advanced Settings	Other network parameters assigned to DHCP clients, including gateway, domain name, DNS servers, NEWS server, POP3 server, SMTP server, WINS servers, NetInfo server, and NetInfo tag. The IP address format of the above servers and gateway is [1-223].[0-225].[0-225].[0-225], and you cannot enter 127.0.0.0-127.255.255.255 or 192.168.255.254. The NetInfo tag name is 0-255 UTF-8 characters. Cannot contain ?'\"<>&.

4.18 DHCPv6

- 4.18.1 Overview
- 4.18.2 Basic configuration steps
- 4.18.3 DHCPv6 Examples
- 4.18.4 Parameter reference

4.18.1 Overview

Designed for IPv6 addressing, DHCPv6 (Dynamic Host Configuration Protocol for IPv6) functions to assign hosts with IPv6 addresses, IPv6 prefixes, and other network configuration parameters. It includes:

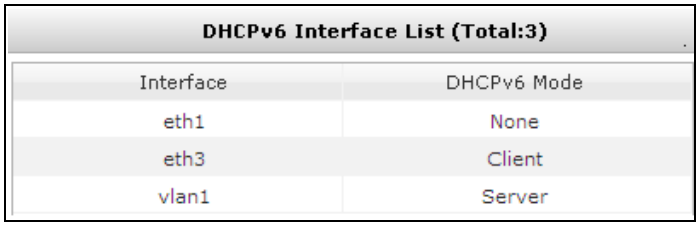
- Stateful DHCPv6 Configuration. Refers to IPv6 address and prefix assignment through a DHPCv6 server. This is stateful configuration because the DHCPv6 server keeps the information of addresses and prefixes assigned.
- Stateless DHCPv6 Configuration. Refers to the configuration of other network parameters (such as DNS server and domain name) through a DHCPv6 server after obtaining IPv6 addresses through stateless address autoconfiguration. This is stateless configuration because the DHCPv6 server does not keep any status information of the assigned configuration parameters.

FGX can work:

- As a DHCPv6 client, requesting for DHCPv6 prefix delegation and other network configuration parameters. Currently, it does not support request for DHCPv6 address assignment.
- As a stateless DHCPv6 server, assigning clients network configuration parameters, such as DNS server addresses, SNTP (Simple Network Time Protocol) server addresses, and domain names.

4.18.2 Basic configuration steps

1. Choose **Network > IPv6 > DHCPv6**.
2. Configure as follows:



DHCPv6 Interface List (Total:3)

Interface	DHCPv6 Mode
eth1	None
eth3	Client
vlan1	Server

   - Before configuring DHCPv6 for a Layer 3 or shared Layer 3 interface, choose **Network > Interfaces** and enable IPv6 on the interface.
   - The following interfaces can work as DHCPv6 clients: Layer 3 or shared Layer 3 Ethernet interfaces, Layer 3 or shared Layer 3 channel interfaces, Layer 3 or shared Layer 3 redundant interfaces, Layer 3 virtual interfaces, VLAN interfaces, and PPPoE interfaces.

- The following interfaces can work as stateless DHCPv6 servers: Layer 3 or shared Layer 3 Ethernet interfaces, Layer 3 or shared Layer 3 channel interfaces, Layer 3 or shared Layer 3 redundant interfaces, Layer 3 virtual interfaces, and VLAN interfaces.
- One DHCPv6 client interface can be used by multiple stateless DHCPv6 servers.
- A client interface cannot be deleted when it is in use.

Table 119 DHCPv6 Commands

dhcpv6 type {**client** | **none** | **server**}	Set a DHCPv6 working mode for a specified Layer 3 or shared Layer 3 interface.
dhcpv6 ip	Set SLA and interface ID for a DHCPv6 client interface.
unset dhcpv6 ip	Delete the SLAs and interface IDs of a DHCPv6 client interface.
dhcpv6 prefix-assignment	Specify a prefix delegation interface for a DHCPv6 client and set the corresponding SLA and interface ID.
unset dhcpv6 prefix-assignment	Delete the prefix delegation interface from a DHCPv6 client and the corresponding SLAs and interface IDs.
dhcpv6 overwrite-dns	Enable DNS overwriting function for a specified DHCPv6 client interface.
unset dhcpv6 overwrite-dns	Disable the DNS overwriting function for a specified DHCPv6 client interface.
dhcpv6 enable-dns-proxy	Enable the function of automatically adding DNS proxy for a DHCPv6 client interface.
unset dhcpv6 enable-dns-proxy	Disable the function of automatically adding DNS proxy for a DHCPv6 client interface.
dhcpv6 client send-request	Send a DHCPv6 client request to a DHCPv6 server.
show dhcpv6-client	Display the configuration information obtained from a DHCPv6 server through DHCPv6 client interfaces.
show dhcpv6-client-config	Display the configuration information about DHCPv6 client interfaces.
dhcpv6 server-type {auto interface | **manual}**	Configure stateless DHCPv6 server information either manually or by automatically updating from a DHCPv6 client interface.
dhcpv6 server {dns | dns2}	Set DNS server information for a stateless DHCPv6 server.
unset dhcpv6 server {dns | dns2}	Delete DNS server information of a stateless DHCPv6 server.
dhcpv6 server domain_search_list	Add a domain name to the domain search list of a stateless DHCPv6 server.
unset dhcpv6 server domain_search_list	Delete a specified domain name from the domain search list of a stateless DHCPv6 server.
dhcpv6 server {sntp | sntp2}	Set SNTP server information for a stateless DHCPv6 server.
unset dhcpv6 server {sntp | sntp2}	Delete SNTP server information of a stateless DHCPv6 server.
show dhcpv6-server-config	Display the configuration information about stateless DHCPv6 server interfaces.

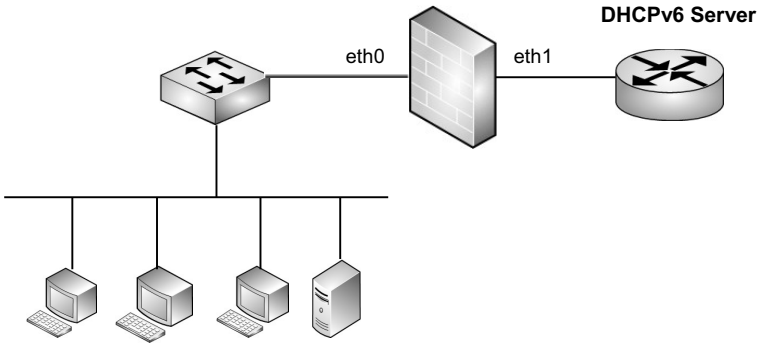
4.18.3 DHCPv6 Examples

- Example 1: Configure DHCPv6 Client
- Example 2: Configure Stateless DHCPv6 Server

Example 1: Configure DHCPv6 Client

The interface eth1 of FGX is a DHCPv6 client connected to a DHCPv6 server. The interface eth0 is connected to the intranet, and it advertises prefix information through the RA message to the hosts in the intranet. The hosts obtain the IPv6 addresses through stateless address autoconfiguration.

Figure 13 Configuring DHCPv6 Client



This example shows how to perform the following configurations:

- Enable IPv6 and stateless address autoconfiguration on eth0 and eth1.
- Configure eth1 as the DHCPv6 client. Configure the SLA in **IPv6 Address List** as 23ed and the interface ID as EUI-64.
- Configure the SLA in **Prefix Delegation List** for eth0 as 32af and the interface ID as EUI-64.
- Replace the DNS server addresses configured on FGX DNS Host with the new DNS server addresses obtained from the DHCPv6 server.

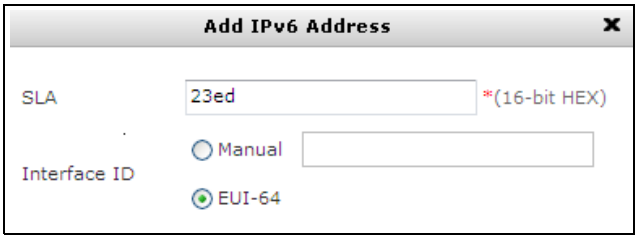
WebUI

1. Choose **Network > Interfaces**.
2. Click corresponding to eth0 and eth1 to open their corresponding Edit pages and configure as follows:

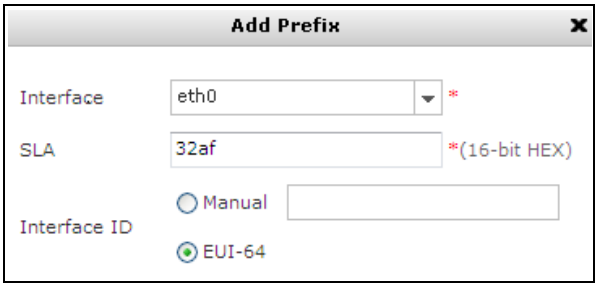
3. Click **OK**.

4. Choose **Network > IPv6 > DHCPv6**.
5. Click corresponding to eth1 to open the Edit page and configure as follows:
   a. Choose **Client** from the **Type** drop-down list.

   b. In **IPv6 Address List**, click **Add** to add an IPv6 address.



   c. In **Prefix Delegation List**, click **Add** to add a prefix.



   d. Check **Overwrite DNS**.
6. Click **OK**.
7. Click corresponding to eth1 to open the Edit page and click **Send DHCP Request.**
8. Click .

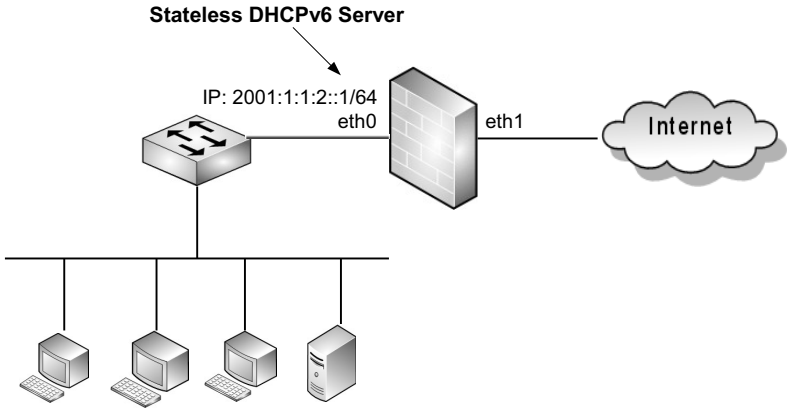
CLI

```
FGX@root> configure mode
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] ipv6 enable
FGX@root-system-if-eth0] ipv6 address autoconfig
FGX@root-system-if-eth0] exit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] ipv6 enable
FGX@root-system-if-eth1] ipv6 address autoconfig
FGX@root-system-if-eth1] dhcpv6 type client
FGX@root-system-if-eth1] dhcpv6 ip SLA 23ed eui-64
FGX@root-system-if-eth1] dhcpv6 prefix-assignment interface ethernet 0
SLA 32af eui-64
FGX@root-system-if-eth1] dhcpv6 overwrite-dns
FGX@root-system-if-eth1] dhcpv6 client send-request
FGX@root-system-if-eth1] end
FGX@root> save config
```

Example 2: Configure Stateless DHCPv6 Server

The interface eth0 with the IPv6 address of 2001:1:1:2::1/64 works as a stateless DHCPv6 server and is connected to the internal network. On FGX, you can manually configure the stateless DHCPv6 information to be assigned to internal hosts, such as DNS, SNTP, and Domain Search List.

Figure 14 Configuring Stateless DHCPv6 Server



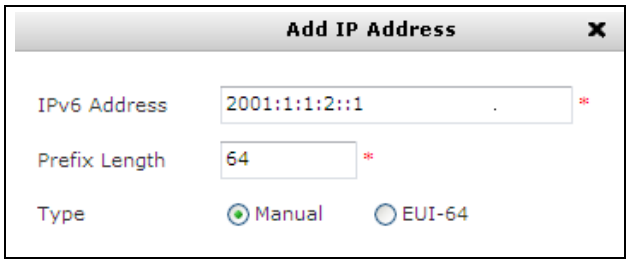
This example shows how to perform the following configurations:

- Enable IPv6 on eth0 and configure its IPv6 address manually.
- Configure eth0 as a stateless DHCPv6 server and set the stateless DHCPv6 information to be assigned to internal hosts.

WebUI

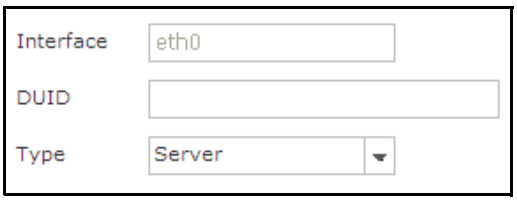
1. Choose **Network > Interfaces**.
2. Click corresponding to eth0 to open the corresponding Edit page and configure as follows:
   a. Check **Enable IPv6**.

   b. In **IPv6 Address List**, click **Add** to add an IPv6 address.

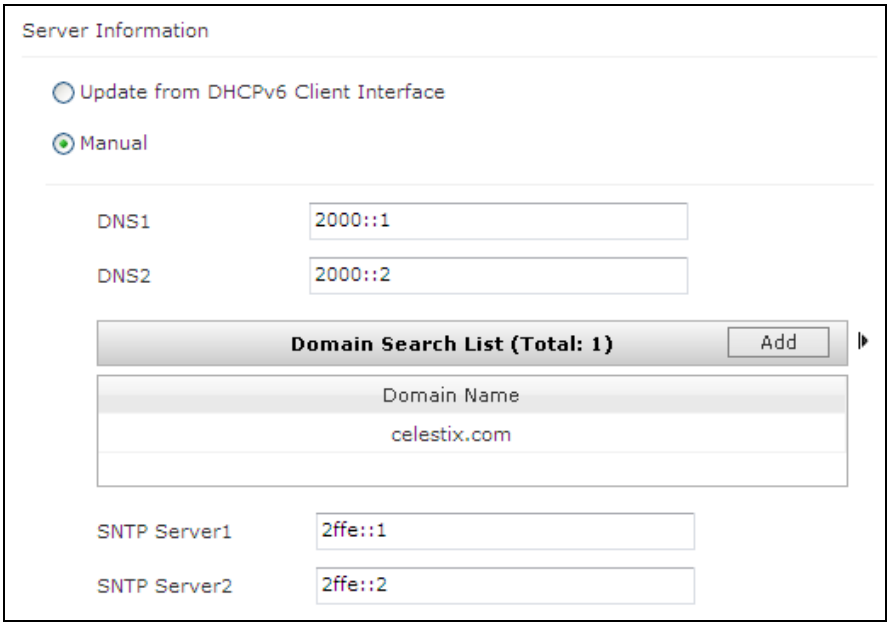


3. Click **OK**.

4. Choose **Network > IPv6 > DHCPv6**.
5. Click corresponding to eth0 to open the Edit page and configure as follows:
   a. Choose **Server** from the **Type** drop-down list.



   b. In the **Server Information** area, choose **Manual** and configure related settings.



6. Click **OK**.
7. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] ipv6 enable
FGX@root-system-if-eth0] ipv6 address 2001:1:1:2::1/64
FGX@root-system-if-eth0] dhcpv6 type server
FGX@root-system-if-eth0] dhcpv6 server dns 2000::1
FGX@root-system-if-eth0] dhcpv6 server dns2 2000::2
FGX@root-system-if-eth0] dhcpv6 server domain_name_list test.com
FGX@root-system-if-eth0] dhcpv6 server sntp 2ffe::1
FGX@root-system-if-eth0] dhcpv6 server sntp2 2ffe::2
FGX@root-system-if-eth0] end
FGX@root> save config
```

4.18.4 Parameter reference

Table 120 Parameters of DHCPv6 Clients

Parameter	Description
Interface	DHCPv6 client interface. Can be Layer 3 or shared Layer 3 Ethernet interfaces, Layer 3 or shared Layer 3 channel interfaces, Layer 3 or shared Layer 3 redundant interfaces, Layer 3 virtual interfaces, VLAN interfaces, and PPPoE interfaces.
DUID	DHCP Unique Identifier which is used to identify a DHCPv6 device (DHCP server, DHCP client, or DHCP relay agent). This value is automatically generated by the system.
Type	DHCPv6 working modes of interfaces, including: • **None—**indicates that DHCPv6 is disabled. • **Client—**indicates DHCPv6 client mode. • **Server—**indicates stateless DHCPv6 server mode.
Send DHCP Request	When you click this button, the interface working as a DHCPv6 client sends DHCP-PD and DHCP-inform requests successively.
IPv6 Address List	Comprises configuration information used to configure IPv6 addresses for those interfaces that work as DHCPv6 clients. Configuration parameters include: • **SLA—**subnet the prefix obtained through DHCPv6. The SLA range is 0000-FFFF. A 64-bit prefix is computed by right-aligning the SLA with the prefix delegated through DHCPv6. • **Interface ID—**includes Manual and EUI-64. When you specify Manual, it indicates manually generating an address without using the EUI-64 format interface identifier. When you specify EUI-64, it indicates the use of EUI-64 format interface identifier to generate an address. An IPv6 address with a prefix length of 64 is formed by combining the prefix obtained through DHCP-PD with SLA and interface ID. IPv6 Address List allows up to eight entries.
Prefix Delegation List	Comprises configuration information used to form 64-bit prefixes and IPv6 addresses for those interfaces that can push RA messages comprising the 64-bit prefixes to the hosts in the directly connected subnet. Configuration parameters include: Interface, SLA, and Interface ID. The interface here refers to a Layer 3 interface (except the loopback interface, tunnel interface, and PPPoE interface) other than the requesting client interface. SLA and Interface ID function the same as those comprised in **IPv6 Address List**. You can configure up to eight entries per interface.
Overwrite DNS	With this function enabled, upon sending a DHCP request, FGX will overwrite DNS server information with the new DNS server information obtained from a DHCPv6 server through stateless DHCPv6. It is disabled by default.
Enable DNS Proxy	With this function enabled, the system automatically adds DNS proxy according to the DNS information obtained through DHCPv6 client interfaces. It is disabled by default.

Table 121 Parameters of Stateless DHCPv6 Servers

Parameter	Description
Interface	Stateless DHCPv6 server interface. Can be Layer 3 or shared Layer 3 Ethernet interfaces, Layer 3 or shared Layer 3 channel interfaces, Layer 3 or shared Layer 3 redundant interfaces, Layer 3 virtual interfaces, and VLAN interfaces.
DUID	DHCP Unique Identifier which is used to identify a DHCPv6 device (DHCP server, DHCP client, or DHCP relay agent). This value is automatically generated by the system.
Type	DHCPv6 working modes of interfaces, including: • **None—**indicates that DHCPv6 is disabled. • **Client—**indicates DHCPv6 client mode. • **Server—**indicates stateless DHCPv6 server mode.
Server Information	Comprises two methods of configuring stateless DHCPv6 server information: • **Update from DHCPv6 Client Interface—**indicates that a stateless DHCPv6 server obtains its stateless DHCPv6 information through a specified DHCPv6 client interface and assigns the information to requesting clients. The server should update its information with the stateless information change of the DHCPv6 client. • **Manual—**indicates that you can manually configure the stateless DHCPv6 information to be assigned by the current server to requesting clients. The information includes: DNS, Domain Search List, and SNTP. **•DNS—**indicates IPv6 addresses of DNS servers, including DNS1 and DNS2. The address cannot be a loopback address (::1), unspecified address (::), multicast address (FF00/8-FFFF/8), or ::FFFF:0:0/96. **•Domain Search List—**comprises up to eight domain names. A domain name can be composed of letters, digits, hyphens, and periods. It cannot start with a period, hyphen, or digit and cannot end with a period or hyphen. The length between two periods must be in 1-63 characters. The length range of a domain name is 2-255 characters. **•SNTP—**indicates IPv6 addresses of SNTP servers, including SNTP Server1 and SNTP Server2. The address cannot be a loopback address (::1), unspecified address (::), multicast address (FF00/8-FFFF/8), or ::FFFF:0:0/96.

4.19 STP

- 4.19.1 Overview
- 4.19.2 Basic configuration steps
- 4.19.3 Example: STP Application
- 4.19.4 Parameter reference

4.19.1 Overview

The Spanning Tree Protocol (STP) is defined in a narrow and broad sense. STP in narrow sense refers to standard STP as defined in IEEE 802.1D. STP in broad sense refers to standard STP as well as those enhanced spanning tree protocols, such as RSTP and MSTP.

4.19.1.1 STP

STP is a Layer 2 switching network management protocol. It forms a tree topology in a network of connected bridges (typically switches) with one bridge as the root and all others spanning like leaves. By blocking some ports on some bridges, it ensures link redundancy and loop-free topology in bridged or switched networks. When an active link fails, those blocked ports provide backup links.

FGX provides Per-VLAN Spanning Tree feature. You can enable STP/RSTP separately for each VLAN on Layer 2 switched network, and each VLAN maintains its own spanning tree. This makes it possible in certain scenarios to create loop-free VLANs and achieve Layer 2 load-balancing.

STP operation goes as follows:

1. Select a root bridge

   A root bridge is the bridge with the smallest bridge ID. On a Layer 2 network, there is only one root bridge that sends BPDUs (Bridge Protocol Data Unit, used for establishing a loop-free STP topology) while other bridges only receive and forward them.

2. Select root port

   A root port is the port on a non-root bridge with the smallest path cost to the root bridge. A non-root bridge has one root port only.

3. Select designated port

   A designated port is the port on a network segment with the smallest path cost to the root bridge. One segment has only one designated port.

4. Set blocked port

   A port that is neither a root port nor a designated port is blocked port, and it only listens to BPDUs.

4.19.1.2 RSTP

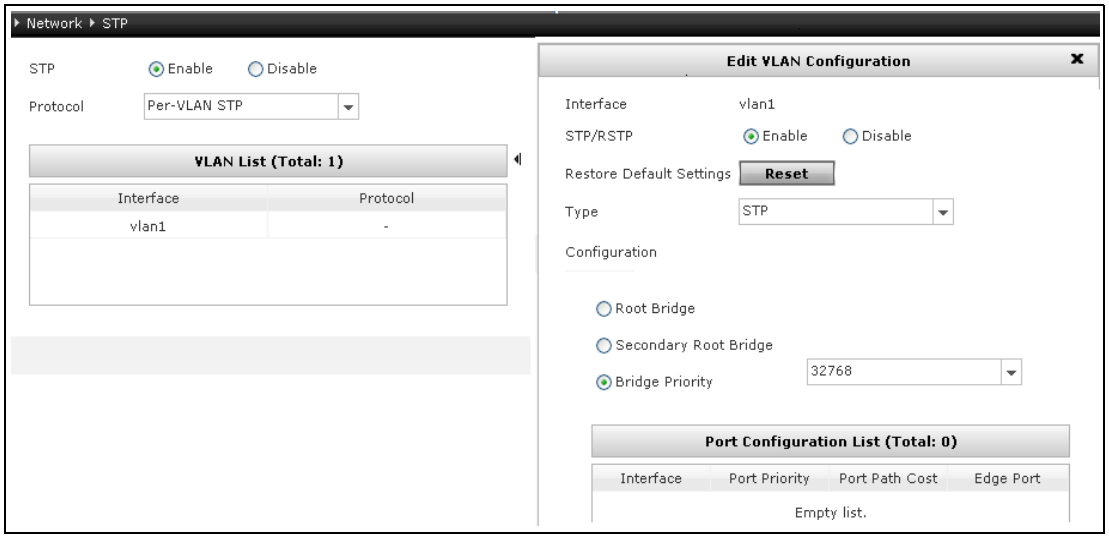
The Rapid Spanning Tree Protocol (RSTP) is defined by IEEE 802.1w. RSTP is an evolution of STP and achieves faster spanning tree convergence after a topology change. It is compatible with STP. According to the protocol version logged in a BPDU received from a counterpart, a bridge running RSTP can automatically recognize whether its counterpart supports STP or RSTP.

By default, STP convergence takes up to 50 seconds while RSTP takes only 1 second to converge.

- Fast Convergence. RSTP depends on the following two factors to achieve fast convergence:
  - Edge Port. An edge port directly connects a bridge or switch with a terminal such as server. It does not participate in STP calculation and can skip over the listening and learning states and go directly into forwarding state without delay.
  - Link Type. When RSTP is enabled, a bridge or switch automatically determines the link type based on the duplexing mode of a port. When the port works in full duplexing mode, it uses the point-to-point link and quickly transitions from discarding state into forwarding state.
- Port Roles. The root ports and designated ports in RSTP function the same as those in STP. RSTP has the following additional port roles for state migration.
  - **Alternate port—**backup for root port.
  - **Backup Port—**backup for a designated port of a network segment.
- Port States. RSTP has three simplified port states: discarding, learning, and forwarding. The discarding state in RSTP combines the disabled, blocking, and listening states in STP.
- Enforcing RSTP. Enforcing RSTP can facilitate data forwarding efficiency. If you're sure that the devices connected to FGX are running RSTP, you can enforce RSTP on FGX. Otherwise, enforcing RSTP will lead to incompatibility if the device directly connected to FGX supports STP only.

4.19.2 Basic configuration steps

1. Choose **Network > STP**.
2. Configure as follows:



- You must double-click on an entry in the VLAN list to edit.
- A VLAN cannot be configured as the root bridge and secondary root bridge simultaneously.

- When a VLAN is deleted, all its STP configurations will be deleted; when an interface is deleted from a VLAN, its configurations are deleted. This does not affect configurations of the other interfaces comprised in the same VLAN.
- You can configure STP timers (Hello, Max-age, and Forward-delay) using the CLI.
- FGX allows you to enable STP/RSTP instances on up to 64 VLANs.

3. Click **OK**.
4. Click  .

Table 122 STP Commands

show spanning-tree {**brief** | **vlan** *vlan_id*}	Display STP information.
spanning-tree {**enable per-vlan-stp** | **disable**}	Enable or disable the STP function on FGX.
spanning-tree {**enable** {**stp** | **rstp** [**protocol-migration**]} | **disable**}	Enable STP on a specific VLAN.
spanning-tree default	Reset STP configurations to their default values.
spanning-tree root {**primary** | **secondary**}	Set a VLAN as the primary or secondary root bridge.
unset spanning-tree root {**primary** | **secondary**}	Unset a primary or secondary root bridge.
spanning-tree bridge-priority	Set STP bridge priority.
spanning-tree interface port-priority	Set port priority for a specified interface.
spanning-tree interface path-cost	Set the port path cost for a specified interface.
spanning-tree interface edge-port	Set a specified interface as an edge port.
unset spanning-tree interface edge-port	Unset a specified interface as an edge port.
spanning-tree forward-delay	Set forward delay time.
spanning-tree hello-time	Set hello time.
spanning-tree max-age	Set maximum lifetime of BPDUs.

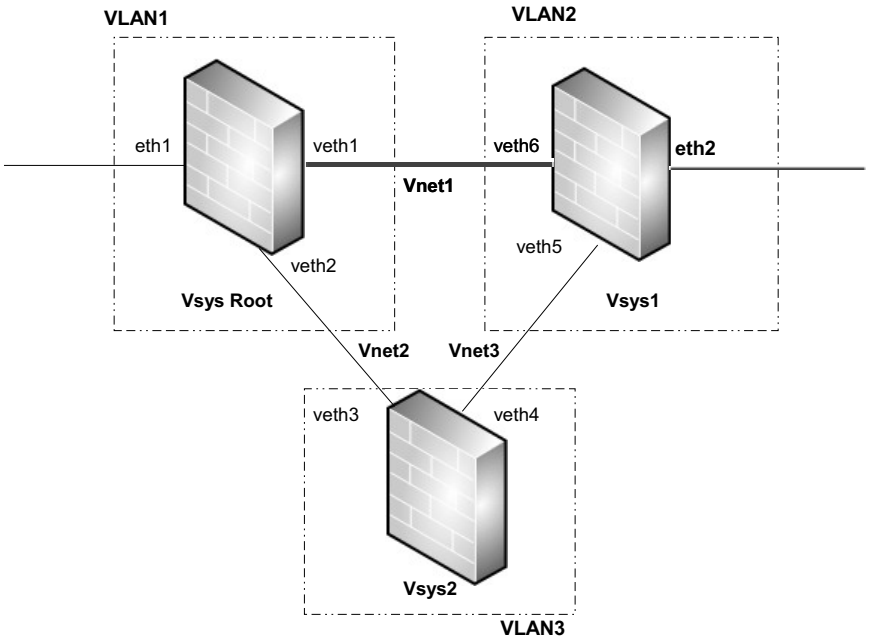
4.19.3 Example: STP Application

This example shows a simple application of STP to check whether any ports are blocked in a redundant network and whether any ports are used when the primary link fails.

You need to set up the following topology on FGX:

- Create VLAN1, VLAN2, and VLAN3. Create veth1 through veth6 and assign interfaces to the VLANs: eth1,veth1, and veth2 are assigned to VLAN1; veth3 and veth4 to VLAN3; eth2, veth5, and veth6 to VLAN2.
- Create Vsys1 and Vsys2. Assign VLAN2 to Vsys1, and VLAN3 to Vsys2.
- Create Vnet1, Vnet2, and Vnet3. Assign veth1 and veth6 to Vnet1 to connect Vsys Root and Vsys1, veth2 and veth3 to Vnet2 to connect Vsys Root and Vsys2, veth4 and veth5 to Vnet3 to connect Vsys1 and Vsys2.
- Enable STP on VLAN1, VLAN2, and VLAN3; set VLAN1 as the root bridge; and set the port path cost of veth5 as 10, veth6 as 20, and use the default port path cost 200,000,000 for other virtual interfaces.

Figure 15 Link Redundancy Topology



This example shows how to perform the following configurations through the WebUI and CLI:

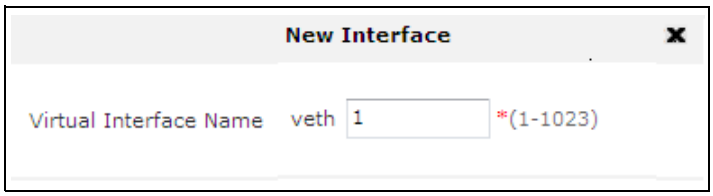
- 1. Create Interfaces
- 2. Create Virtual Systems
- 3. Create Virtual Networks
- 4. Configure STP
- 5. View Results

1. Create Interfaces

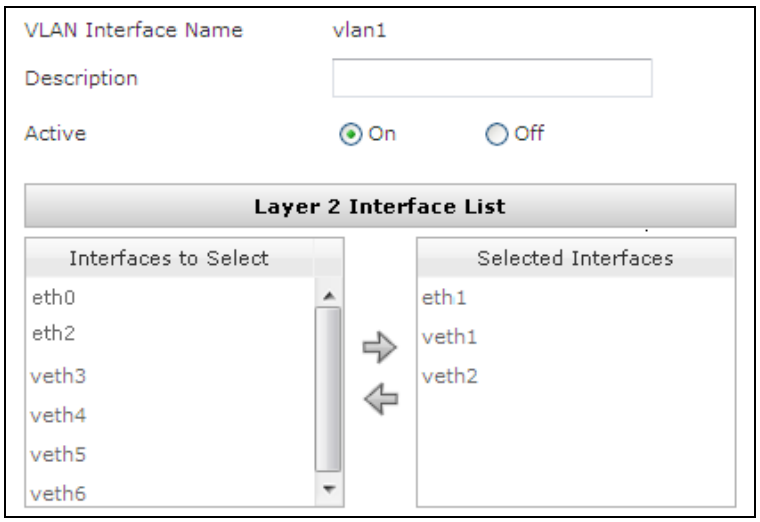
WebUI

1. Choose **Network > Interfaces**.
2. Click **New**. Choose **VLAN** and create VLAN1.

3. VLAN2 and VLAN3 are created the same way.
4. Click **New**. Choose **Virtual Interface** and create veth1.



5. The virtual interfaces veth2 through veth6 are created the same way.
6. In **Interfaces List**, click corresponding to VLAN1 to open the Edit page.
7. In **Layer 2 Interface List**, choose eth1, veth1, and veth2 from **Interfaces to Select** and click to add them to **Selected Interfaces** on the right. These interfaces are assigned to VLAN1.



8. Click **OK**.
9. Assign eth2, veth5, and veth6 to VLAN2; assign veth3 and veth4 to VLAN3.
10. Click .

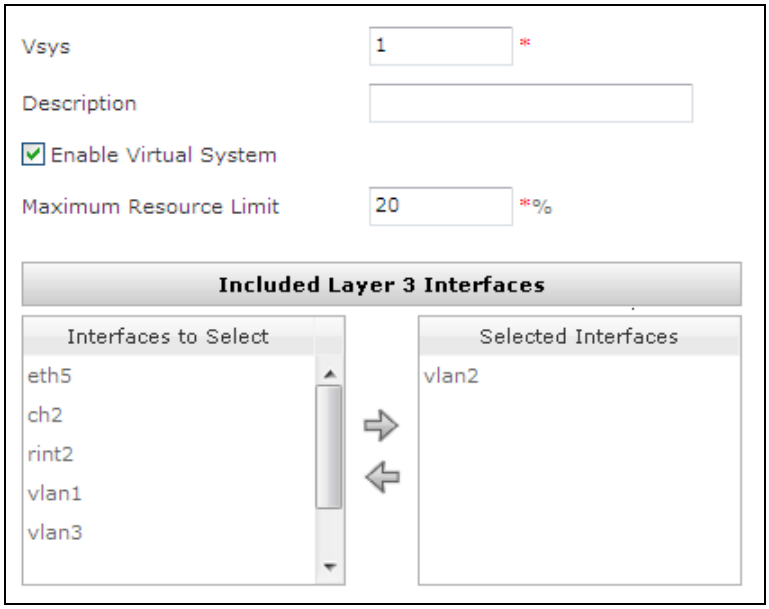
CLI

```
FGX@root> configure mode
FGX@root-system] vlan 1
FGX@root-system-vlan1] vlan 2
FGX@root-system-vlan2] vlan 3
FGX@root-system-vlan3] veth 1
FGX@root-system-veth1] veth 2
FGX@root-system-veth2] veth 3
FGX@root-system-veth3] veth 4
FGX@root-system-veth4] veth 5
FGX@root-system-veth5] veth 6
FGX@root-system-veth6] exit
FGX@root-system] vlan 1
FGX@root-system-vlan1] hold ethernet eth1
FGX@root-system-vlan1] hold veth veth1,veth2
FGX@root-system-vlan1] vlan 2
FGX@root-system-vlan2] hold ethernet eth2
FGX@root-system-vlan2] hold veth veth5,veth6
FGX@root-system-vlan2] vlan 3
FGX@root-system-vlan3] hold veth veth3,veth4
FGX@root-system-vlan3] end
FGX@root> save config
```

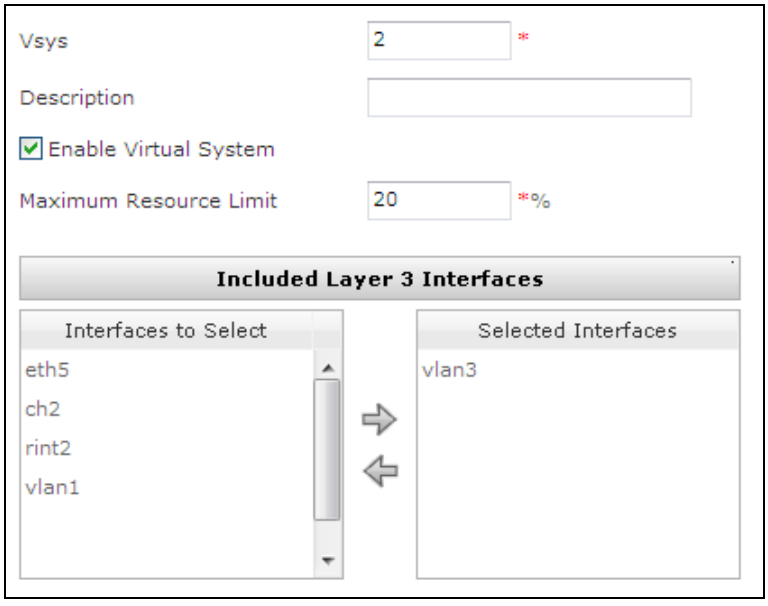
2. Create Virtual Systems

WebUI

1. Choose **System > Virtual Systems > Virtual Systems**.
2. Click **New**. Create Vsys1 and assign VLAN2 to Vsys1.



3. Click **New**. Create Vsys2 and assign VLAN3 to Vsys2.



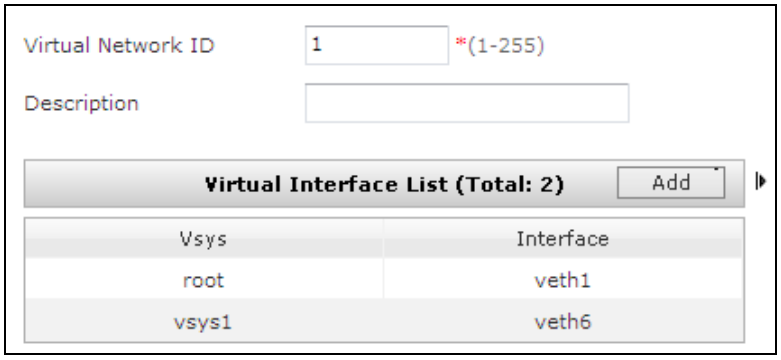
4. Click **OK**.
5. Click .

CLI

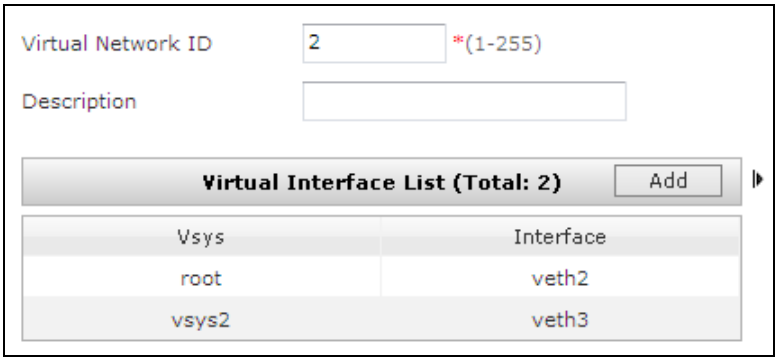
```
FGX@root> configure mode
FGX@root-system] vsys 1 resource-limit 20
FGX@root-system-vsys1] hold vlan 2
FGX@root-system-vsys1] exit
FGX@root-system] vsys 2 resource-limit 20
FGX@root-system-vsys2] hold vlan 3
FGX@root-system-vsys2] end
FGX@root> save config
```

3. Create Virtual Networks

1. Choose **System > Virtual Systems > Virtual Networks**.
2. Click **New**. Create Vnet1 and configure as follows.

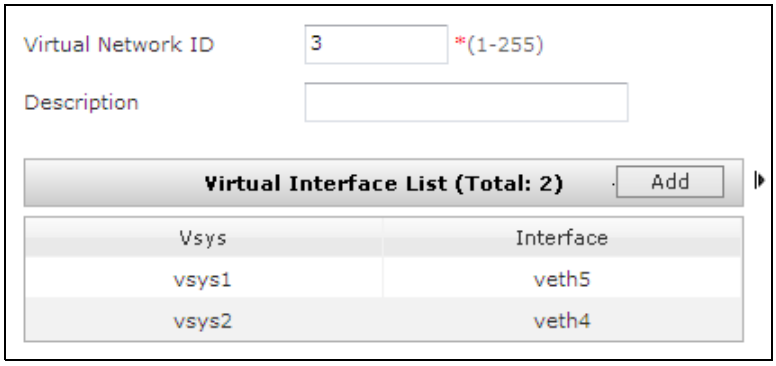


3. Click **OK**.
4. Click **New**. Create Vnet2 and configure as follows.



5. Click **OK**.

6. Click **New**. Create Vnet3 and configure as follows.



7. Click **OK**.
8. Click .

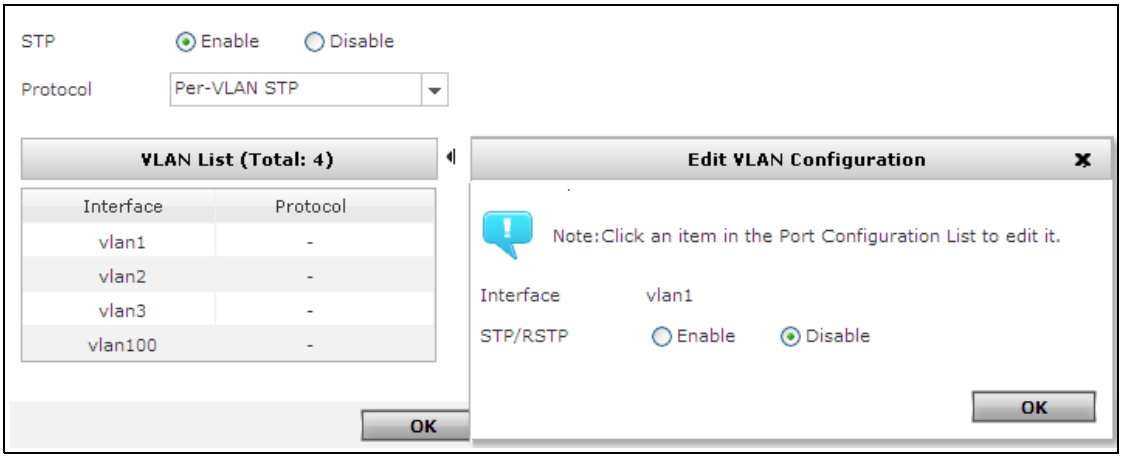
CLI

```
FGX@root> configure mode
FGX@root-system] vnet 1
FGX@root-system-vnet1] hold veth 1
FGX@root-system-vnet1] hold veth 6
FGX@root-system-vnet1] vnet 2
FGX@root-system-vnet2] hold veth 2
FGX@root-system-vnet2] hold veth 3
FGX@root-system-vnet2] vnet 3
FGX@root-system-vnet3] hold veth 4
FGX@root-system-vnet3] hold veth 5
FGX@root-system-vnet3] end
FGX@root> save config
```

4. Configure STP

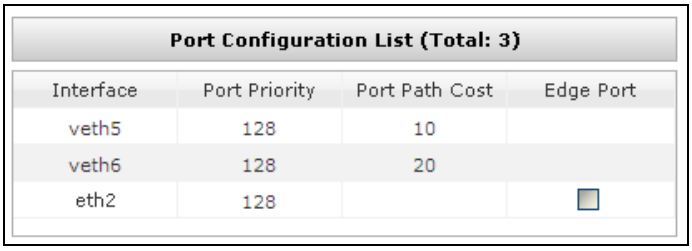
WebUI

1. Choose **Network > STP**.
2. Click **Enable** in the **STP** field.
3. Double-click VLAN1 in **VLAN List**, and the **Edit VLAN Configuration** window pops up.



4. Click **Enable** in the **STP/RSTP** field and set VLAN1 as the root bridge.

5. Click **OK**.
6. Double-click VLAN2 in **VLAN List**, and the **Edit VLAN Configuration** window pops up.
7. Click **Enable** in the **STP/RSTP** field.
8. In **Port Configuration List**, click veth5 and enter 10 in the **Port Path Cost** field; click veth 6 and enter20 in the field.



9. Click **OK**.
10. Double-click VLAN3 in **VLAN List**, and the **Edit VLAN Configuration** window pops up.
11. Click **Enable** in the **STP/RSTP** field.
12. Click **OK** twice.
13. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] spanning-tree enable per-vlan-stp
FGX@root-system] vlan 1
FGX@root-system-vlan1] spanning-tree enable stp
FGX@root-system-vlan1] spanning-tree root primary
FGX@root-system-vlan1] vlan 2
FGX@root-system-vlan2] spanning-tree enable stp
FGX@root-system-vlan2] spanning-tree interface veth5 path-cost 10
FGX@root-system-vlan2] spanning-tree interface veth6 path-cost 20
FGX@root-system-vlan2] vlan 3
FGX@root-system-vlan3] spanning-tree enable stp
FGX@root-system-vlan3] end
FGX@root> save config
```

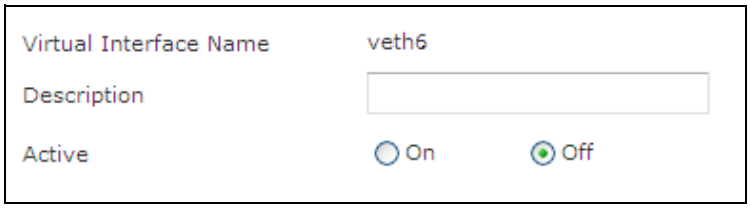
5. View Results

After completing the operations above, you can view realtime STP information in the WebUI or the CLI. Choose **Monitor > STP** or use the **show spanning-tree vlan** command in the CLI. Because VLAN1 is the root bridge, veth6 becomes the root port for VLAN2 and veth3 for VLAN3. veth5 is the designated port for this network because it has a smaller path cost (20+10=30) as compared to veth4 (200,000,000x2=400,000,000). veth4 is neither the root port nor the designated port so it's blocked. You will see that veth4 is in the Blocking state and the other interfaces are in the Forwarding state.

You can manually disable veth6 and check whether the blocked port veth4 is enabled to ensure network link connectivity.

WebUI

1. Choose **Network > Interfaces**.
2. In **Interface List**, click corresponding to veth6 to open the Edit page and disable veth6.



3. Click **OK**.
4. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] veth 6
FGX@root-system-veth6] shutdown
FGX@root-system-veth6] end
FGX@root> save config
```

After completing the operations above, you can see the STP information on the STP page in the WebUI. This page will display that veth6 is in the Disable state and the other interfaces are in the Forwarding state. You can see the realtime STP information using the **show spanning-tree vlan** command in the CLI.

4.19.4 Parameter reference

On FGX, STP can be configured only in the root Vsys. STP configurations can be viewed in any Vsys. STP does not support HA synchronization.

Table 123 Parameters of STP

Param	Description
STP	Enable or disable Spanning Tree Protocol (STP) on FGX. STP is disabled by default. When STP is disabled, FGX supports BPDU transparent transmission for STP and RSTP. That is, it does not process received BPDUs but directly forwards them.
Protocol	Comprises only one option of Per-VLAN STP.
VLAN List	• **Interface—**a VLAN interface that you can enable STP/RSTP for. • **Protocol—**STP, RSTP, or Enforce RSTP. When a Layer 2 interface is added to a VLAN, FGX automatically detects the interface and assign it a set of default STP configurations, such as port path cost. You can double-click a VLAN item in the list to open the **Edit VLAN Configuration** page.
STP/RSTP	Enable or disable STP/RSTP on a VLAN. Each VLAN has separate STP configurations. Disabled by default. When a VLAN comprises no Layer 2 interfaces, STP operations do not work even if STP/RSTP is enabled.
Restore Default Settings	Click **Reset** to restore default STP configurations for the current VLAN.
Type	The type of STP protocol to be used by a bridge, including: • **STP—**indicates that a bridge supports STP only. This is the default. • **RSTP—**a bridge supports RSTP but will automatically use STP when the bridge connected to it uses STP. • **Enforce RSTP—**forced to run RSTP and will not be compatible with STP devices in a Layer 2 network.
Root Bridge	Set current VLAN as the root bridge of the Layer 2 bridged network. A Layer 2 network can only have one root bridge.If multiple bridges are configured as root bridge in the same Layer 2 network, the MAC addresses of those bridges will be compared to determine the bridge with the lowest MAC address be the root bridge. Priority is 0.
Secondary Root Bridge	Set current VLAN as secondary root bridge of the Layer 2 bridged network. A secondary root bridge backs up the root bridge. A Layer 2 network can host multiple secondary root bridges. Priority is 4,096.
Bridge Priority	Customize VLAN bridge priority. Root bridge (default), secondary root bridge, and bridge priority are wholly exclusive. The priority range is 0-61,440 and must be a multiple of 4,096. The default priority is 32,768.
Port Priority	Set the priority of all ports comprised in a VLAN. The port priority range is 0-240 and must be a multiple of 16. The default priority is 128.
Port Path Cost	Set path cost for all ports comprised in a VLAN. The cost range is 1-200,000,000. By default, the system automatically determines path cost according to the port link speed. The higher the link speed, the lower the cost.
Edge Port	Set a Layer 2 Ethernet interface working in access mode as the edge port. An edge port can quickly transition to the forwarding state without delay, facilitating convergence. When you uncheck **Edge Port** or the edge port receives BPDUs from the network, it becomes a normal STP port that participates in STP algorithm calculation.

4.20 Neighbor Discovery

- 4.20.1 Overview
- 4.20.2 Basic Configuration Steps
- 4.20.3 ND Examples
- 4.20.4 Parameter reference

4.20.1 Overview

The Neighbor Discovery (ND) protocol is used by nodes (hosts and routers) to discover the neighbors on the same link so that they can communicate with each other.

- ND Message Types.

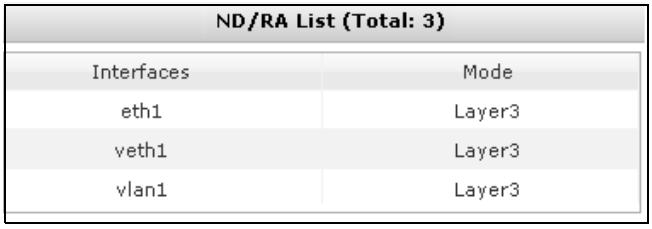
Table 124 ND Message Types

Message Type	ICMPv6 Type Value	Functionality
Router Solicitation (RS)	133	When IPv6 is enabled on an interface, a host sends an RS message to request a router to generate RA messages quickly without having to wait at scheduled intervals.
Router Advertisement (RA)	134	A router sends an RA message in response to an RS message or periodically sends unsolicited RA messages to hosts, informing of its existence and advertising link parameters and network parameters, such as prefixes and current hop limit.
Neighbor Solicitation (NS)	135	A node sends an NS message to obtain link-layer address of a neighbor, verify whether a neighbor is reachable, or request for duplicate address detection.
Neighbor Advertisement (NA)	136	A node sends an NA message in response to an NS message or periodically sends unsolicited NA messages to inform neighbors of the link-layer address change.
Redirect	137	A router sends a Redirect message to inform a source host of a better next-hop node to get to a destination.

- ND Mechanisms. ND offers the following main mechanisms to address the issues related to communication and interaction between neighboring nodes on the network:
  - Router/Prefix/Parameter Discovery
  - Next-Hop Determination
  - Address Resolution & Neighbor Unreachability Detection
  - Stateless Address Autoconfiguration & Duplicate Address Detection
  - Redirect

4.20.2 Basic Configuration Steps

1. Choose **Network > IPv6 > Neighbor Discovery**.
2. Configure as follows:



Before you configure ND, choose **Network > Interfaces** and enable IPv6 on a Layer 3 or shared Layer 3 interface.

Table 125 ND Commands

ipv6 nd dad detect	Set the number of sending Neighbor Solicitation (NS) messages for Duplicate Address Detection (DAD).
ipv6 nd reachable-time	Set a specified interface to maintain the neighbor reachable time.
ipv6 nd retrans-timer	Set the interval of retransmitting NS messages for a specified interface.
ipv6 nd ra suppress	Suppress a specified interface from sending RA messages.
unset ipv6 nd ra suppress	Allow a specified interface to send RA messages.
ipv6 nd ra router-lifetime	Set the router lifetime in RA messages.
ipv6 nd ra interval	Set the interval of advertising RA messages.
ipv6 nd ra hop-limit	Set a hop limit in RA messages.
ipv6 nd ra managed-flag {**on** | **off**}	Set the Managed Address Configuration flag in RA messages.
ipv6 nd ra other-flag {**on** | **off**}	Set the Other Configuration flag in RA messages.
ipv6 nd ra retrans-timer {**on** | **off**}	Set whether to carry the interval of retransmitting NS messages in RA messages.
ipv6 nd ra reachable-time {**on** | **off**}	Set whether to carry in RA messages the length of time an interface maintains its neighbor reachable status.
ipv6 nd ra link-address {**on** | **off**}	Set whether to carry the MAC address of an interface in RA messages.
ipv6 nd ra advlinkmtu {**on** | **off**}	Set whether to carry the MTU of an interface in RA messages.
ipv6 nd ra prefix	Set the prefix information and related parameters advertised by RA messages.
unset ipv6 nd ra prefix	Delete the prefix information and related parameters from RA messages.

4.20.3 ND Examples

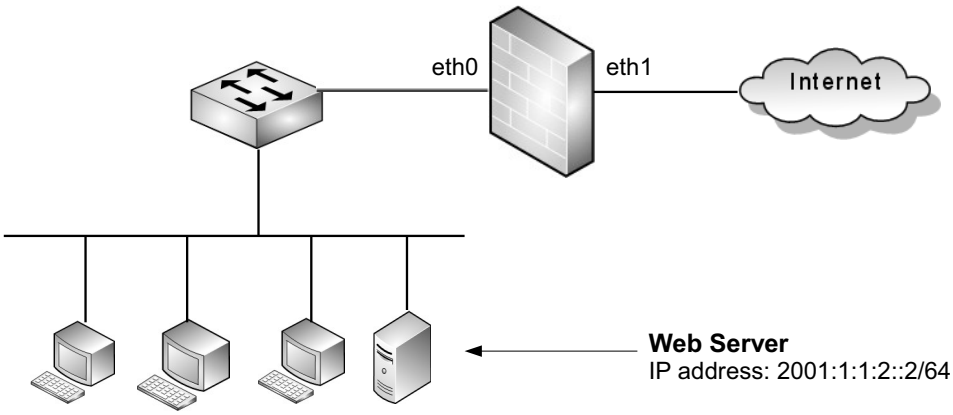
- Example 1: Duplicate Address Detection
- Example 2: Configure Router Advertisement

Note: Before you configure ND, choose **Network > Interfaces** and enable IPv6 on a Layer 3 or shared Layer 3 interface.

Example 1: Duplicate Address Detection

The interface eth0 of FGX is connected to the intranet. There is a Web server residing in the intranet with the IP address 2001:1:1:2::2/64.

Figure 16 Configuring Neighbor Discovery

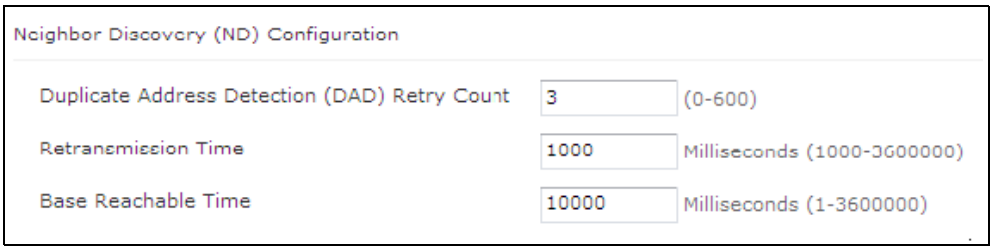


This example shows how to configure the following:

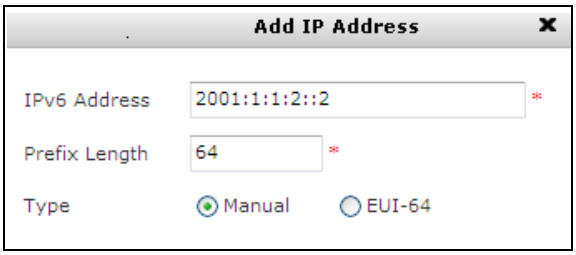
- The firewall device performs DAD (Duplicate Address Detection) with 3 attempts for eth0.
- ND messages are retransmitted from eth0 at the interval of 1,000 milliseconds.
- The approximate length of time eth0 maintains the neighboring Web server's reachability status is 10,000 milliseconds. If no reachability confirmation is received from the Web server during this time, eth0 will stop forwarding traffic to the server.
- Configure the interface eth0 with the IPv6 address 2001:1:1:2::2/64. The state of this IP address will then become DUPLICATE.
- Configure the interface eth0 with the IPv6 address 2001:1:1:2::1/64, which is unique in the intranet. The state of this IP address will then become PREFERRED.

WebUI

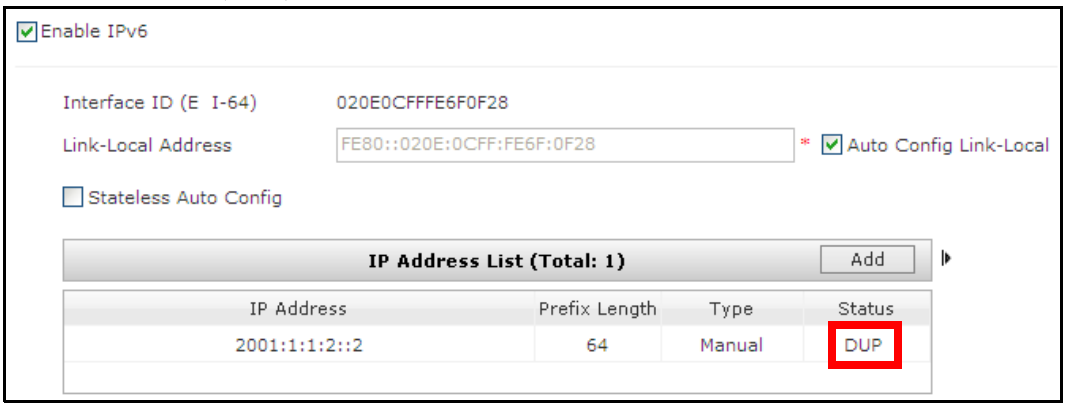
1. Choose **Network > IPv6 > Neighbor Discovery Configuration**.
2. In **ND/RA List**, click corresponding to eth0 to open the Edit page and configure as follows:



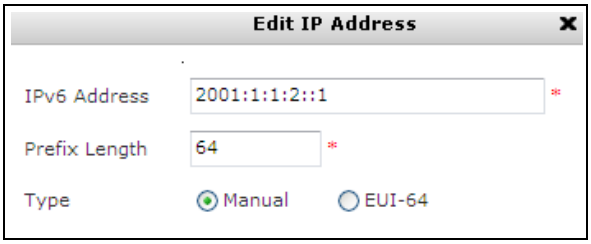
3. Click **OK**.
4. Choose **Network > Interfaces**.
5. Click corresponding to eth0 to open the Edit page.
6. In **IP Address List**, click **Add** to add an IPv6 address.



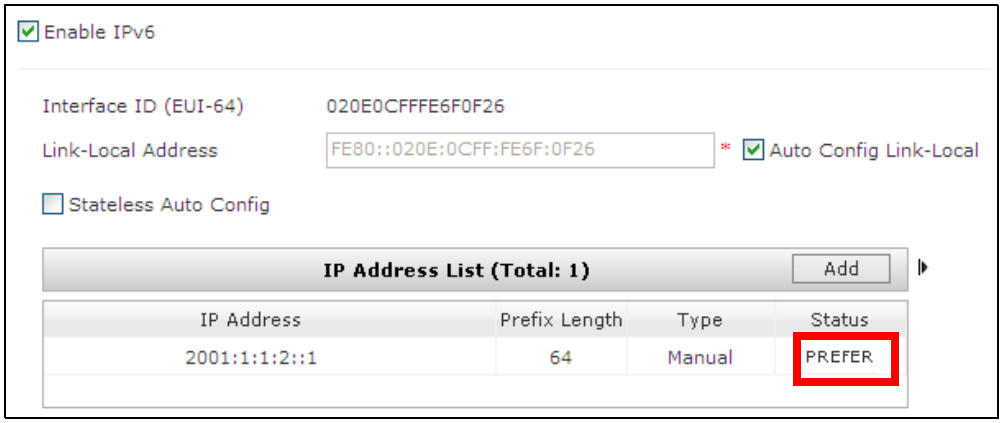
7. Click **OK**.
8. Click corresponding to eth0 to open the Edit page. View the interface status as DUPLICATE (DUP):



9. The IPv6 address 2001:1:1:2::1 is configured the same as step 6.



10. Click **OK**.
11. Click corresponding to eth0 to open the Edit page. View the interface status as PREFERRED (PREFER):



12. Click **OK**.
13. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] ipv6 enable
FGX@root-system-if-eth0] ipv6 nd dad detect 3
FGX@root-system-if-eth0] ipv6 nd retrans-timer 1000
FGX@root-system-if-eth0] ipv6 nd reachable-time 10000
FGX@root-system-if-eth0] ipv6 address 2001:1:1:2::2/64
FGX@root-system-if-eth0] ipv6 address 2001:1:1:2::1/64
FGX@root-system-if-eth0] end
FGX@root> save config
```

After completing the operations above, execute the **show interface ethernet 0** command and view the following:

- DAD is enabled with maximum 3 attempts, ND messages are transmitted every 1,000 milliseconds, and the base reachable time is 10,000 milliseconds.

```
ND DAD is enabled, number of DAD attempts 3
ND retransmit time is 1000 milliseconds
ND base reachable time is 10000 milliseconds
```

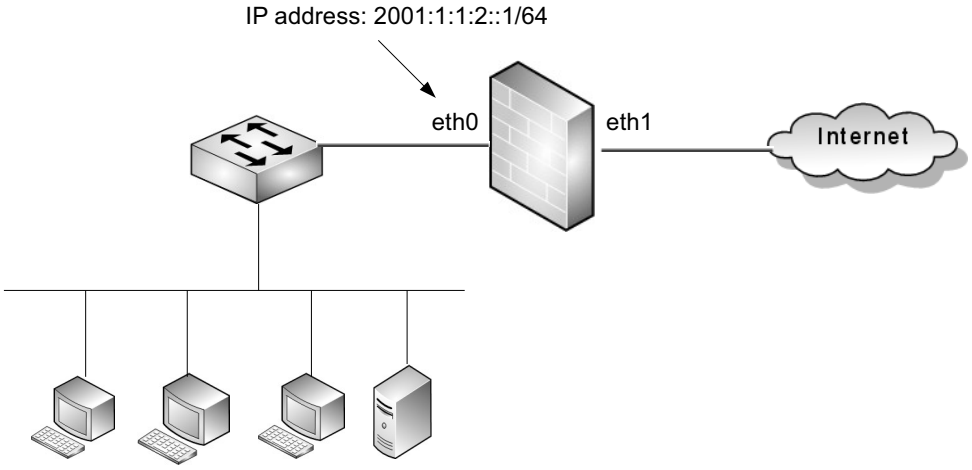
- The IPv6 address 2001:1:1:2::2 is in the DUP status, which means it is already used by another interface on the network. The address 2001:1:1:2::1/64 in the PREFER status can be configured on eth0.

```
Global unicast address(es):
  2001:1:1:2::2 , subnet is 2001:1:1:2::/64   [DUP]
  2001:1:1:2::1 , subnet is 2001:1:1:2::/64   [PREFER]
```

Example 2: Configure Router Advertisement

The interface eth0 of FGX is connected to the intranet, and the interface IP address is 2001:1:1:2::1/64.

Figure 17 Configuring RA

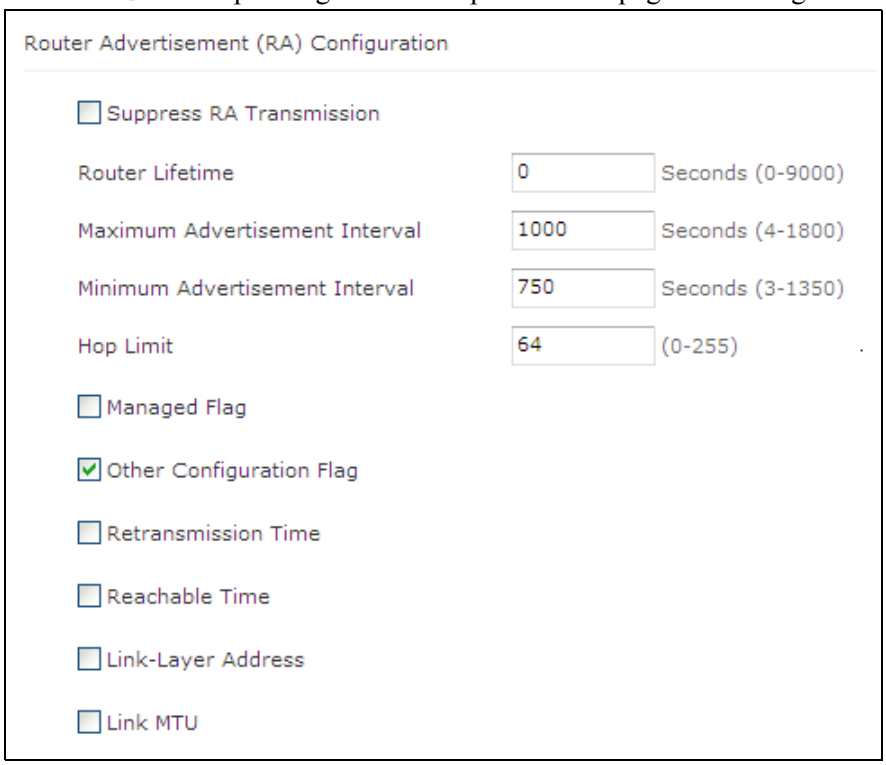


This example shows how to:

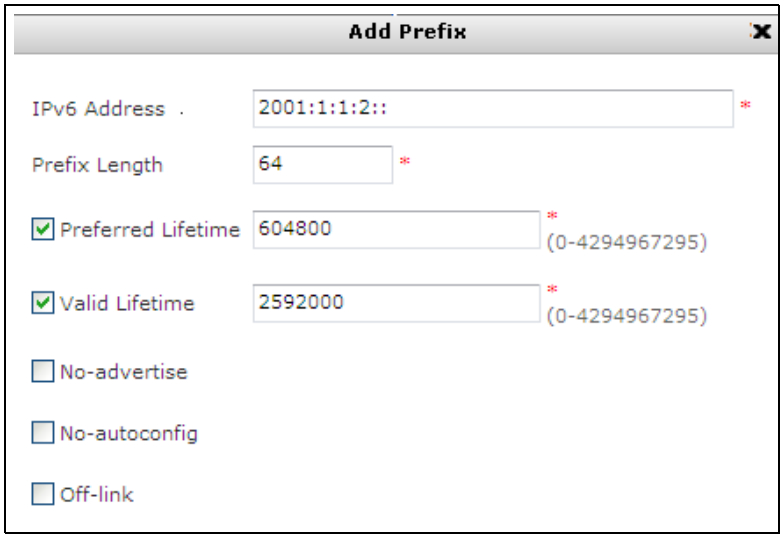
- Manually configure the IP address of eth0 as 2001:1:1:2::1/64.
- Configure RA for eth0:
  - RA parameters:
    - the interface eth0 can advertise RA messages to the intranet but it does not act as the default router;
    - RA messages are retransmitted at an interval of 750-1,000 seconds;
    - the hop limit is 64;
    - the hosts in the intranet can obtain IPv6 addresses only through stateless address autoconfiguration and they can obtain other network parameters through DHCPv6 stateless configuration;
    - RA messages do not carry the link-layer address and MTU of eth0.
  - Prefix information:
    - the prefix 2001:1:1:2::/64 is advertised;
    - the prefix is used in stateless address autoconfiguration for hosts in the intranet;
    - no on-link determination is performed.

WebUI

1. Choose **Network > IPv6 > Neighbor Discovery Configuration**.
2. Click corresponding to eth0 to open the Edit page and configure as follows:



3. In **Prefix List**, click **Add** to add a prefix.



4. Click **OK**.
5. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] ipv6 enable
FGX@root-system-if-eth0] ipv6 nd ra router-lifetime 0
FGX@root-system-if-eth0] ipv6 nd ra interval 750 1000
FGX@root-system-if-eth0] ipv6 nd ra hop-limit 64
FGX@root-system-if-eth0] ipv6 nd ra managed-flag off
FGX@root-system-if-eth0] ipv6 nd ra other-flag on
FGX@root-system-if-eth0] ipv6 nd ra link-address off
FGX@root-system-if-eth0] ipv6 nd ra advlinkmtu off
FGX@root-system-if-eth0] ipv6 nd ra prefix 2001:1:1:2::/64 valid-
lifetime default preferred-lifetime default no-adv off
no-autoconfig off off-link off
FGX@root-system-if-eth0] exit
FGX@root> save config
```

4.20.4 Parameter reference

Table 126 Parameters of ND

Parameter	Description
Duplicate Address Detection (DAD) Retry Count	Number of times for sending NS messages while performing DAD for an interface. The count range is 0-600, and the default count is 1.
Retransmission Time	The length of time between retransmissions of NS messages while performing DAD. The time range is 1,000-3,600,000 milliseconds, and the default time is 1,000 milliseconds. If a device receives no response within a specified retransmission time, it will continue to send NS messages until the number of NS messages sent reaches the DAD retry attempt limit. If there is still no response, the device will consider the address being detected as available.
Base Reachable Time	A base value for computing reachable time, during which an interface maintains a neighbor's reachable status. The interface forwards traffic to the neighbor within the reachable time. The time range is 1-3,600,000 milliseconds, and the default is 30,000 milliseconds.

Table 127 Parameters of RA

Parameter	Description
Suppress RA Transmission	Suppress RA message transmission on an interface. It is disabled by default, which indicates RA can be transmitted on a specified interface. During the initialization process, if you choose transparent mode, this function will be enabled by default; if you choose routing mode, this function will be disabled by default.
Router Lifetime	The router lifetime advertised in an RA message. That is, the length of time the device stays as a default router. The lifetime range is 0-9,000 seconds, and the default lifetime is 1,800 seconds. A lifetime of zero indicates that FGX is not a default router. Upon the receipt of an RA message, a host can determine whether to set the advertising device as the default router according to the lifetime value specified in the message.
Maximum Advertisement Interval	The maximum time allowed between transmissions of unsolicited RA messages. The interval range is 4-1,800 seconds, and the default interval is 600 seconds. This interval must be no greater than the router lifetime. After the maximum and minimum advertisement intervals are configured, the device will randomly select either as the interval of periodically advertising RA messages.
Minimum Advertisement Interval	The minimum time allowed between transmissions of unsolicited RA messages. The interval range is 3-1,350 seconds, and the default interval is 200 seconds. This interval must be no greater than 0.75 times the maximum advertisement interval.
Hop Limit	The hop limit advertised in an RA message. The range is 0-255, and the default hop limit is 64.
Managed Flag	With this function enabled, the interface receiving an RA message can obtain IPv6 addresses through stateful address autoconfiguration in addition to stateless address autoconfiguration; otherwise, it can only obtain IPv6 addresses through stateless address autoconfiguration. It is disabled by default.

Table 127 Parameters of RA (*continued*)

Parameter	Description
Other Configuration Flag	With this function enabled, the interface receiving an RA message can obtain other network configuration parameters other than IPv6 addresses through DHCPv6 stateless configuration; otherwise, it cannot obtain these parameters through DHCPv6 stateless configuration. It is disabled by default.
Retransmission Time	Indicates whether to carry Retransmission Time in an RA message. With this function enabled, the Retransmission Time value that you configure for ND will be carried in an RA message. When the device sends an NS message and receives no response within a specified interval, it will resend the NS message. It is disabled by default.
Reachable Time	Indicates whether to carry Reachable Time in an RA message. With this function enabled, the Reachable Time value that you configure for ND will be carried in an RA message. A neighbor is considered reachable within a specified reachable time. After the time expires, a node needs to verify again whether the neighbor is reachable through neighbor unreachability detection in order to communicate with the neighbor. It is disabled by default.
Link-Layer Address	Indicates whether to carry the Link-Layer Address in an RA message. With this function enabled, the source link-layer address of the advertising interface will be carried in the RA message. It is enabled by default.
Link MTU	Indicates whether to carry MTU in an RA message. With this function enabled, the MTU value of the advertising interface will be carried in the RA message. It is enabled by default.
Prefix List	Provides configuration information about prefixes advertised in RA messages. Configuration parameters include: • **IPv6 Address—**the prefix advertised by RA messages. • **Prefix Length—**the advertised prefix length. • **Preferred Lifetime—**the length of time an advertised prefix is preferred before it becomes deprecated. The lifetime range is 0-4,294,967,295 seconds, and the default is 604,800 seconds. It is enabled by default. • **Valid Lifetime—**the length of time an advertised prefix is valid before it becomes invalid. The lifetime range is s 0-4,294,967,295 seconds, and the default is 2,592,000 seconds. It is enabled by default. • **No-advertise—**not to advertise a prefix by an RA message. This function is disabled by default, which indicates the prefix is to be advertised by an RA message. • **No-autoconfig—**not to use a prefix for stateless address autoconfiguration. This function is disabled by default, which indicates the prefix can be used for stateless address autoconfiguration. • **Off-link—**set the prefix off-link. Upon receiving an RA message from FGX, the interface will determine whether it is on the same link as the advertising interface of FGX based on the L flag comprised in the RA message. This function is disabled by default, which indicates the prefix is on-link. You can add up to 32 advertised prefixes, which cannot be overlapped. In addition, the advertised prefixes cannot be link-local prefixes, all-zero prefixes, or multicast prefixes.

5 Network Address Translation

This chapter describes the network address translation (NAT) feature of FGX:

- 5.1. Overview. Describes NAT concepts and fundamentals.
- 5.2. Basic Configuration Steps. Describes basic configuration steps and the UI dialogs. Your scenario will not require all of these steps.
- 5.3. Examples. Describes how to configure different NAT types.
- 5.4. Parameter Reference. Describes in detail all parameters.

5.1.Overview

This section introduces basic NAT concepts. NAT rules define what packets are translated and how they are translated.

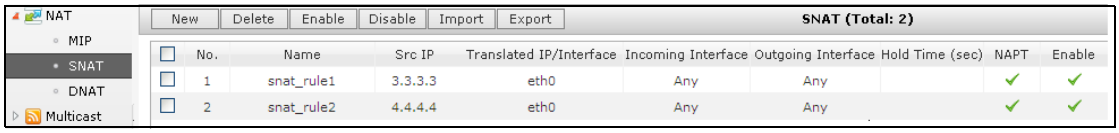
- 5.1.1. NAT Rule Creation and Selection describes NAT rules and how a rule is selected for a packet.
- The 3 NAT rule types are:
  - 5.1.2. SNAT Rules
  - 5.1.3. DNAT Rules
  - 5.1.4. MIP Rules
- 5.1.5. Import / Export describes NAT settings import/export.

5.1.1.NAT Rule Creation and Selection

- 5.1.1.1. Rule List
- 5.1.1.2. Rule Policy
- 5.1.1.3. Rule Priority (number)

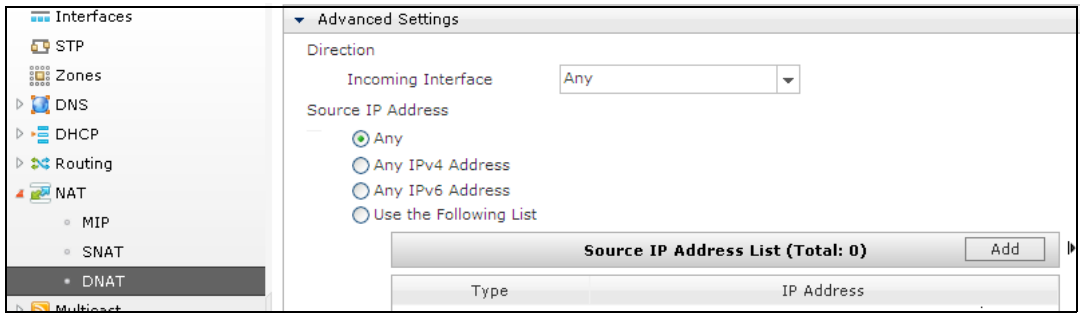
5.1.1.1.Rule List

You can create SNAT, DNAT, and MIP rules. A rule defines conditions for a packet to be translated.



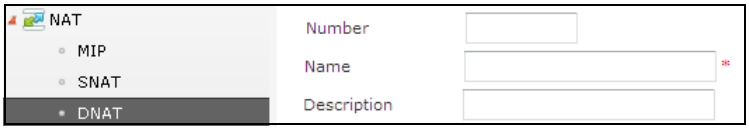
5.1.1.2.Rule Policy

You can set a rule policy that determines if the rule can be selected for the packet based on packet parameters (such as incoming interface, source IP address).



5.1.1.3.Rule Priority (number)

The matching rule with the lowest number has the highest priority. MIP rules take priority over SNAT and DNAT rules.



5.1.2.SNAT Rules

Translates private source IP addresses to public IP addresses. SNAT rules are typically used when an internal user accesses external network services.

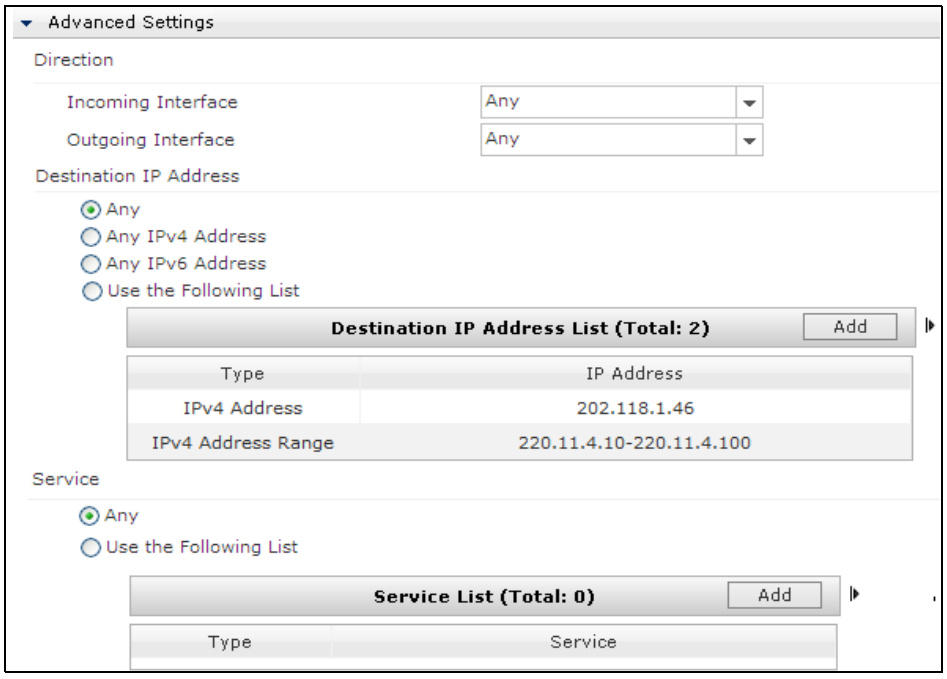
- 5.1.2.1. Policy and Priority
- 5.1.2.2. NAPT
- 5.1.2.3. Hold Time
- 5.1.2.4. One-to-One
- 5.1.2.5. Many-to-One
- 5.1.2.6. Many-to-Many

5.1.2.1.Policy and Priority

You can create policy-based SNAT rules. When receiving a packet from the internal network, if the packet does not belong to any existing session, matches no MIP policies, FGX will match it against SNAT rules and will translate the packet source IP address as specified in the highest-priority SNAT rule matching the packet. All subsequent packets of the same session are translated according to this rule.

SNAT rule matching conditions are:

- Direction
- Destination IP address
- Service



5.1.2.2.NAPT

NAPT can be enabled or disabled. When it is enabled, the port number is also translated. The translated port number can not be specified. For each translated IP address, port numbers are assigned from 65534 to 1024 repeatedly.

- One-to-one SNAT: Optional
- Many-to-one SNAT: Required
- Many-to-Many SNAT: Recommended

5.1.2.3.Hold Time

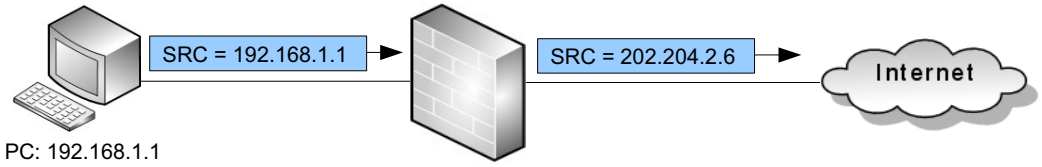
The length of time a mapping relationship will remain after all the corresponding sessions terminate.

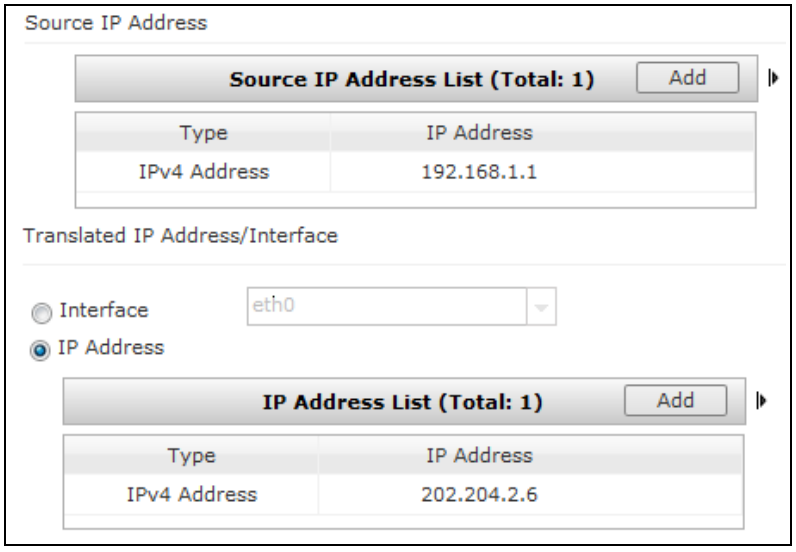
Hold time is required only when NAPT is disabled.

5.1.2.4.One-to-One

Translates one source IP address to one IP address or one interface IP address.

Figure 18 One-to-One SNAT



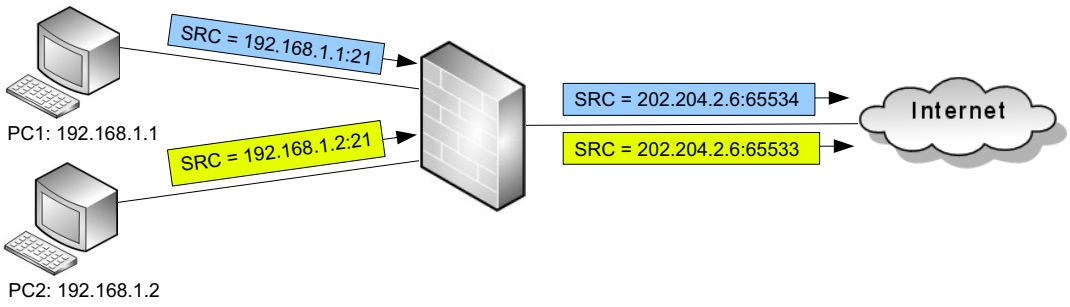


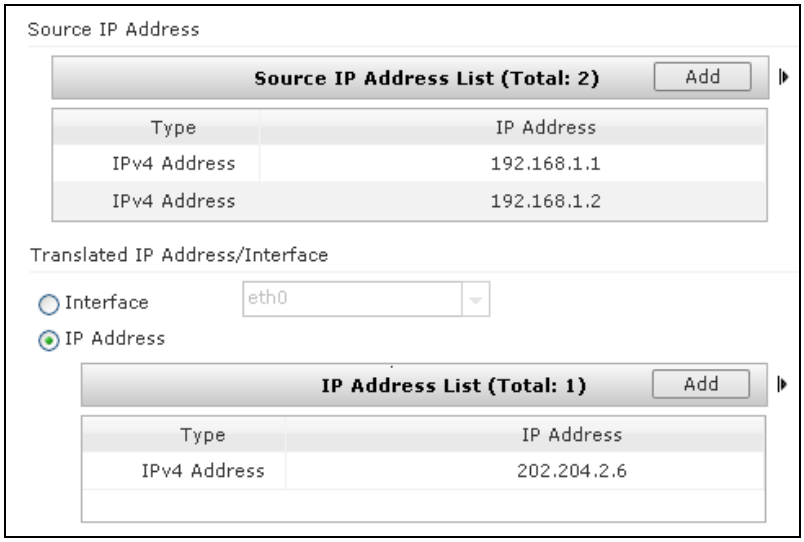
5.1.2.5.Many-to-One

Translates several source IP addresses to one IP address or one interface IP address.

NAPT is required (TCP and UDP packets), or else not all IP addresses can be translated simultaneously. For example, source IP addresses A and B both need to be translated to C. When FGX receives packets from A earlier, it translates A to C, and B needs to wait. Only when the session from A terminates and the hold time elapses can B be translated to C.

Figure 19 Many-to-One SNAT



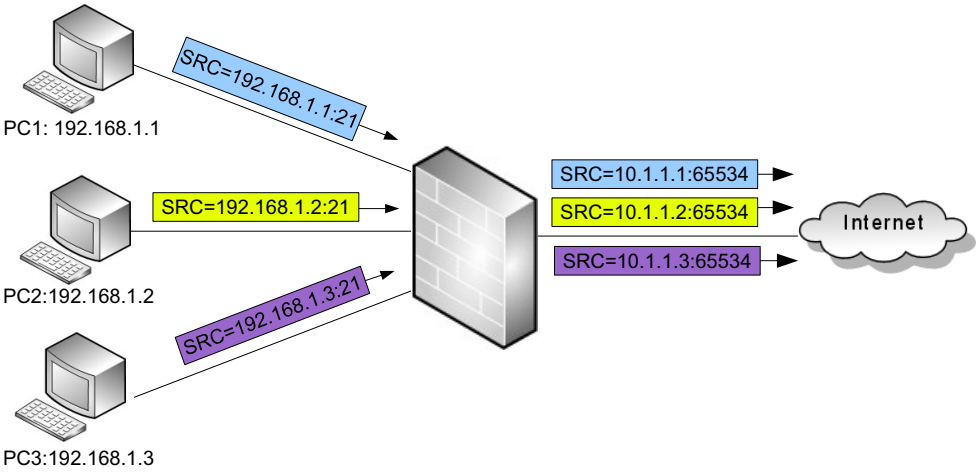


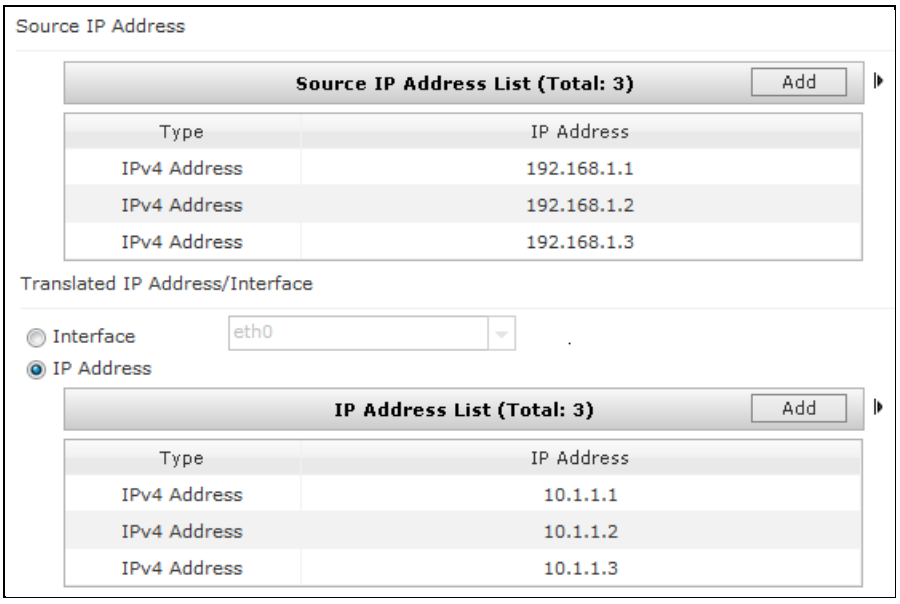
5.1.2.6.Many-to-Many

Translates multiple source IP addresses to multiple IP addresses or the IP addresses of an interface.

NAPT is recommended (TCP and UDP packets) to avoid that fewer translated IP addresses are assigned. For example, 6 client IP addresses all need to be translated, but there are only 5 translated IP addresses that can be assigned. In this case, one of the clients cannot get a translated IP address and thus cannot access the external network. When NAPT is enabled, two clients can use the same IP address with different port numbers, and all clients can access the external network.

Figure 20 Many-to-Many SNAT





5.1.3.DNAT Rules

Translates public destination IP addresses to private IP addresses. DNAT rules are typically used when an external client accesses internal network services.

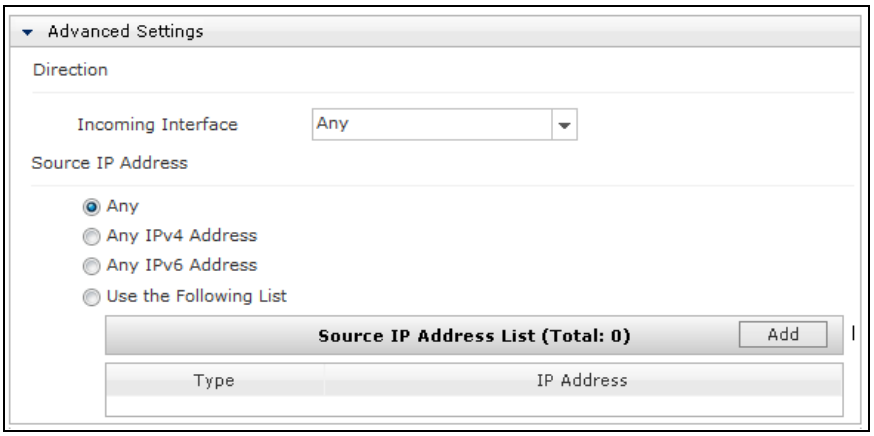
- 5.1.3.1. Policy and Priority
- 5.1.3.2. NAPT
- 5.1.3.3. One-to-One
- 5.1.3.4. One-to-Many
- 5.1.3.5. Load Balancing
- 5.1.3.6. Link Probes
- 5.1.3.7. Domain Name (DNS Rewrite)

5.1.3.1.Policy and Priority

You can create policy-based DNAT rules. When receiving a packet from the external network, if the packet does not belong to any existing session, matches no MIP policies, FGX will match it against DNAT rules and will translate the packet destination IP address as specified in the highest-priority DNAT rule matching the packet. All subsequent packets of the same session are translated according to this rule.

DNAT rule matching conditions are:

- Direction
- Source IP address



5.1.3.2.NAPT

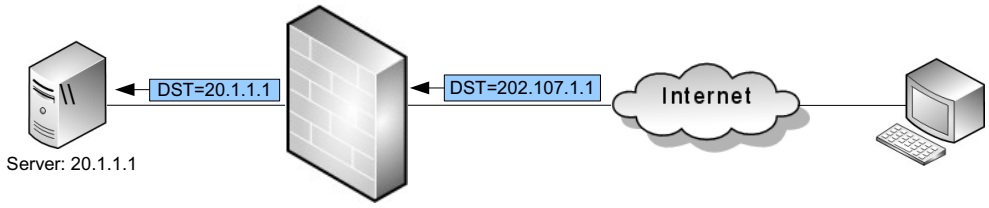
NAPT can be enabled or disabled. When it is enabled, the port number is also translated. You can specify translated port numbers.

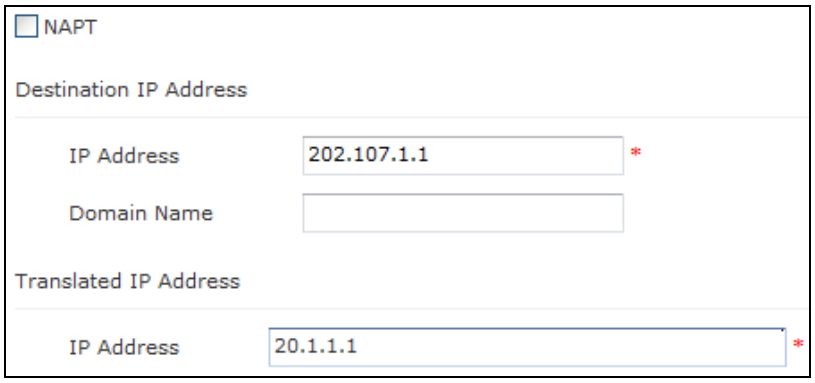
- One-to-one DNAT: Optional
- One-to-many DNAT: Required

5.1.3.3.One-to-One

Translates one destination IP address to one IP address.

Figure 21 One-to-One DNAT



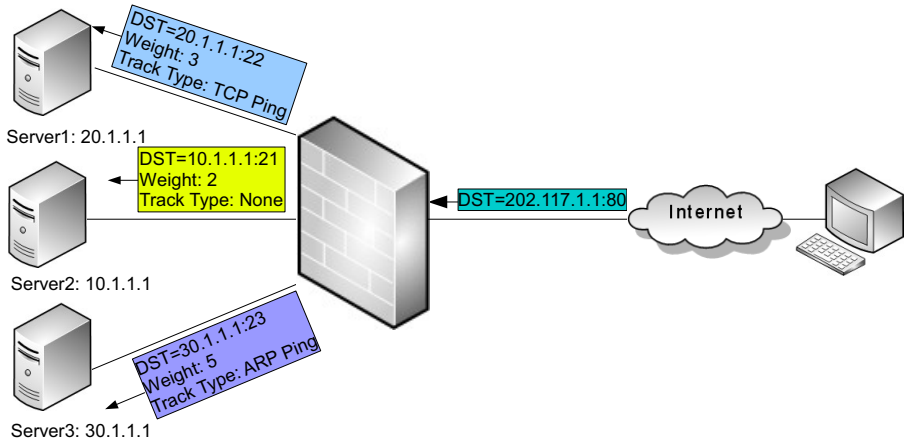


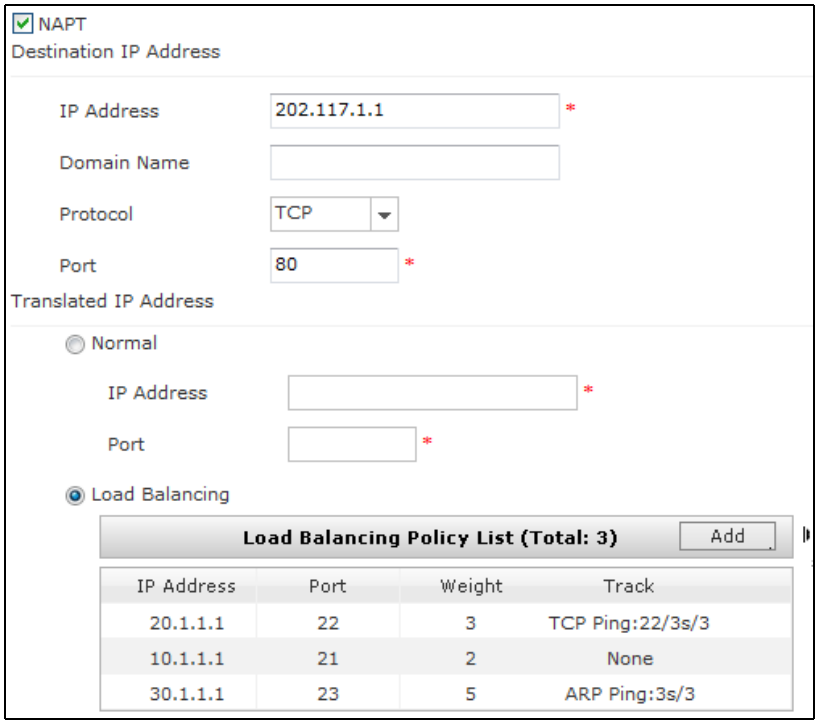
5.1.3.4.One-to-Many

Translates one destination IP address to multiple IP addresses.

NAPT is required (TCP and UDP packets) to realize load balancing. For example, an external user wants to access internal FTP service through FGX. When receiving a packet from the user, if the packet matches a DNAT rule, FGX translates the packet destination IP address to two internal FTP server IP addresses A and B (as specified in the matching DNAT rule) with port numbers which define the same service type. Now the session can be allocated properly to two servers, and if link failure occurs on one server, the user can continue to access another server.

Figure 22 One-to-Many DNAT





5.1.3.5.Load Balancing

With DNAT-based load balancing, a new session is allocated to several links according to server weight in order to avoid server overload or unavailable services due to link failure.

5.1.3.6.Link Probes

Used when DNAT-based load balancing is enabled. A session is allocated to several servers and FGX tests the connectivity between the servers and itself using link probe. If one link fails, the corresponding server weight becomes 0, and the session is continued on the other servers. The server weight recovers together with the link.

FGX provides four types of link probes:

- ARP Probe
- TCP Probe
- ICMP Probe
- NS Probe

For information, see 6.1.1.2 Load balancing / link probe.

5.1.3.7.Domain Name (DNS Rewrite)

You can set domain names corresponding to destination IP addresses in DNAT rules. When FGX receives a packet from a DNS server, it matches the packet destination IP address corresponding to the domain name against DNAT rules. If a matching rule is found, the packet destination IP address will be translated to the IP address specified in the DNAT rule.

5.1.4.MIP Rules

MIP is a direct one-to-one mapping of a private IP address to a public IP address without NAPT. MIP is bidirectional.

- 5.1.4.1. Policy and Priority
- 5.1.4.2. Domain Name (DNS Rewrite)

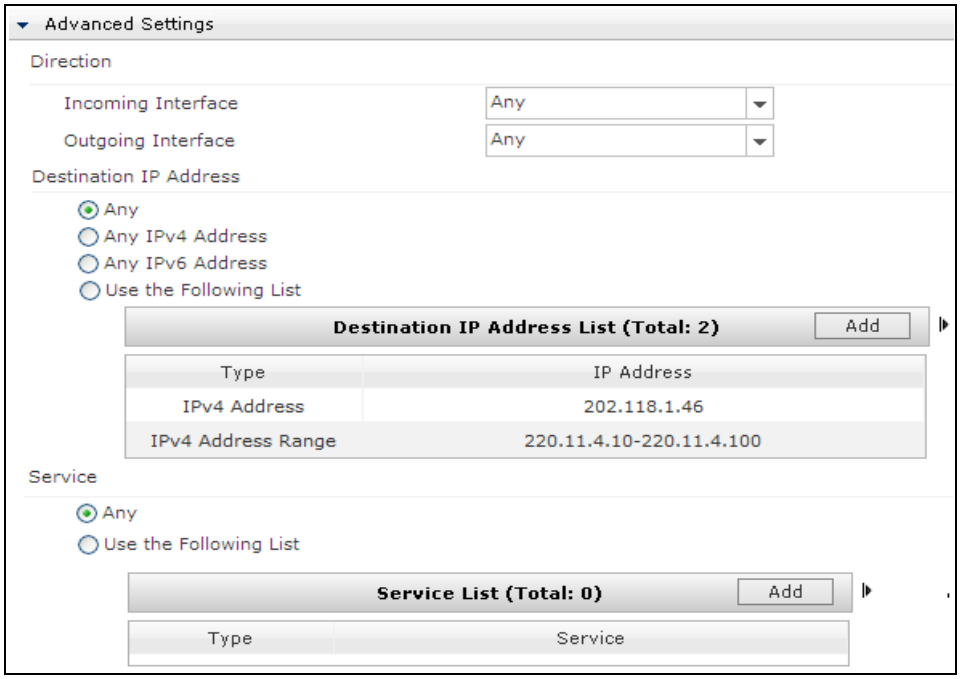
5.1.4.1.Policy and Priority

You can create policy-based MIP rules. When receiving a packet, if the packet does not belong to any existing session, FGX will match it against MIP rules and will translate the packet IP address as specified in the highest-priority MIP rule matching the packet. All subsequent packets of the same session are translated according to this rule.

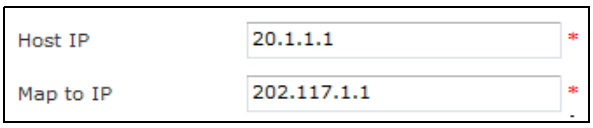
MIP rules take priority over SNAT and DNAT rules. If a packet does not match a MIP rule, FGX will continue to match it against SNAT or DNAT rules.

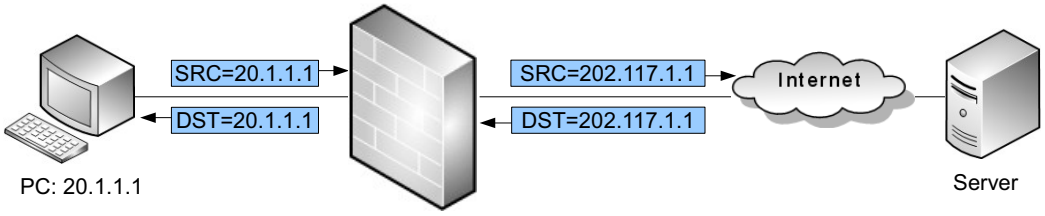
MIP rule matching conditions are:

- Direction
- Destination IP address
- Service



The mapping relationship is set up by configuring a host IP and a mapping IP.





5.1.4.2.Domain Name (DNS Rewrite)

You can set domain names corresponding to destination IP addresses in MIP rules. When FGX receives a packet from a DNS server, it matches the packet destination IP address corresponding to the domain name against MIP rules. If a matching rule is found, the packet destination IP address will be translated to the IP address specified in the MIP rule.

5.1.5.Import / Export

You can import any existing NAT rules or export NAT configurations to text files.

5.2.Basic Configuration Steps

This section describes the basic configuration procedure. For your scenario you will do only a subset of the steps listed below (see example scenarios in 5.3. Examples).

- 5.2.1. Create SNAT Rule
- 5.2.2. Create DNAT Rule
- 5.2.3. Create MIP Rule

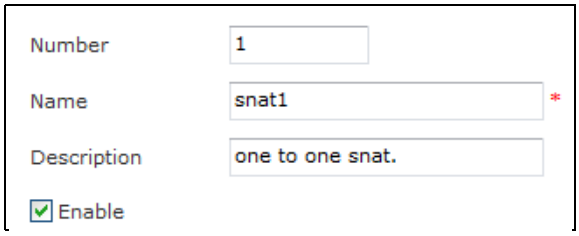
Note
IPv4 and IPv6 addresses cannot be set for the same SNAT, DNAT, or MIP rule.

5.2.1.Create SNAT Rule

- 5.2.1.1. Create Rule
- 5.2.1.2. Advanced Settings
- 5.2.1.3. One-to-One SNAT without NAPT
- 5.2.1.4. Many-to-One SNAT with NAPT
- 5.2.1.5. Many-to-Many SNAT with NAPT

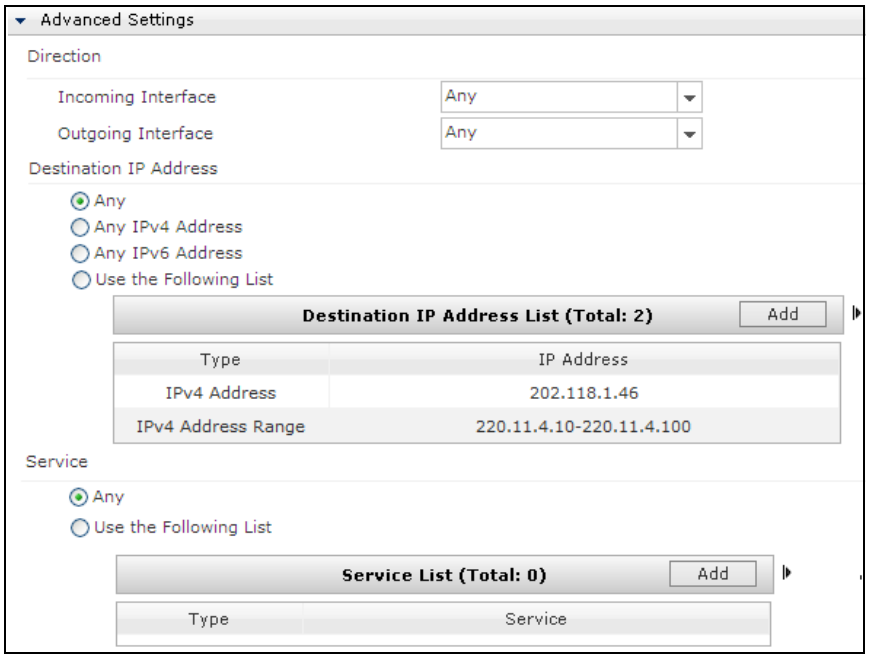
5.2.1.1.Create Rule

1. Choose **Network** > **NAT** > **SNAT**.
2. Click **New** to create an SNAT rule. Specify rule name, description, and number (priority) and enable or disable the rule.



5.2.1.2.Advanced Settings

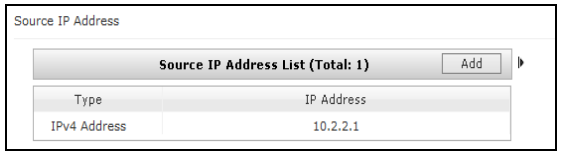
In **Advanced Settings** section, set matching conditions. Only packets matching all conditions can be translated.



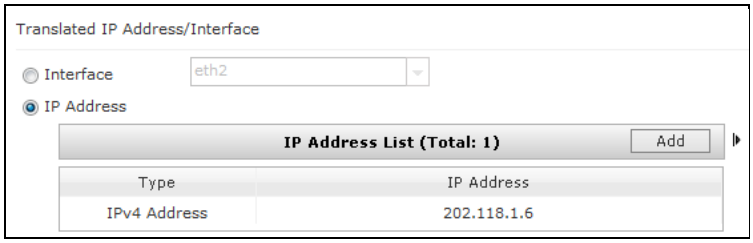
5.2.1.3.One-to-One SNAT without NAPT

1. Uncheck **NAPT** and set hold time.

2. Add a source IP address to **Source IP Address List**.



3. Choose an interface from the **Interface** drop-down list or add a translated IP address to **IP Address List**.



5.2.1.4.Many-to-One SNAT with NAPT

1. Check **NAPT**.
2. Add multiple source IP addresses to **Source IP Address List**.
3. Choose an interface from the **Interface** drop-down list or add a translated IP address to **IP Address List**.

5.2.1.5.Many-to-Many SNAT with NAPT

1. Check **NAPT**.
2. Add multiple source IP addresses to **Source IP Address List**.
3. Add multiple translated IP addresses to **IP Address List**.

Table 128 SNAT Rule Commands

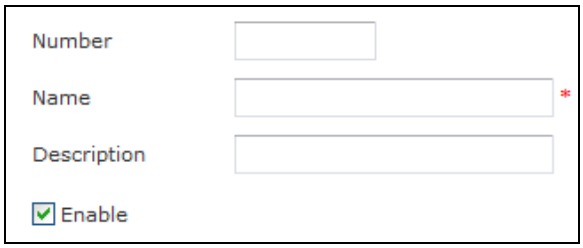
policy snat *policy_name*	Adds a SNAT rule.
policy snat *policy_name* append	Adds source/translated IP addresses.
policy snat *policy_name* **description**	Adds description for a rule.
policy snat *policy_name* {**enable** | **disable**}	Enables or disables a rule.
policy snat *policy_name* **matching**	Adds criteria for matching packets.
policy snat *policy_name* **number** *pri*	Changes the priority of a rule.
show policy snat [*policy_name*]	Displays rule information.
unset policy snat [*policy_name*]	Deletes rules.
unset policy snat *policy_name* **matching**	Deletes criteria for matching packets.

5.2.2.Create DNAT Rule

- 5.2.2.1. Create Rule
- 5.2.2.2. Advanced Settings
- 5.2.2.3. One-to-One DNAT without NAPT
- 5.2.2.4. One-to-One DNAT with NAPT
- 5.2.2.5. One-to-Many DNAT with NAPT

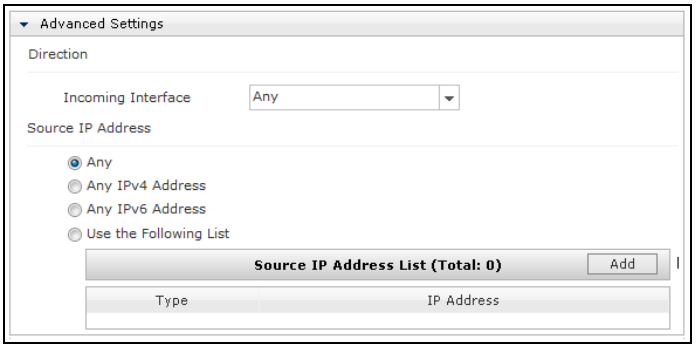
5.2.2.1.Create Rule

1. Choose **Network** > **NAT** > **DNAT**.
2. Click **New** to create a DNAT rule. Specify rule name, description, and number (priority). Enable or disable the rule.



5.2.2.2.Advanced Settings

In **Advanced Settings** section, set matching conditions. Only packets matching all conditions can be translated.

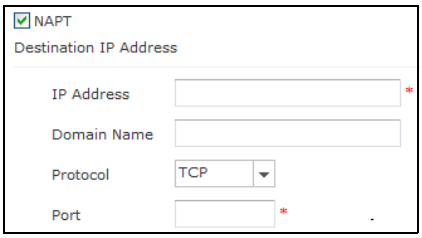


5.2.2.3.One-to-One DNAT without NAPT

1. Uncheck **NAPT**.
2. Add a destination IP address (or a domain name) and a translated IP address.

5.2.2.4.One-to-One DNAT with NAPT

1. Check **NAPT**.
2. In the **Destination IP Address** section, add a destination IP address (or a domain name) and corresponding port number and specify a protocol type.



3. In the **Translated IP Address** section, click **Normal** and add an IP address and corresponding port number.

5.2.2.5.One-to-Many DNAT with NAPT

1. Check **NAPT**.
2. In the **Destination IP Address** section, Add a destination IP address (or a domain name) and corresponding port number and specify a protocol type.
3. In the **Translated IP Address** section, click **Load Balancing** and add load balancing policies (IP address, destination port, weight, and track type) to **Load Balancing Policy List**.

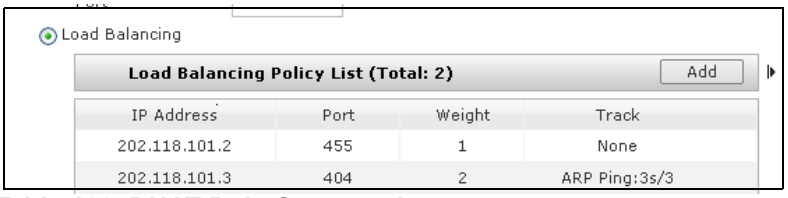


Table 129 DNAT Rule Commands

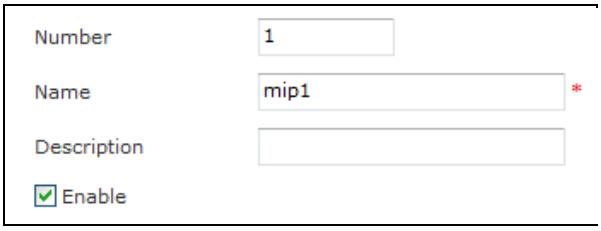
policy dnat *policy_name*	Adds a DNAT rule.
policy dnat *policy_name* **load-balancing**	Adds a rule with load-balancing.
policy dnat *policy_name* **description**	Adds description for a rule.
policy dnat *policy_name* {**enable** | **disable**}	Enables or disables a rule.
policy dnat *policy_name* **matching**	Adds criteria for matching packets.
policy dnat *policy_name* **number** *pri*	Changes the priority of a rule.
show policy dnat [*policy_name*]	Displays rule information.
unset policy dnat [*policy_name*]	Deletes rules.
unset policy dnat *policy_name* **matching**	Deletes criteria for matching packets.

5.2.3.Create MIP Rule

- 5.2.3.1. Create Rule
- 5.2.3.2. Advanced Settings
- 5.2.3.3. One-to-One Mapping

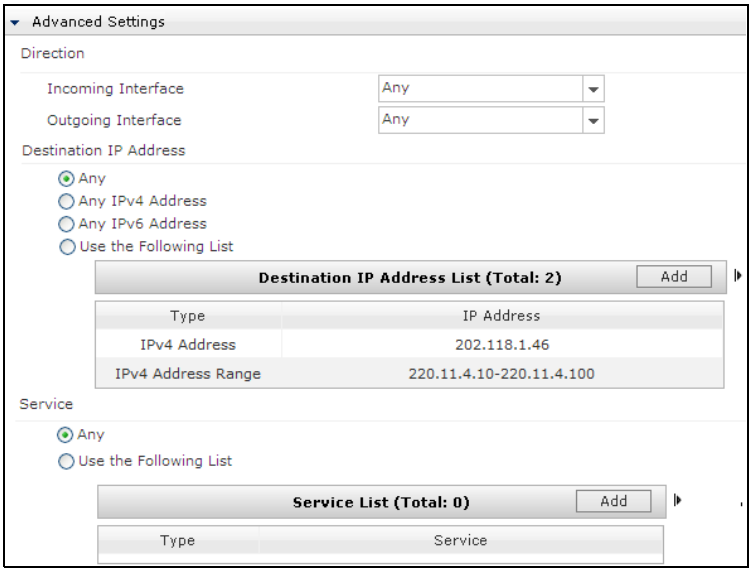
5.2.3.1.Create Rule

1. Choose **Network** > **NAT** > **MIP**.
2. Click **New** to create an MIP rule. Specify rule name, description, and number (priority). Enable or disable the rule.



5.2.3.2.Advanced Settings

In **Advanced Settings** section, set matching conditions. Only packets matching all conditions can be translated.



5.2.3.3.One-to-One Mapping

Enter a host IP and a translated IP it maps to (or a corresponding domain name).

Table 130 MIP Rule Commands

policy mip *policy_name*	Adds a MIP rule.
policy mip *policy_name* **description**	Adds description for a rule.

Table 130 MIP Rule Commands (*continued*)

policy mip *policy_name* {**enable** | **disable**}	Enables or disables a rule.
policy mip *policy_name* **matching**	Adds criteria for matching packets.
policy mip *policy_name* **number** *pri*	Changes the priority of a rule.
show policy mip [*policy_name*]	Displays rule information.
unset policy mip [*policy_name*]	Deletes rules.
unset policy mip *policy_name* **matching**	Deletes criteria for matching packets.

5.3.Examples

This section gives the following examples about how to configure NAT rules:

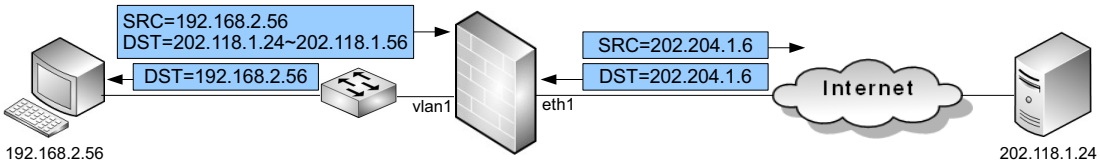
- Example 1: Create One-to-One SNAT Rule
- Example 2: Create Many-to-One SNAT Rule with NAPT
- Example 3: Create One-to-One DNAT Rule
- Example 4: Create One-to-Many DNAT Rule with NAPT
- Example 5: Create MIP Rule
- Example 6: DNS Rewrite

Example 1: Create One-to-One SNAT Rule

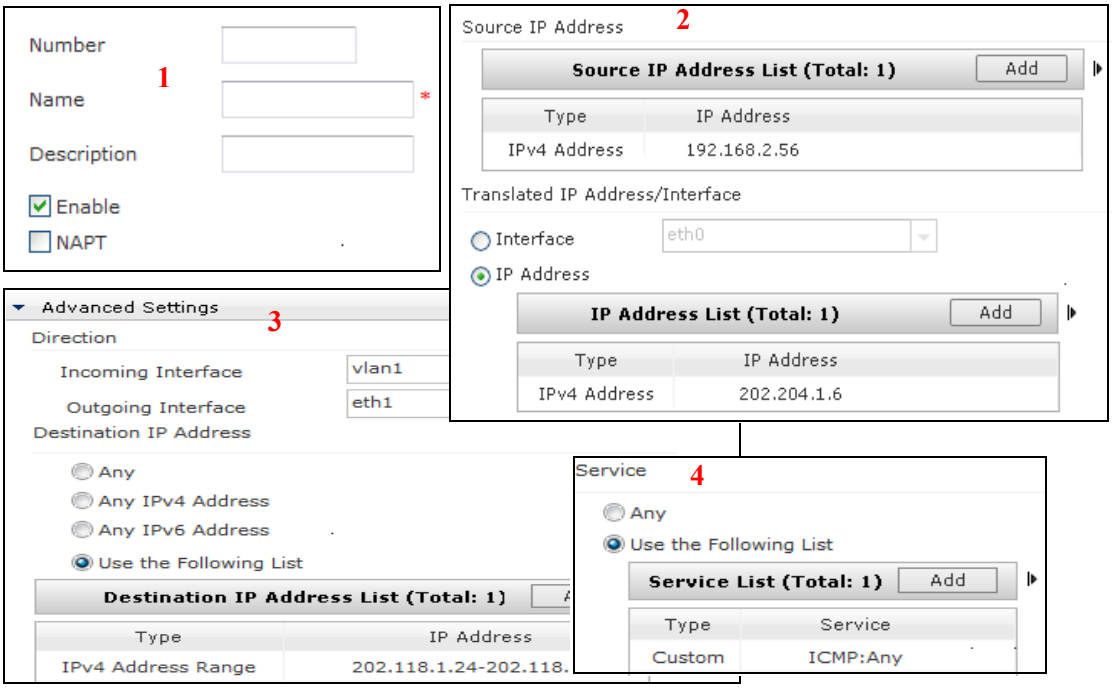
In this example, you want an internal host (IP: 192.168.2.56) to access the Internet using a public IP address 202.204.1.6. You configure a one-to-one SNAT rule and require FGX to perform SNAT on packets from the host only when the following requirements are satisfied:

1. The destination IP address range is 202.118.1.24-202.118.1.56.
2. The incoming and outgoing interfaces are vlan1 and eth1.
3. The service type is ICMP any.

Figure 23 One-to-One SNAT



1. Choose **Network** > **NAT** > **SNAT** and click **New** to create the following SNAT rule:



2. Click **OK**.
3. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] policy snat snat1 iplist 192.168.2.56 iplist
202.204.1.6 napt enable
FGX@root-system] policy snat snat1 matching input-interface vlan1
FGX@root-system] policy snat snat1 matching output-interface eth1
FGX@root-system] policy snat snat1 matching dip 202.118.1.24
202.118.1.56
FGX@root-system] policy snat snat1 matching protocol icmp any
FGX@root-system] exit
FGX@root> save config
```

SNAT result seen from the external server:

Source	Destination	Protocol	Info
202.204.1.6	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.6	ICMP	Echo (ping) reply
202.204.1.6	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.6	ICMP	Echo (ping) reply

SNAT result seen from the internal client:

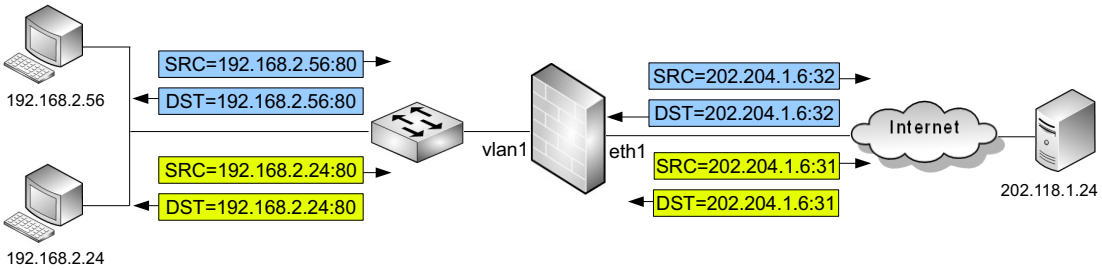
Source	Destination	Protocol	Info
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply

Example 2: Create Many-to-One SNAT Rule with NAPT

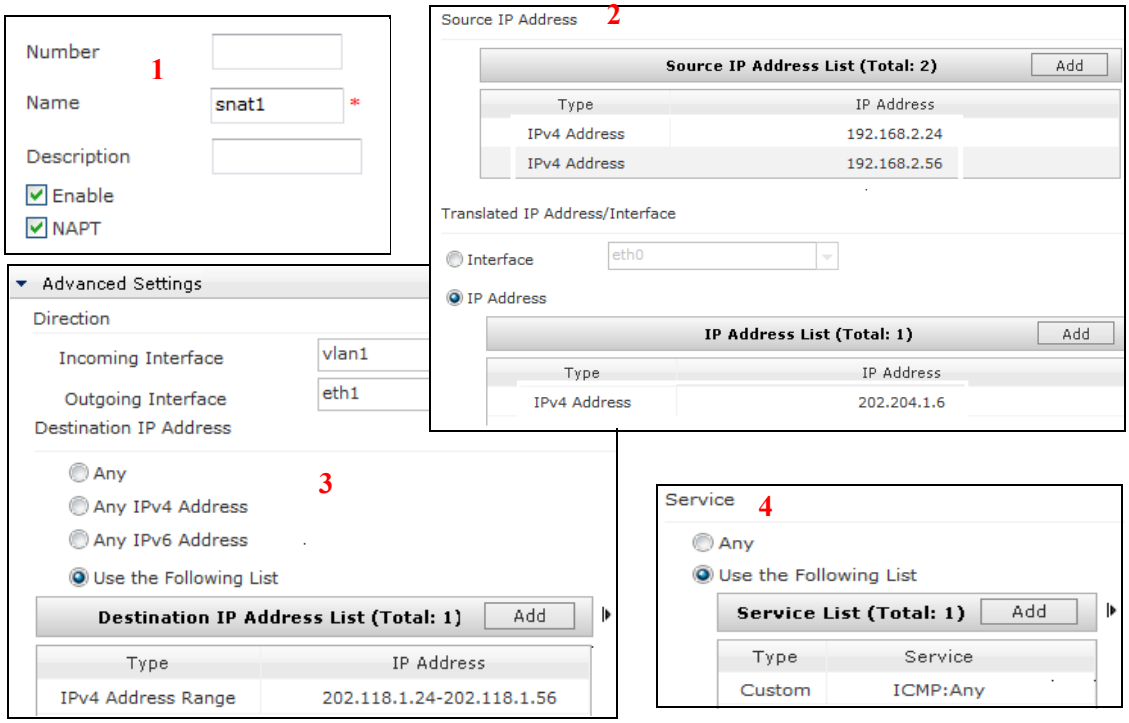
In this example, you want two internal hosts (IP: 192.168.2.56 and 192.168.2.24) to access the Internet using a public IP address 202.204.1.6. You configure a many-to-one SNAT rule with NAPT enabled and require FGX to perform SNAT on packets from the hosts when the following requirements are satisfied:

1. The destination IP addresses range is 202.118.1.24-202.118.1.56.
2. The incoming and outgoing interfaces are vlan1 and eth1.
3. The service type is ICMP any.

Figure 24 Port-Based SNAT



1. Choose **Network** > **NAT** > **SNAT** and click **New** to create the following SNAT rule:



2. Click **OK**.
3. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] policy snat snat1 iplist
192.168.2.24,192.168.2.56 iplist 202.204.1.6 napt enable
FGX@root-system] policy snat snat1 matching input-interface vlan1
FGX@root-system] policy snat snat1 matching output-interface eth1
FGX@root-system] policy snat snat1 matching dip 202.118.1.24
202.118.1.56
FGX@root-system] policy snat snat1 matching protocol icmp any
FGX@root-system] exit
FGX@root> save config
```

SNAT result seen from the external server:

Source	Destination	Protocol	Info
202.204.1.6	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.6	ICMP	Echo (ping) reply
202.204.1.6	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.6	ICMP	Echo (ping) reply

SNAT result seen from the internal client:

Source	Destination	Protocol	Info
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply

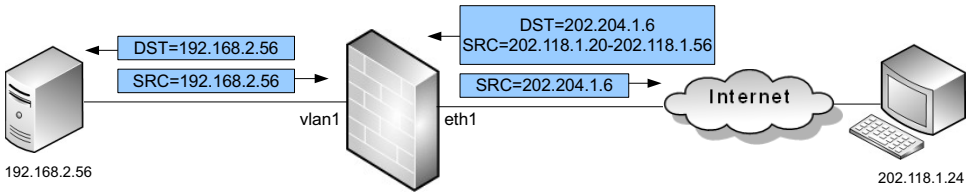
Source	Destination	Protocol	Info
192.168.2.24	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.24	ICMP	Echo (ping) reply
192.168.2.24	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.24	ICMP	Echo (ping) reply

Example 3: Create One-to-One DNAT Rule

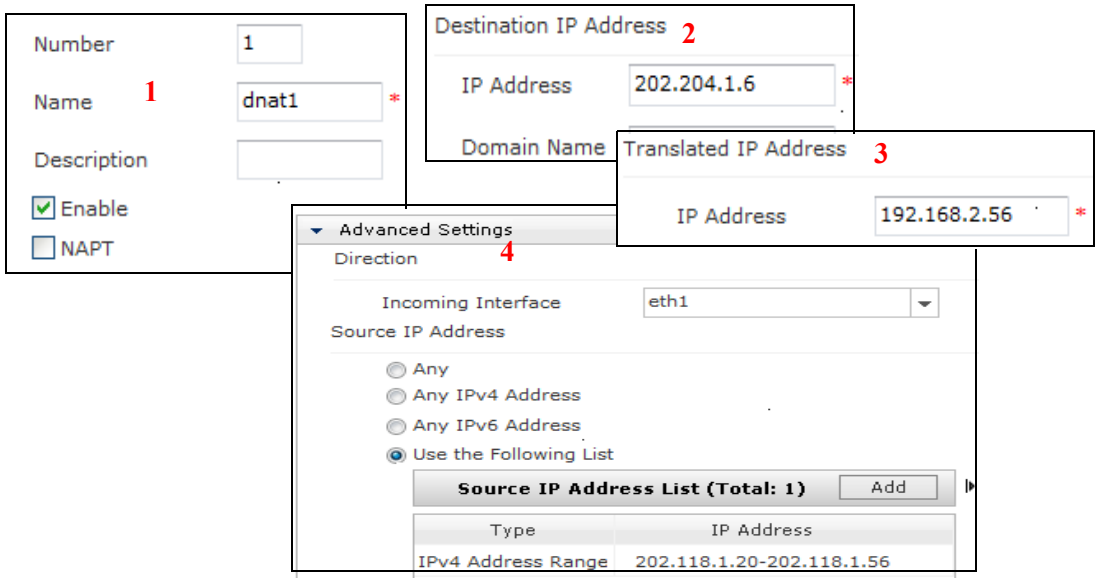
In this example, you want external hosts to access an internal server (IP: 192.168.2.56) using a public IP address 202.204.1.6. You configure a one-to-one DNAT rule and require FGX to perform DNAT on the packets from the Internet only when the following requirements are satisfied:

1. The source IP addresses range of the external hosts are 202.118.1.20-202.118.1.56.
2. The incoming interface is eth1.

Figure 25 Network Topology of DNAT



1. Choose **Network** > **NAT** > **DNAT** and click **New** to create the following DNAT rule:



2. Click **OK**.
3. Click  .

CLI

```
FGX@root> configure mode
FGX@root-system] policy dnat dnat1 202.204.1.6 192.168.2.56 enable
FGX@root-system] policy dnat dnat1 matching input-interface eth1
FGX@root-system] policy dnat dnat1 matching sip 202.118.1.20
202.118.1.56
FGX@root-system] exit
FGX@root> save config
```

DNAT result seen from the external client:

Source	Destination	Protocol	Info
202.118.1.24	202.204.1.6	ICMP	Echo (ping) request
202.204.1.6	202.118.1.24	ICMP	Echo (ping) reply
202.118.1.24	202.204.1.6	ICMP	Echo (ping) request
202.204.1.6	202.118.1.24	ICMP	Echo (ping) reply

DNAT result seen from the internal server:

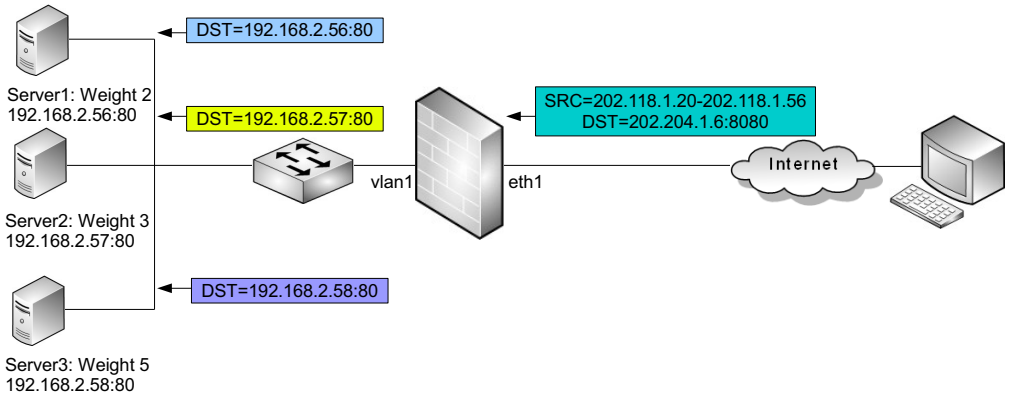
Source	Destination	Protocol	Info
202.118.1.24	192.168.2.56	ICMP	Echo (ping) request
192.168.2.56	202.118.1.24	ICMP	Echo (ping) reply
202.118.1.24	192.168.2.56	ICMP	Echo (ping) request
192.168.2.56	202.118.1.24	ICMP	Echo (ping) reply

Example 4: Create One-to-Many DNAT Rule with NAPT

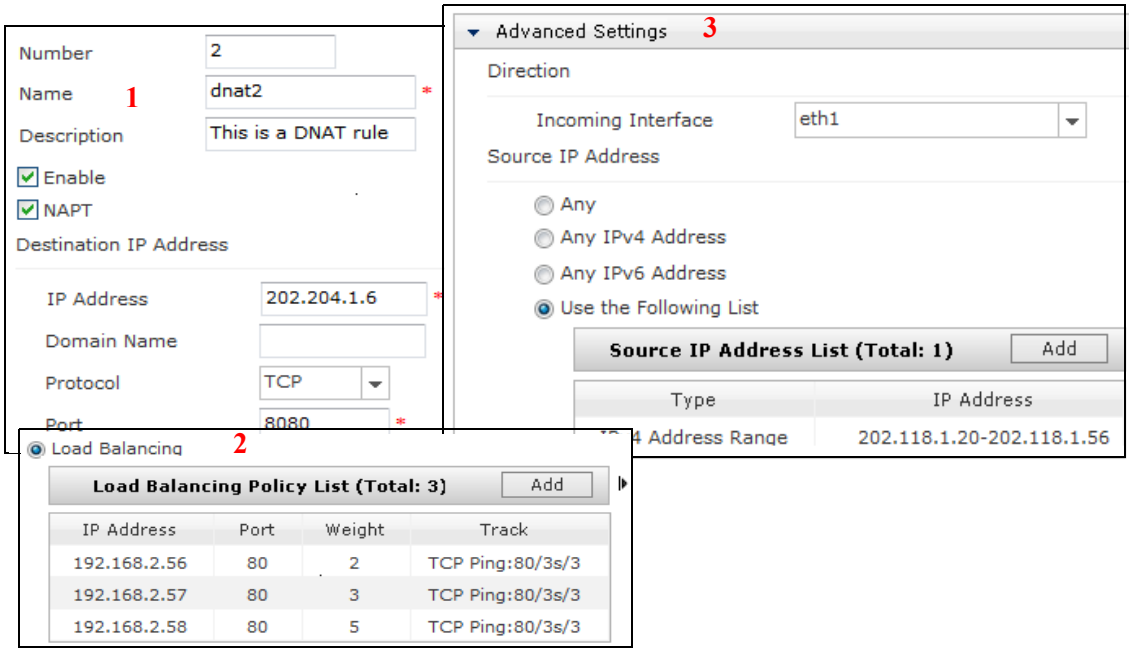
In this example, external hosts want to access internal Web service using 202.204.1.6, and there are 3 internal Web servers. You configure a one-to-many DNAT rule with NAPT enabled so traffic load from the Internet can be allocated properly to the 3 internal servers. FGX performs DNAT on the packets from the Internet only when the following requirements are satisfied:

1. The source IP addresses range of the external hosts is 202.118.1.20-202.118.1.56.
2. The incoming interface is eth1.

Figure 26 NAT-Based Load Balancing



1. Choose **Network** > **NAT** > **DNAT** and click **New** to create the following DNAT rule:



2. Click **OK**.
3. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] policy dnat dnat2 load-balancing 202.204.1.6 tcp
8080 192.168.2.56 80 2 ip-track tcpping port 80 3 3 enable
FGX@root-system] policy dnat dnat2 matching load-balancing
192.168.2.57 80 3 ip-track tcpping port 80 3 3
FGX@root-system] policy dnat dnat2 matching load-balancing
192.168.2.58 80 5 ip-track tcpping port 80 3 3
FGX@root-system] policy dnat dnat2 matching sip 202.118.1.20
202.118.1.56
FGX@root-system] policy dnat dnat2 matching input-interface eth1
FGX@root-system] exit
FGX@root> save config
```

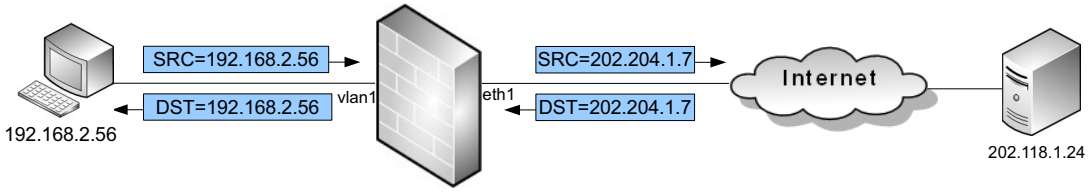
After the above operations are done, when the external host initiates a session to FGX, FGX allocates the session to Server3 which has the greatest weight. The servers' weight comes to 2:3:4. FGX continues to allocate new sessions to Server3. When servers' weight comes to 2:3:2, FGX allocates a new session to Server2. It allocates new sessions this way until servers' weight comes to 0:0:0. Then it allocates new sessions according to servers' weight 2:3:5 again.

Example 5: Create MIP Rule

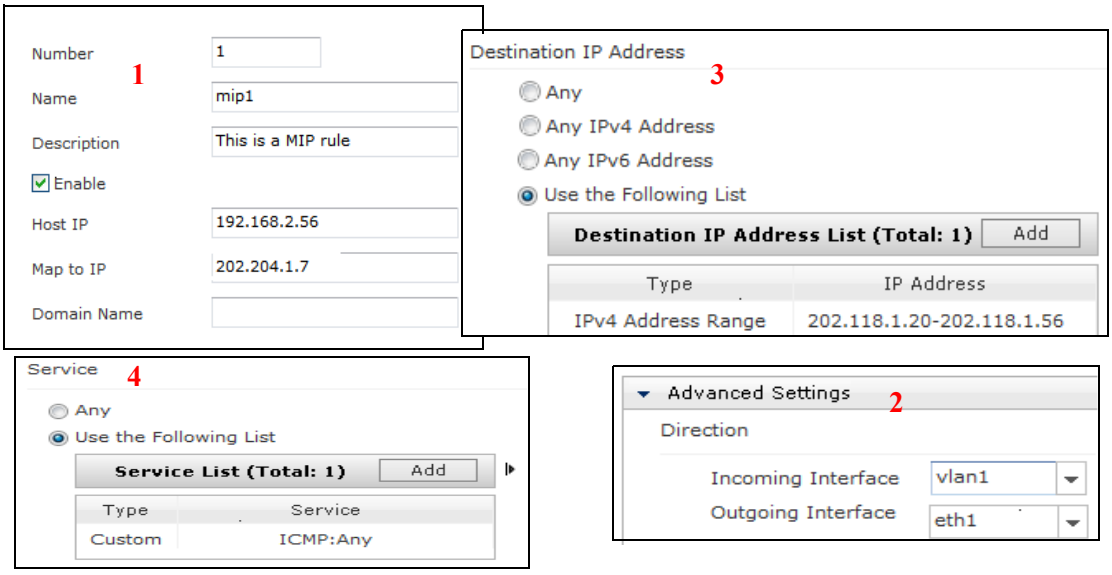
In this example:

1. When the internal client sends packets to the external server, FGX changes the packet source IP address from 192.168.2.56 to 202.204.1.7.
2. When external server replies to the internal client, FGX changes the packet destination IP address from 202.204.1.7 to 192.168.2.56.

Figure 27 Network Topology of MIP



1. Choose **Network** > **NAT** > **MIP** and click **New** to create a the following MIP rule:



2. Click **OK**.
3. Click  .

CLI

```
FGX@root> configure mode
FGX@root-system] policy mip mip1 192.168.2.56 202.204.1.7 enable
FGX@root-system] policy mip mip1 matching input-interface vlan1
FGX@root-system] policy mip mip1 matching output-interface eth1
FGX@root-system] policy mip mip1 matching dip 202.118.1.20
202.118.1.56
FGX@root-system] policy mip mip1 matching protocol icmp any
FGX@root-system] exit
FGX@root> save config
```

When the internal client sends packets to the external server, MIP result seen from the internal client:

Source	Destination	Protocol	Info
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply
192.168.2.56	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	192.168.2.56	ICMP	Echo (ping) reply

MIP result seen from the external server:

Source	Destination	Protocol	Info
202.204.1.7	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.7	ICMP	Echo (ping) reply
202.204.1.7	202.118.1.24	ICMP	Echo (ping) request
202.118.1.24	202.204.1.7	ICMP	Echo (ping) reply

When the external server replies to the internal client, MIP result seen from the internal client:

Source	Destination	Protocol	Info
202.118.1.24	192.168.2.56	ICMP	Echo (ping) request
192.168.2.56	202.118.1.24	ICMP	Echo (ping) reply
202.118.1.24	192.168.2.56	ICMP	Echo (ping) request
192.168.2.56	202.118.1.24	ICMP	Echo (ping) reply

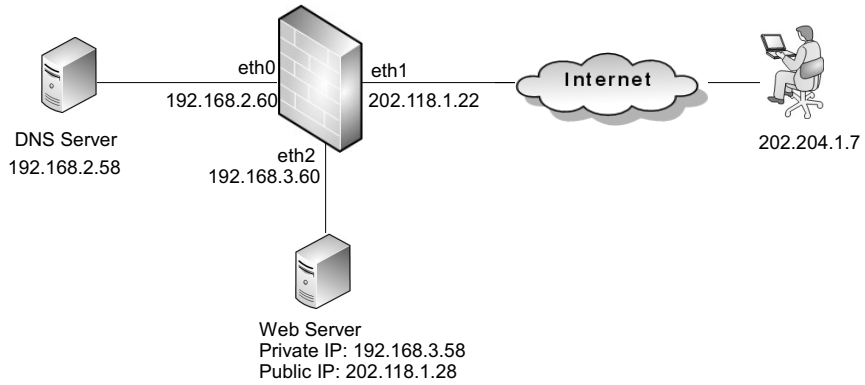
MIP result seen from the external server:

Source	Destination	Protocol	Info
202.118.1.24	202.204.1.7	ICMP	Echo (ping) request
202.204.1.7	202.118.1.24	ICMP	Echo (ping) reply
202.118.1.24	202.204.1.7	ICMP	Echo (ping) request
202.204.1.7	202.118.1.24	ICMP	Echo (ping) reply

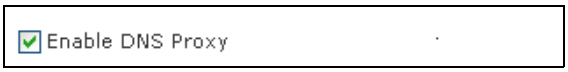
Example 6: DNS Rewrite

In this example, the external client sends a DNS request to the DNS server. The DNS server reply specifies that the domain name orresponds to 202.118.1.28. When FGX receives the reply, it translates this public IP address to 192.168.3.58 (internal Web server) as specified in the DNAT rule.

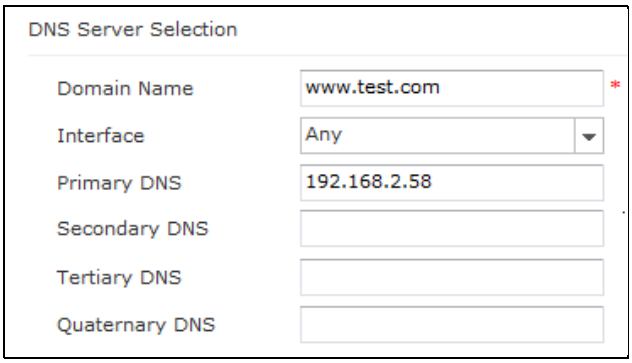
Figure 28 DNS Rewrite in DNAT



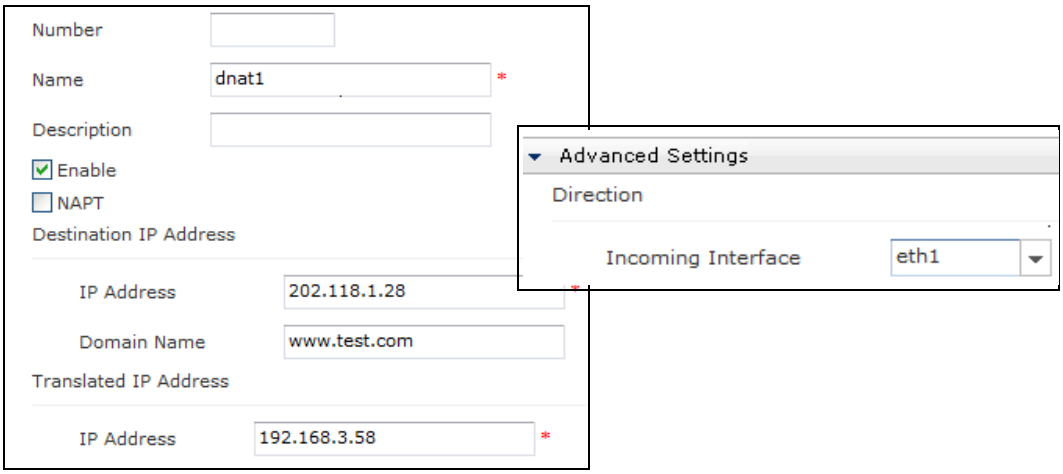
1. Choose **Firewall > Access Policies**. Click **New** to create an access policy (use default settings). Check **Enable DNS Proxy**.



2. Choose **Network** > **DNS** > **DNS Proxy**. Click **New** to set DNS proxy.



3. Choose **Network** > **NAT** > **DNAT**. Click **New** to create a DNAT policy.



4. Click **OK**.
5. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] policy access policy1 any any any any any any permit enable
FGX@root-system] policy access policy1 dns-proxy enable
FGX@root-system] dns server-select www.test.com output-interface any primary 192.168.3.58
FGX@root-system] policy dnat dnat1 202.118.1.28 domain www.test.com 192.168.3.58 enable
FGX@root-system] policy dnat dnat1 matching input-interface eth1
FGX@root-system] exit
FGX@root> save config
```

5.4.Parameter Reference

This section describes NAT rule parameters:

- 5.4.1. SNAT Rule Parameters
- 5.4.2. DNAT Rule Parameters
- 5.4.3. MIP Rule Parameters

5.4.1. SNAT Rule Parameters

Table 131 Parameters of SNAT Rules

Parameter	Description
Number	SNAT rule priority. Integer in 1-80,000. The lower the number, the higher the priority. If you do not specify a number for a new rule, the rule will get the lowest priority.
Name	SNAT rule name. 1-63 UTF-8 characters except ? , ” ' \ < > & # and spaces. SNAT rule names must be unique within a virtual system.
Description	SNAT rule description. 0-255 UTF-8 characters except ? ” ' \ < > &
Enable	Used to enable or disable a SNAT rule. A SNAT rule is enabled by default. Only after SNAT rules are enabled can they be matched.
NAPT	Used to enable or disable port translation for SNAT. NAPT is enabled by default.
Hold Time	The length of time a mapping relationship will remain after all the corresponding sessions are terminated. The range is 30-99,999,999 seconds.
Source IP Address	The real IP address from which packets are sent. A source IP address can be an IP address object, IP object group, IPv4/IPv6 address, IPv4/IPv6 address range, IPv4 address and mask length, or IPv6 address and prefix length. You can configure up to 32 source IP address entries.
Translated IP Address/ Interface	The IP address into which one or more source IP addresses are translated. A translated IP address can be either of the following types: • **Interface—**sets interface IP address(es) as translated IP address(es). • **IP Address—**includes IPv4/IPv6 address, IPv4/ IPv6 address range, IPv4 address and mask length, and IPv6 address and prefix length. IPv4 Address is set by default. You can configure up to 8 translated IP address entries.
Advanced Settings	Used to configure conditions for packets to match. Packets matching all conditions can be translated. • **Direction** **Incoming Interface—**the Layer 3 interface through which packets are received on FGX. Any by default. **Outgoing Interface—**the Layer 3 interface through which packets are sent out on FGX. Any by default. • **Destination IP Address—**the IP address to which packets are sent. A destination IP address can be an IP address object, IP object group, IPv4/IPv6 address, IPv4/IPv6 address range, IPv4 address and mask length, or IPv6 address and prefix length. IP Address Object is set by default. You can configure up to 32 destination IP address entries. • **Service—**Packet service type, and it can be an object, object group, or custom protocols. Custom protocols include ICMP, ICMPv6, TCP, UDP, and other protocols. The destination port number range of TCP or UDP is 1-65535. Other protocol number range is 1-255. You can configure up to 32 service entries.

5.4.2.DNAT Rule Parameters

Table 132 Parameters of DNAT Rules

Parameter	Description
Number	DNAT rule priority. Integer in 1-80,000. The lower the number, the higher the priority. If you do not specify a number for a new rule, the rule will get the lowest priority.
Name	DNAT rule name. 1-63 UTF-8 characters except ? , ” ' \ < > & # and spaces. DNAT rule names must be unique within a virtual system.
Description	DNAT rule description. 0-255 UTF-8 characters except ? ” ' \ < > &
Enable	Used to enable or disable a DNAT rule. A DNAT rule is enabled by default. Only after DNAT rules are enabled can they be matched.
NAPT	Used to enable or disable port translation. NAPT is enabled by default.
Destination IP Address	The original destination IP address of packets. You can configure the following: • **IP Address—**the original IPv4 or IPv6 address to which packets are sent. • **Domain Name—**domain name corresponding to a destination IP address. 2-255 characters. When DNS rewrite is required, you can enter a domain name. • **Protocol—**the protocol used by packets, including TCP and UDP. TCP is set by default. Required only if you enable NAPT. • **Port—**the original destination port before translation. Required only if you enable NAPT. The destination port number range is 1-65535.
Translated IP Address	Used to set one or more translated IP addresses for a DNAT rule. A translated IP address can be either of the following types with NAPT enabled: • **Normal—**used to configure one translated IP address and one translated port. Normal is set by default. • **Load Balancing—**used to configure load balancing policies with multiple translated IP addresses. You are required to set only one translated IP address if NAPT is disabled.
Normal	You are required to configure the following: • **IP Address—**the IPv4 or IPv6 address to which an original destination IPv4 or IPv6 address is translated. • **Port—**the destination port after translation.

Table 132 Parameters of DNAT Rules (*continued*)

Parameter	Description
Load Balancing	You can configure the following parameters for a load balancing policy: • **IP Address** • **Destination Port** • **Weight—**the session proportion that a server can get. The weight range is 1-255. It is 1 by default. • **Track Type—**the method used for link track. FGX supports ARP Ping, Ping, and TCP Ping. You can also set the track type as None. None is the default track type. ARP ping is used to track only IPv4 addresses in internal networks of FGX, and NS ping is used to track IPv6 addresses. • **Track Port—**the port of a server to be tracked when TCP Ping is used. The port range is 1-65535. • **Track Interval—**the interval (in seconds) between two link tracks. The interval range is 1-30,000 seconds. It is 3 seconds by default. • **Track Failure Threshold—**the maximum number of consecutive failures allowed when FGX tracks an IP address. If the number of track failures reaches the threshold and no replies are received, the link is considered to have failed. The threshold range is 1-999. It is 3 by default. You can configure up to 8 load balancing policies.
Advanced Settings	Used to configure conditions for packets to match. Packets matching all conditions can be translated. • **Direction** **Incoming Interface—**the Layer 3 interface through which packets are received on FGX. Any by default. • **Source IP Address—**the IP address from which packets are sent. A source IP address can be an IP address object, IP object group, IPv4/IPv6 address, IPv4/IPv6 address range, IPv4 address and mask length, or IPv6 address and prefix length. IP Address Object is set by default. You can configure up to 32 source IP address entries.

5.4.3.MIP Rule Parameters

Table 133 Parameters of MIP Rules

Parameter	Description
Number	MIP rule priority. Integer in 1-80,000. The lower the number, the higher the priority. If you do not specify a number for a new rule, the rule will get the lowest priority.
Name	MIP rule name. 1-63 UTF-8 characters except ? , ” ' \ < > & # and spaces. MIP rule names must be unique within a virtual system.
Description	MIP rule description. 0-255 UTF-8 characters except ? “ ' \ < > &
Enable	Used to enable or disable a MIP rule. A MIP rule is enabled by default. Only after MIP rules are enabled can they be matched.
Host IP	The private IPv4 or IPv6 address of an internal host. When a packet is initiated from an internal network to an external network, the host IP address is the source IP address before mapping. When the packet is initiated from the external network to the internal network, the host IP address is the translated destination IP address.
Map to IP	The public IPv4 or IPv6 address to which an internal IPv4 or IPv6 address is mapped. When a packet is initiated from an internal network to an external network, the map to IP address is the translated source IP address of a packet. When a packet is initiated from the external network to the internal network, the map to IP address is the original destination IP address of a packet.
Domain Name	The domain name corresponding to a map to IP address. Length range 2-255 characters. When DNS rewrite is required, you can enter a domain name.
Advanced Settings	Used to configure conditions for packets to match. Packets matching all conditions can be translated. • **Direction** **Incoming Interface—**the Layer 3 interface that is connected to an internal network. When a packet is initiated from an internal network to an external network, the incoming interface is the interface receiving the packet. When a packet is initiated from the external network to the internal network, the incoming interface is the interface sending out the packet. **Outgoing Interface—**the Layer 3 interface that is connected to an external network. When a packet is initiated from an internal network to an external network, the outgoing interface is the interface sending out the packet. When a packet is initiated from the external network to the internal network, the outgoing interface is the interface receiving the packet. • **Destination IP Address—**when a session is initiated from an internal network to an external network, the destination IP address is the IP address to which packets are sent. When a session is initiated from the external network to the internal network, the destination IP address is the IP address from which packets are sent. A destination IP address can be an IP address object, IP object group, IPv4/IPv6 address, IPv4/IPv6 address range, IPv4 address and mask length, or IPv6 address and prefix length. IP Address Object is set by default. You can configure up to 32 destination IP address entries. • **Service—**Packet service type, and it can be an object, object group, or custom. Custom protocols include ICMP, ICMPv6, TCP, UDP, and other protocols. The destination port number range of TCP or UDP is 1-65535. Other protocol number range is 1-255. You can configure up to 32 service entries.

6 Routing

This chapter explains the routing and multicasting features of FGX:

- **6.1. Overview**. Presents a basic conceptual overview.
- **6.2. Basic Configuration Steps**. A step-by-step guide for using the UI and CLI for most common configuration tasks.
- **6.3. Basic examples**. Basic examples of routing and switching configuration (unicast, multicast stastic and dynamic).
- **6.4. Advanced Examples**.
- **6.5. Parameter Reference**.

6.1.Overview

When FGX receives a packet, if the packet belongs to

1. Existing session: FGX forwards the packet as specified in the routing table.
2. No session: FGX determines the routing.

This section describes FGX routing/switching concepts for

- **6.1.1 L3 Unicast**
- **6.1.2 L3 Multicast**
- **6.1.3 L2 Multicast**

6.1.1 L3 Unicast

6.1.1.1 (Default policy) routes

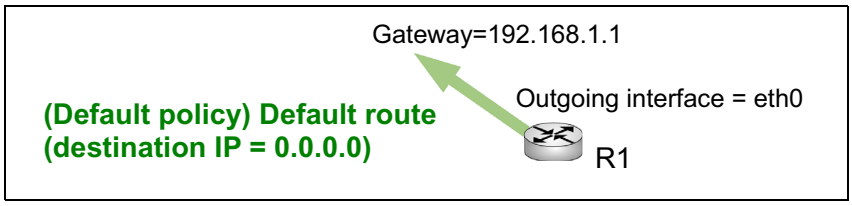
Based on the destination IP, the default routing table determines the

1. Outgoing interface (set the outgoing interface of a route as "Null' to drop packets to avoid route loops)
2. Gateway

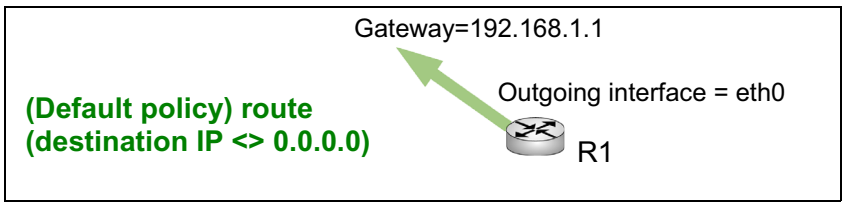
A default route is used if no policy-based route matches the packet (a policy-based route is similar to a default route, but also specifies incoming interface(s), source IP(s), service(s) and TOS).

There are 2 basic types of default routes:

1. Route with destination IP 0.0.0.0/0. Selected if no other default route matches.

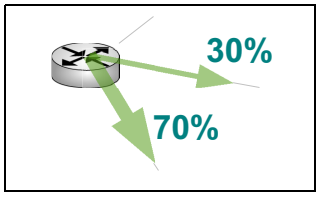


2. Routes with the actual destination IP address or range.



6.1.1.2 Load balancing / link probe

Load Balancing: A new session is assigned to the link (outgoing interface/gateway) with the lowest weight-adjusted load. If the link fails, a new link is selected.



Link probe: Send out probe packets at each track interval to next-hop device.

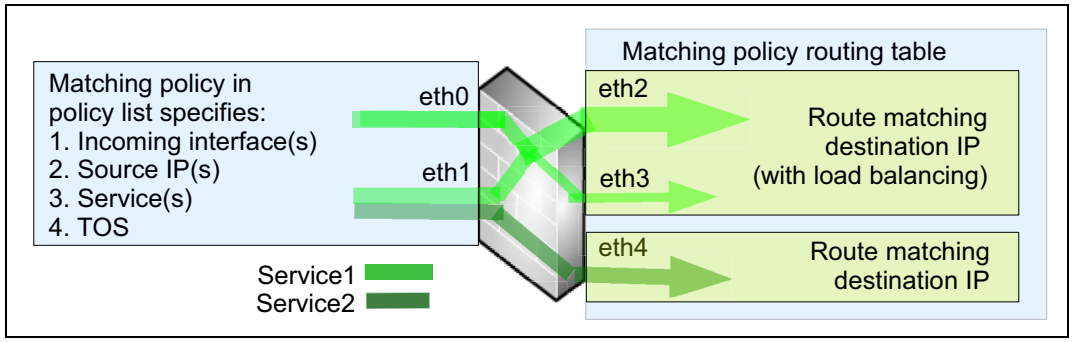
The following situations are link failures:

- Track failure threshold (the maximum number of consecutive response failures allowed) is reached and no response was received within a track interval.
- Outgoing interfaces are disabled or have failed.

FGX provides the following types of link probes:

Probe Type	Address Type	Packet Sent	Packet Reply
ARP Ping (ARP probe)	IPv4	ARP request packet	ARP reply packet containing the MAC address
TCP Ping (TCP probe)	IPv4 & IPv6	SYN packet	SYN/ACK packet
Ping (ICMP probe)	IPv4 & IPv6	ICMP echo request packet through the ping or ping6 command	Echo reply
NS Ping (NS probe)	IPv6	Neighbor solicitation (NS) message	Neighbor advertisement (NA) message

6.1.1.3 Policy-based routing



The **policy list table** contains policies that specify:

1. Incoming interface(s)
2. Source IP(s)
3. Service(s)
4. TOS (type of service)

Each policy has it's own **routing table**. These routes are similar to default policy routes, and based on the destination IP determine

1. Outgoing interface
2. Gateway
3. Load balancing

The **selected policy** is the

1. Highest priority policy that matches packet source parameters.
2. And that has a matching (destination IP) outgoing route in the routing table.

Selected route: If multiple routes in the same routing table have the same destination IP, then the following parameters (in order of priority) are used to select the route

a. Longest mask length or prefix length.

b. Lowest metric.

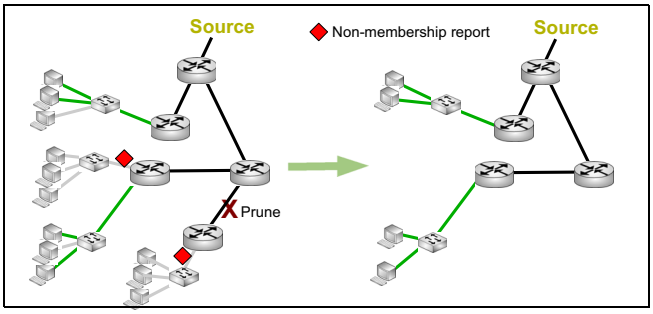
c. First route added.

6.1.2 L3 Multicast

- 6.1.2.1 L3 Multicast dynamic.
- 6.1.2.2 L3 Multicast static.

6.1.2.1 L3 Multicast dynamic

- **Determine route** (DVMRP, metric). Dynamically generate a routing table with distances for the multicast group interfaces based on DVMRP. Metric is used to select a route. A lower metric indicates a better route.
- **Cache lifetime**. The length of time that a multicast route learned dynamically stay in the cache.
- **Threshold**. Threshold is a TTL limit for forwarding multicast packets. A multicast packet cannot be forwarded unless its TTL value at the receiving DVMRP interface is greater than the interface threshold value.
- **Prune lifetime**. Through a "broadcast & prune" technique, DVMRP builds and maintains a multicast delivery tree for each source and group. If leaf routers discover that there are no group members on their directly-attached leaf subnetworks, they transmit prune messages back toward the source and temporarily remove unnecessary leaves from the tree. DVMRP can also graft a new branch to the delivery tree if a router discovers that new members want to jon the multicast group. The following diagram shows how branches are pruned.

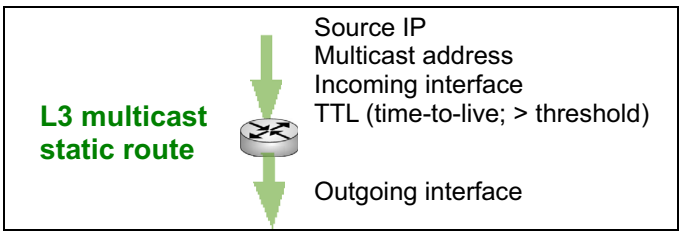


6.1.2.2 L3 Multicast static

L3 multicast routing table static routes determine the forwarding interface(s) based on

1. Source IP address
2. Multicast group IP address.
3. Incoming interface.

DVMRP must be enabled for the forwarding interface (DVMRP functionality is still required for a static route).



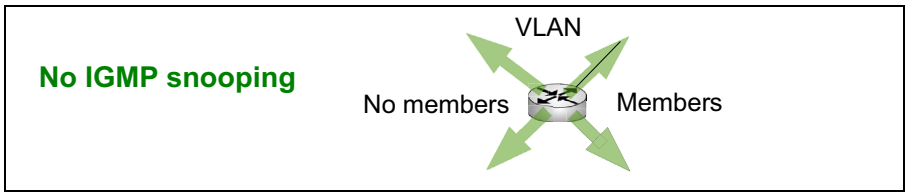
6.1.3 L2 Multicast

This section describes

- **6.1.3.1 L2 Multicast dynamic (IGMP snooping)**
- **6.1.3.2 L2 Multicast static**.

6.1.3.1 L2 Multicast dynamic (IGMP snooping)

Hosts use IGMP to dynamically join multicast groups. FGX supports IGMPv1 and IGMPv2.

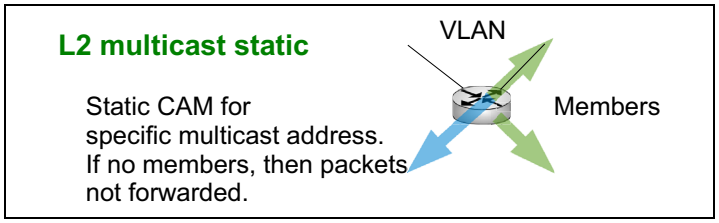


6.1.3.2 L2 Multicast static

L2 multicast tables determine the forwarding interface(s) based on

1. Multicast destination IP address (MAC address)

IGMP snooping must be enabled (even if route is static).



6.2.Basic Configuration Steps

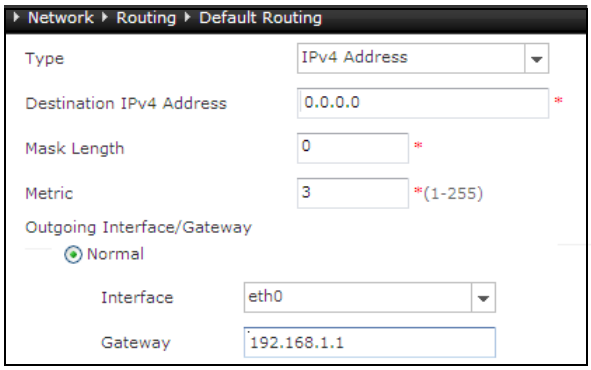
6.2.1 L3 Unicast
6.2.2 L3 Multicast
6.2.3 L2 Multicast

6.2.1 L3 Unicast

- 6.2.1.1 Static L3 default policy / default route
- 6.2.1.2 Load balancing
- 6.2.1.3 Static L3 policy / routes

6.2.1.1 Static L3 default policy / default route

1. Specify the default route: For IP address enter 0.0.0.0. Specify the mask length, metric, and outgoing interface/gateway.



2. Specify the non-default routes for specific destination IPs (these routes have no priority; therefore, you should not create more than one route for a destination IP).

The default policy routes are shown in the (default policy) routing table.

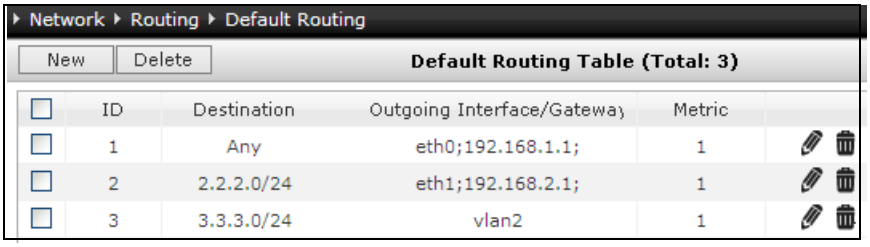


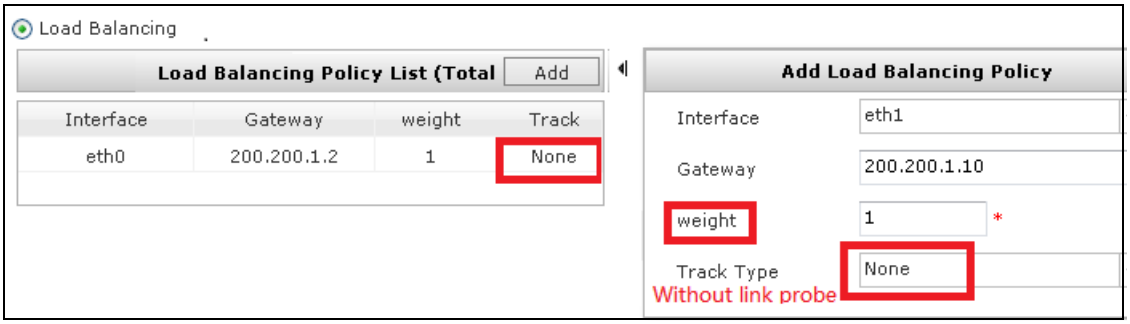
Table 134 Default Route CLI Commands

route	Adds a default route.
show route	Displays default route information.
unset route	Deletes default routes.

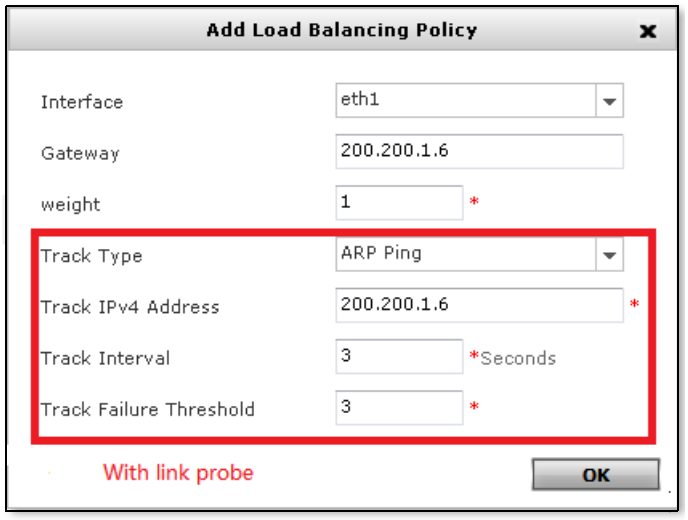
6.2.1.2 Load balancing

Specify load balancing (this shows configuration for default route; specifying load balancing for non-default and policy routes is similar).

- Without tracking.



- With tracking.



Default routing table:

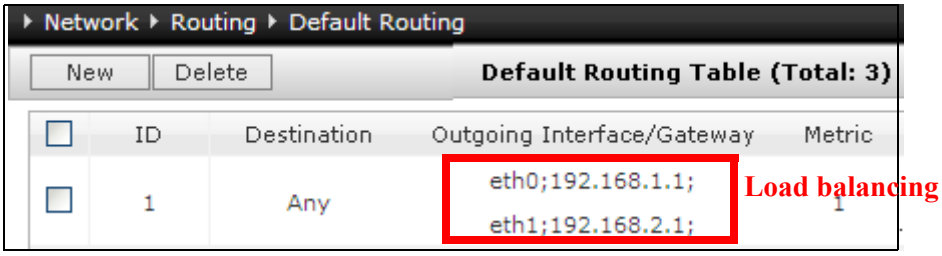


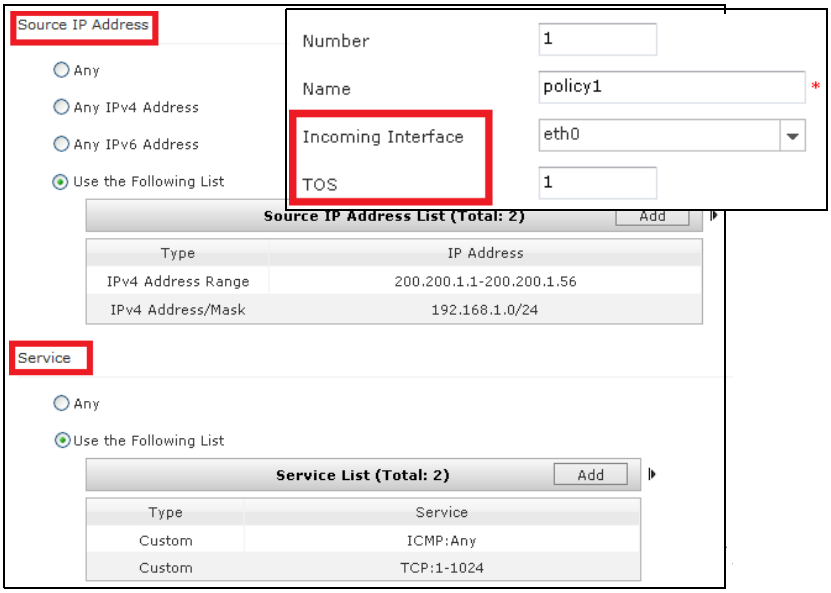
Table 135 Route Load Balancing CLI Commands

route {**default** | *ipv4 netmask*} **load-balancing**	Adds an IPv4 route with load-balancing.
route {**default-v6** | *ipv6 prefix_length*} **load-balancing**	Adds an IPv6 route with load-balancing.

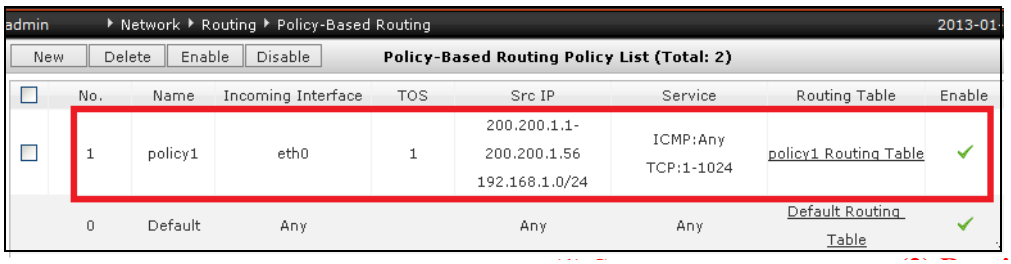
6.2.1.3 Static L3 policy / routes

Step 1: Policy for Matching Incoming Packets

1. Choose Network > Routing > Policy-Based Routing > New.
2. Set incoming interface, TOS, source IP addresses, and services.



3. Click OK. Click  . View the routing policy:

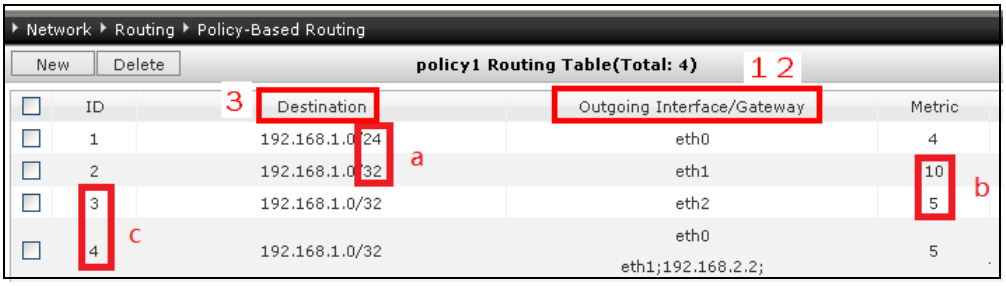


By default, a routing policy is enabled after being created. If you delete a routing policy, its routing table will be deleted.

Step 2: Outgoing Interfaces/Gateways (Route).

4. Click “policy1 Routing Table” to set forwarding routes for packets matching policy1. Configuration is same as in “6.2.1.1 Static L3 default policy / default route” on page 285.

Each policy has it’s own routing table. Policy routing table routes are similar to default policy routes.



A route determines

1. Outgoing interface
2. Gateway
3. Load balancing

If multiple routes in the same routing table have the same destination IP, then the following parameters (in order of priority) are used to select the route

a. Longest mask length or prefix length.

b. Lowest metric.

c. First route added.

.

Table 136 Policy Route CLI Commands

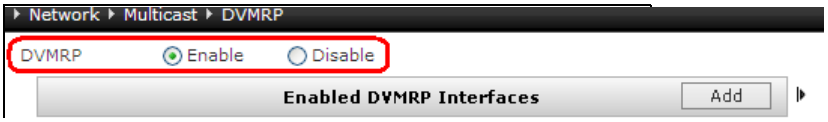
policy route *policy_name* [**number** *pri*]	Adds a policy-based routing policy.
matching	Adds criteria for matching packets to a policy.
policy route *policy_name* {**enable** | **disable**}	Enables or disables a policy.
show policy route [*policy_name*]	Displays policy-based routing policy information.

6.2.2 L3 Multicast

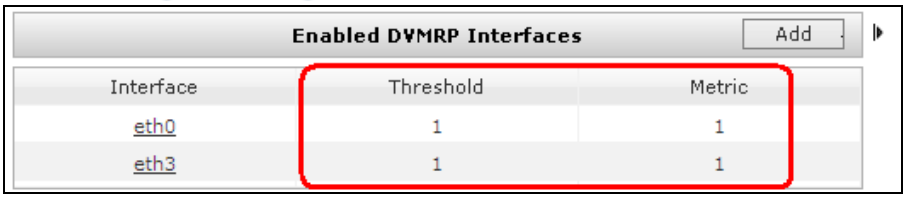
- 6.2.2.1 L3 Multicast Dynamic
- 6.2.2.2 L3 Multicast Static

6.2.2.1 L3 Multicast Dynamic

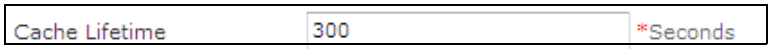
1. Choose Network > Multicast > DVMRP.
2. Enable DVMRP.



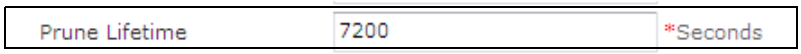
3. Choose DVMRP interfaces for forwarding multicast packets. Click Add. Choose DVMRP interfaces for forwarding multicast packets. Set threshold and metric for DVMRP interfaces.



4. Optionally set **cache lifetime** (length of time that a dynamically learned multicast route remains in the cache).



5. Optionally set **prune lifetime** (length of time in which FGX should hold a prune state)..



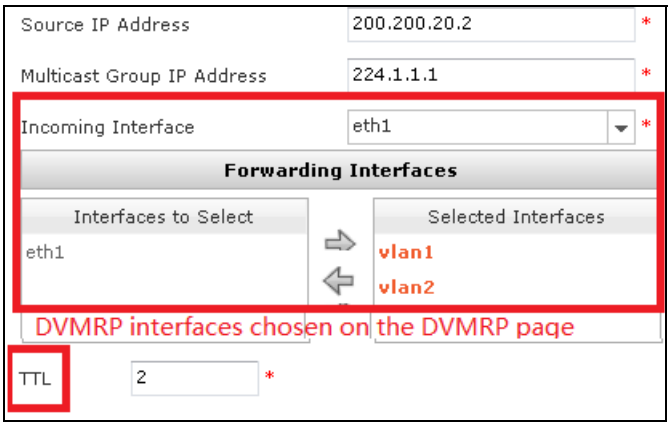
6. Click OK. Click  .

Table 137 DVMRP CLI Commands

dvmrp {**enable** | **disable**}	Enables or disables DVMRP.
dvmrp cache-lifetime *time*	Sets the length of time a DVMRP route stays in multicast cache.
dvmrp prune-lifetime *time*	Sets the length of time FGX should hold a prune state.
dvmrp metric {*metric_value* | **default**}	Sets Layer 3 interface DVMRP metric values.
dvmrp {**on** | **off**}	Enables or disables DVMRP on Layer 3 interface.
dvmrp pim {**enable** | **disable**}	Enables or disables PIM neighbor discovery.
dvmrp threshold {*threshold_value* | **default**}	Sets TTL threshold values for Layer 3 interfaces.
show dvmrp {**interface** | **neighbor** | **timer**}	Displays DVMRP monitoring information.
show dvmrp state	Displays DVMRP configuration information.

6.2.2.2 L3 Multicast Static

1. Choose Network > Routing > Multicast Routing > New to create the route:



Multicast packets with a TTL value > the TTL value you set will be forwarded out.

2. Click OK.Click .

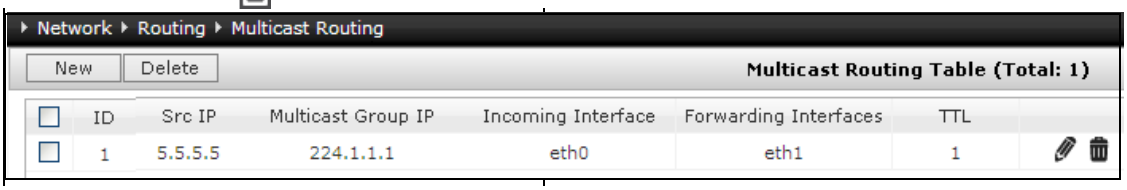


Table 138 Static Multicast Route CLI Commands

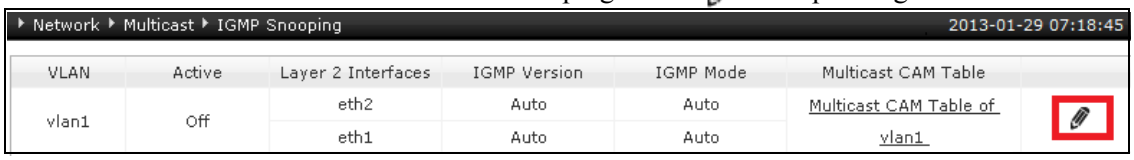
dvmrp route	Adds a static multicast route.
show dvmrp route	Displays multicast route information.
unset dvmrp route	Deletes static multicast routes.

6.2.3 L2 Multicast

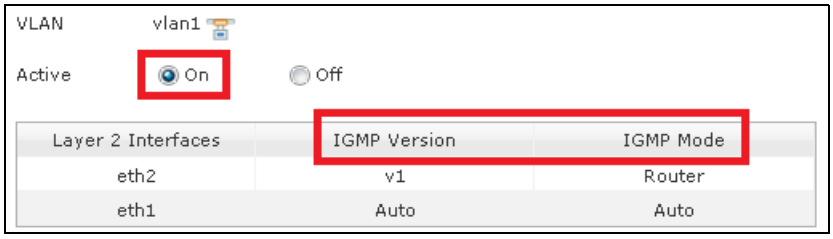
- 6.2.3.1 L2 multicast dynamic
- 6.2.3.2 L2 multicast static

6.2.3.1 L2 multicast dynamic

1. Choose Network > Multicast > IGMP Snooping. Click corresponding to vlan1.



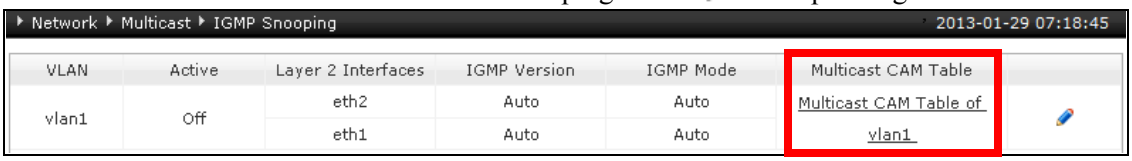
2. Click On in the Active field to enable IGMP snooping.
3. Click any interface item to set IGMP version and mode for the interface.



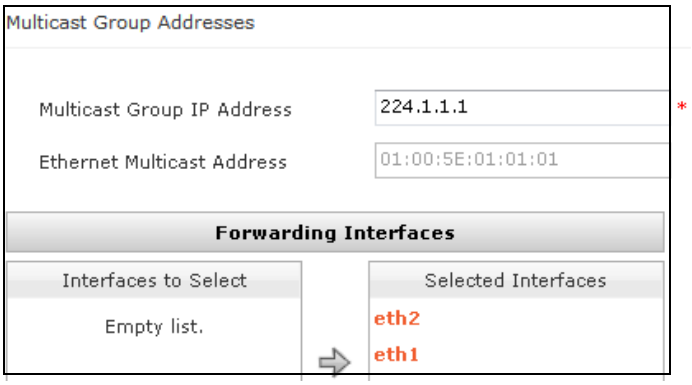
4. Click OK. Click .
5. To view IGMP snooping state, click the IGMP Snooping State hyperlink or choose Monitor > Multicast > IGMP Snooping State. For more information, see"14.15.2 IGMP Snooping State" on page 743.

6.2.3.2 L2 multicast static

1. Choose Network > Multicast > IGMP Snooping. Click corresponding to vlan1.



2. Enable IGMP snooping.
3. Click the "Multicast CAM table of vlan1" hyperlink. Click New to create a static multicast CAM entry.



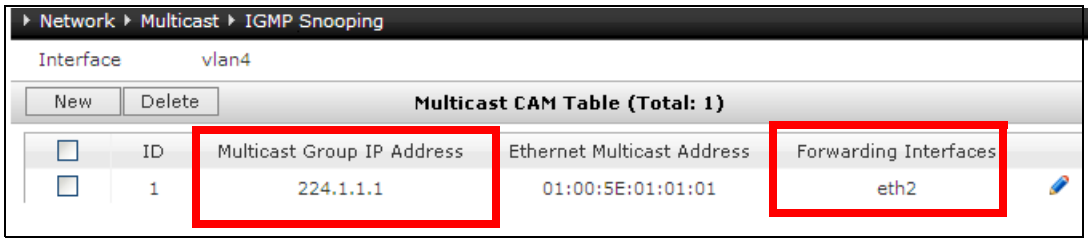


Table 139 IGMP Snooping CLI Commands

igmp-snooping {**on** | **off**}	Enables or disables IGMP snooping.
igmp-snooping interface-flags	Sets the type of the network that is connected with a Layer 2 interface in a VLAN.
igmp-snooping version	Sets the IGMP version.
multicast cam-table	Adds a static multicast CAM entry.
show igmp-snooping state [**vlan** *vlan_id*]	Displays the IGMP snooping state.
unset multicast cam-table	Delete static multicast CAM entries.

6.3.Basic examples

This section gives the following examples about how to configure routing and multicasting.

6.3.1 Unicast
6.3.2 L3 Multicast
6.3.3 L2 multicast

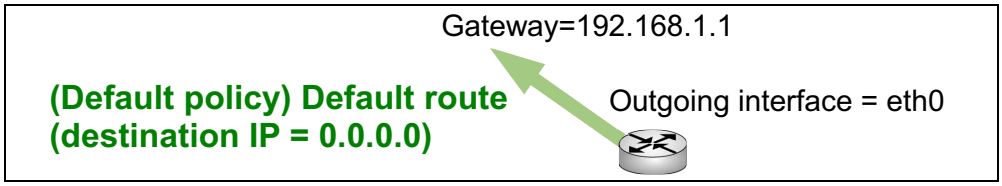
6.3.1 Unicast

This section describes simple examples for unicast.

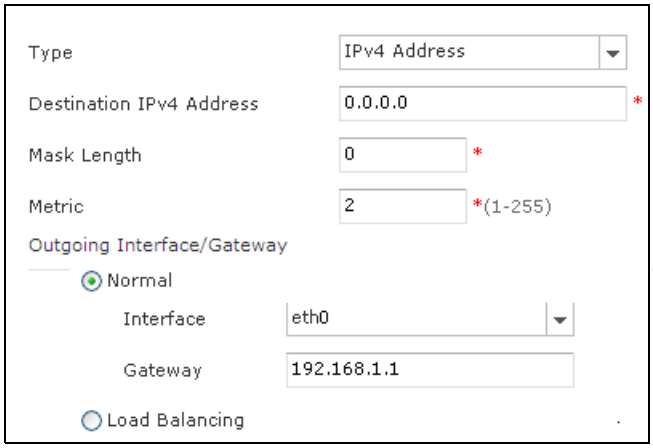
- 6.3.1.1 (Default policy) routes
- 6.3.1.2 Route load balancing
- 6.3.1.3 Policy-based route

6.3.1.1 (Default policy) routes

This example shows how to create following default route.



1. Click New to create a normal default route.

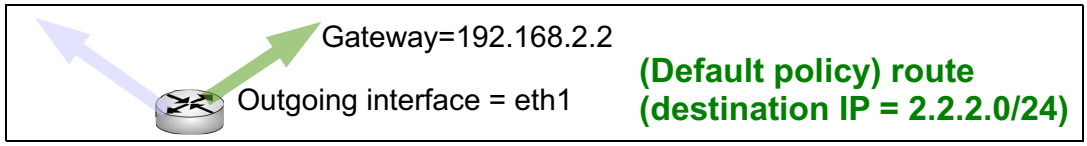


2. Click OK. Click .

CLI

```
FGX@root> configure mode override
FGX@root-system] route 0.0.0.0 0.0.0.0 interface eth0 gateway
192.168.1.1 2
FGX@root-system] exit
FGX@root> save config
```

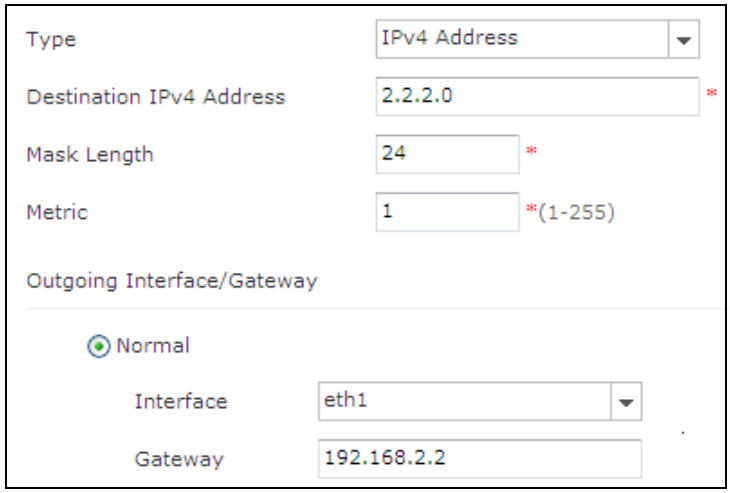
This example shows how to create the following route.



Specify the outgoing interface and/or gateway for packets that match

- No policy (policy example shown later) and
- Specified destination IP
- No other higher priority route in the default routing table

Do the following:

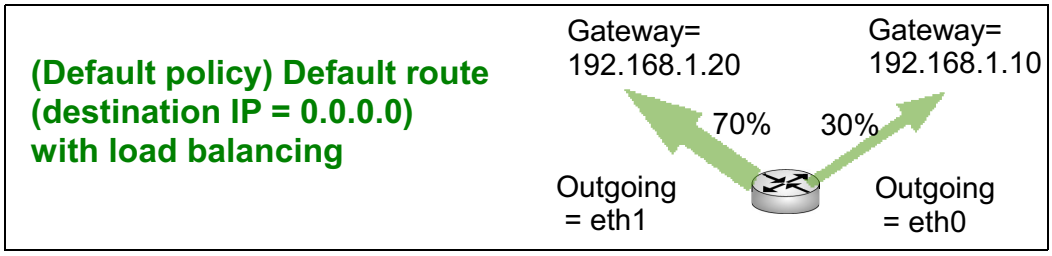


CLI

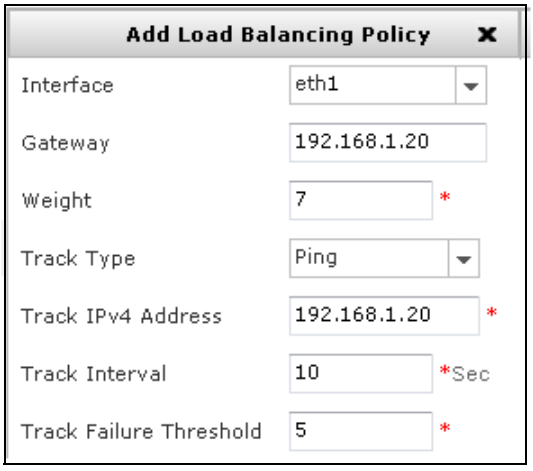
```
FGX@root> configure mode override
FGX@root-system] route 2.2.2.0 255.255.255.0 interface eth1 gateway
192.168.2.2 1
FGX@root-system] exit
```

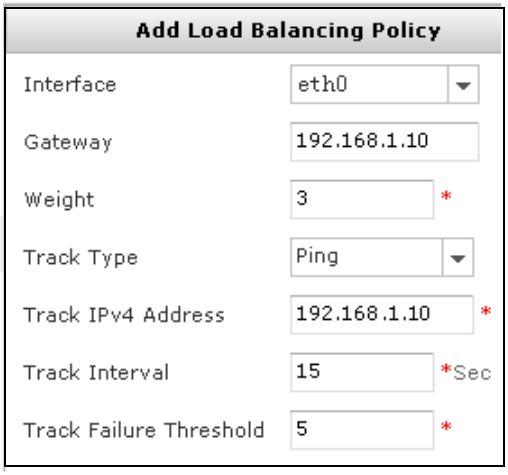
6.3.1.2 Route load balancing

This example shows how to load balance for the default policy default route.



1. In Load Balancing Policy List, click Add to add the following two load balancing policies:





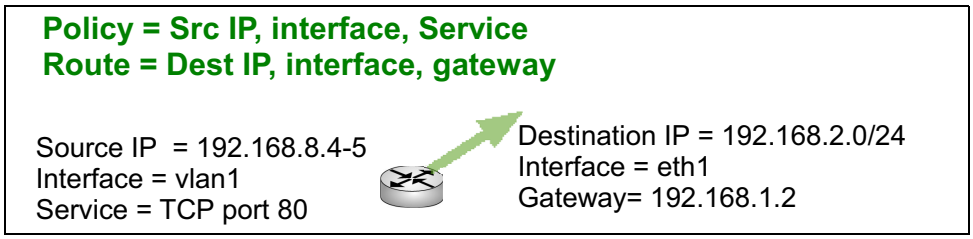
2. Click OK. Click .

CLI

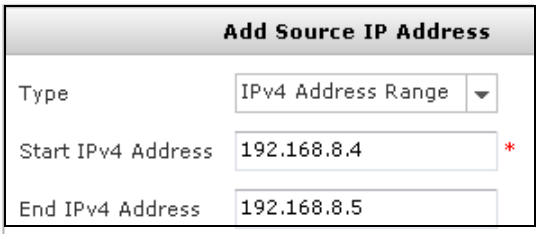
```
FGX@root> configure mode override
FGX@root-system] route 0.0.0.0 0.0.0.0 load-balancing interface eth0
gateway 192.168.1.10 3 ip-track ping 192.168.1.10 15 5 1
FGX@root-system] route 0.0.0.0 0.0.0.0 load-balancing interface eth1
gateway 192.168.1.20 7 ip-track ping 192.168.1.20 10 5 1
FGX@root-system] exit
FGX@root> save config
```

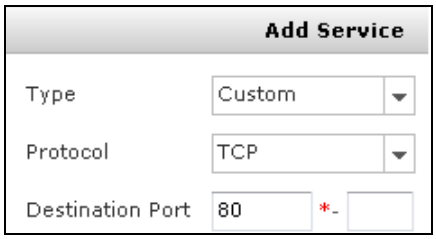
6.3.1.3 Policy-based route

This example shows how to create a policy-based route.

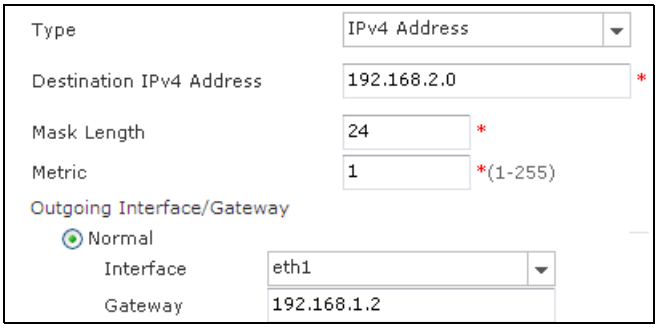


1. Choose Network > Routing > Policy-Based Routing > New.
2. Create the following policy-based routing policy:





3. Click OK.
4. Click "policy2 Routing Table" and click New to create a normal static route.



5. Click OK. Click .

CLI

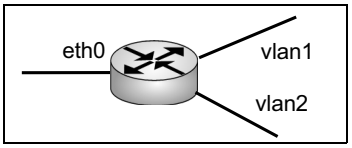
```
FGX@root> configure mode override
FGX@root-system] policy route policy2 enable
FGX@root-system-routepolicy-policy2] matching input-interface vlan1
FGX@root-system-routepolicy-policy2] matching sip 192.168.8.4
192.168.8.5
FGX@root-system-routepolicy-policy2] matching protocol tcp 80
FGX@root-system-routepolicy-policy2] route 192.168.2.0 255.255.255.0
interface eth1 gateway 192.168.1.2 1
FGX@root-system-routepolicy-policy2] end
FGX@root> save config
```

6.3.2 L3 Multicast

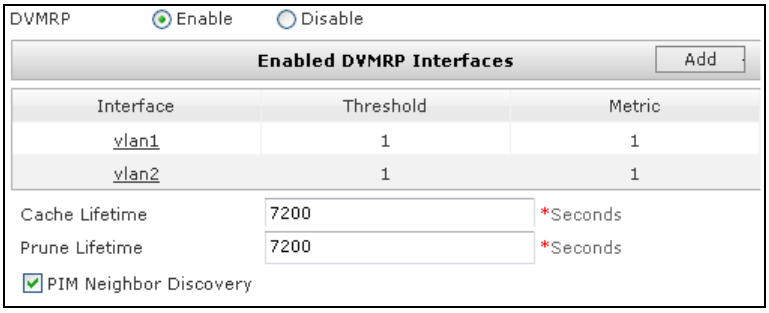
- 6.3.2.1 L3 Multicast Dynamic
- 6.3.2.2 L3 Multicast Static

6.3.2.1 L3 Multicast Dynamic

This example shows how to configure dynamic multicast for the following:



1. Choose Network > Multicast > DVMRP.
2. Click Enable to enable the DVMRP function.
3. Click Add and configure DVMRP interfaces as follows:
   a. Choose the interface vlan1 for forwarding multicast packets.
   b. Set the threshold of vlan1 as 1.
   c. Set the metric of vlan1 as 1 for route exchange. Click OK..



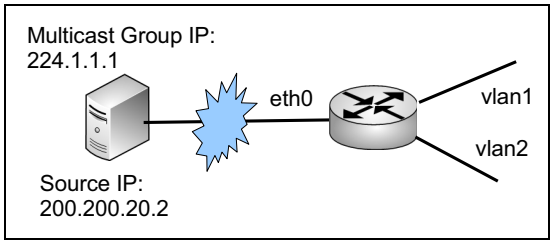
4. Set vlan2 the same way
5. Set the cache lifetime as 7,200 seconds. If not used for 2 hours, the route will be removed from the cache.
6. Set the prune lifetime as 7,200 seconds. If multicast packets are pruned, then pruning stops (packet forwarding resumed) after this period.
7. Click OK.Click .
8. To monitor, choose Monitor > Multicast > DVMRP Neighbors.

CLI

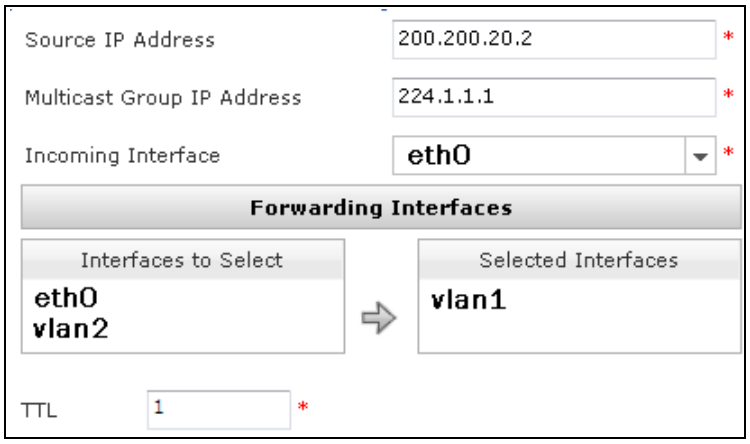
```
FGX@root> configure mode
FGX@root-system] dvmrp enable
FGX@root-system] vlan 1
FGX@root-system-vlan1] dvmrp on
FGX@root-system-vlan1] vlan 2
FGX@root-system-vlan2] dvmrp on
FGX@root-system-vlan2] exit
FGX@root-system] dvmrp cache-lifetime 7200
FGX@root-system] dvmrp pim enable
FGX@root-system] exit
FGX@root> save config
```

6.3.2.2 L3 Multicast Static

Create a static multicast route to vlan1.



1. Click the Multicast Routing hyperlink or choose Network > Routing > Multicast Routing.
2. Click New to create the following static multicast route:



IF the TTL value of the multicast packet is 2, the packet will be forwarded.

3. Click OK. Click .

CLI

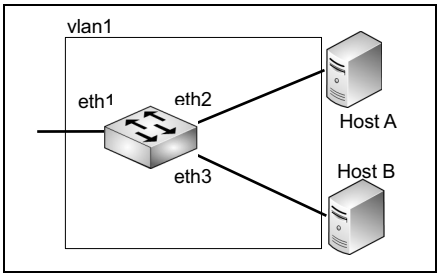
```
FGX@root> configure mode
FGX@root-system] dvmrp route 200.200.20.2 224.1.1.1 input eth0
forwarding vlan1 threshold 2
FGX@root-system] exit
FGX@root> save config
```

6.3.3 L2 multicast

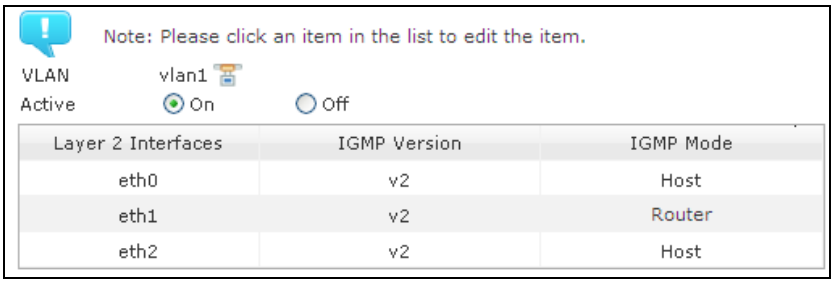
- 6.3.3.1 L2 Multicast Dynamic
- 6.3.3.2 L2 Multicast Static

6.3.3.1 L2 Multicast Dynamic

This example shows how to configure dynamic multicast for the following:



1. Choose Network > Multicast > IGMP Snooping and click corresponding to vlan1.
2. Click On in the Active field to enable IGMP snooping and set as follows:



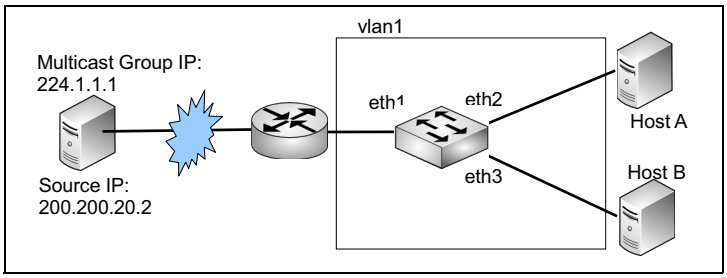
3. Click OK. Click .
4. Choose Monitor > CAM.

CLI

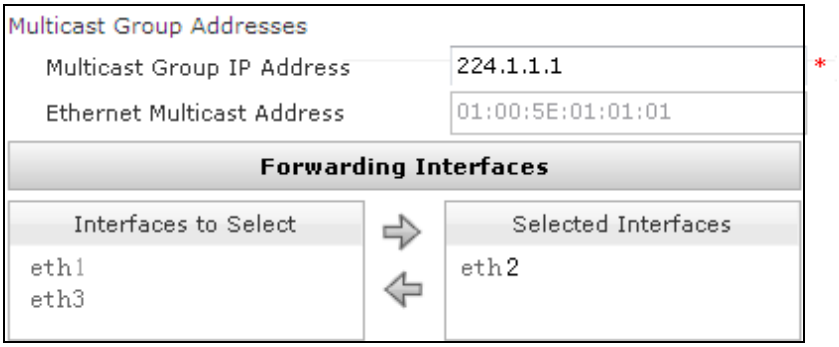
```
FGX@root> configure mode override
FGX@root-system] vlan 1
FGX@root-system-vlan1] igmp-snooping on
FGX@root-system-vlan1] igmp-snooping version ethernet 0 v2
FGX@root-system-vlan1] igmp-snooping version ethernet 1 v2
FGX@root-system-vlan1] igmp-snooping version ethernet 2 v2
FGX@root-system-vlan1] igmp-snooping interface-flags ethernet 0 host
FGX@root-system-vlan1] igmp-snooping interface-flags ethernet 1
multicast-router
FGX@root-system-vlan1] igmp-snooping interface-flags ethernet 2 host
FGX@root-system-vlan1] end
FGX@root> save config
```

6.3.3.2 L2 Multicast Static

This example shows how to configure static multicast for packets with multicast group IP of 224.1.1.1 to host A:



1. Choose Network > Multicast > IGMP Snooping.
2. Click the Multicast CAM table of vlan1 hyperlink.
3. Click New to create the following static multicast CAM entry:



4. Click OK.Click .
5. Choose Monitor > CAM.

CLI

```
FGX@root> configure mode override
FGX@root-system] vlan 1
FGX@root-system-vlan1] multicast cam-table 224.1.1.1 eth1
FGX@root-system-vlan1] end
FGX@root> save config
```

6.4.Advanced Examples

The examples in this section show how to configure routing and multicasting:

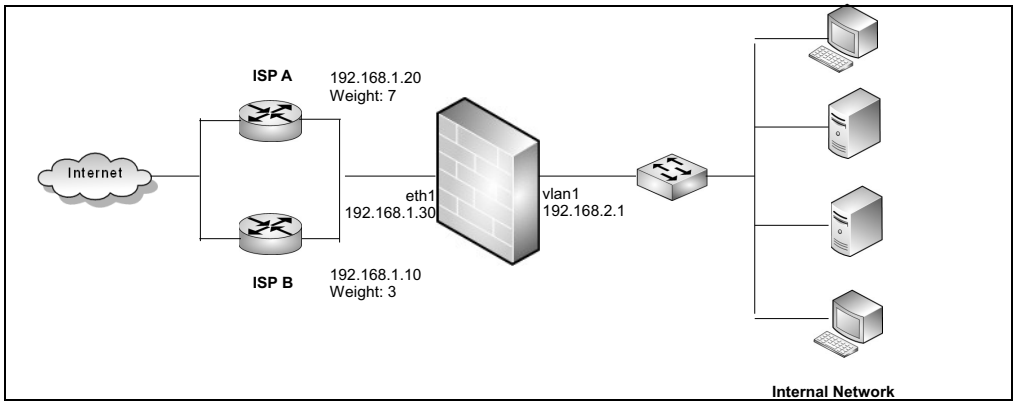
- Example 1: L3 Unicast: (default policy) Route / Load Balancing
- Example 2: L3 Unicast: Policy-based routes
- Example 3: L3 multicast dynamic (DVMRP)
- Example 4: L3 multicast static
- Example 5: L2 multicast dynamic (IGMP Snooping)
- Example 6: L2 multicast static

For each scenario, you must do the following in advance:

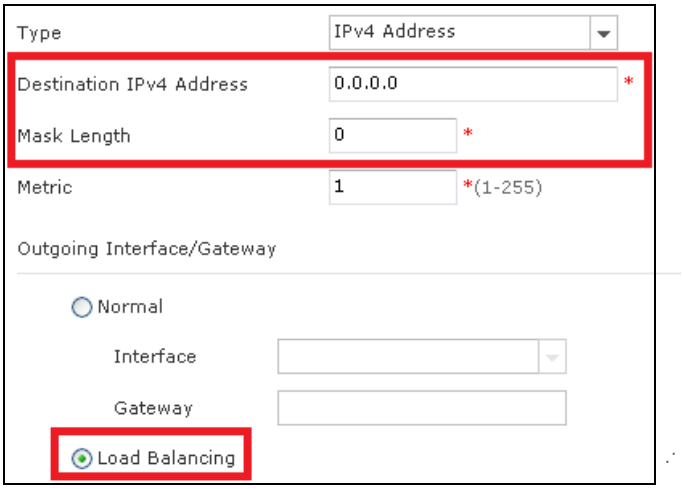
1. Choose **Network > Interfaces** to configure FGX interfaces. See Chapter 4, "Network Configuration."
2. If zones are needed, choose **Network > Zones** to create them. See 4.12 Zones.
3. Choose **Firewall > Default Policy Settings** to configure the default inter-zone action as **Permit** or choose **Firewall > Access Policies** to create an access policy permitting any traffic. See Chapter 8, "Policies."

Example 1: L3 Unicast: (default policy) Route / Load Balancing

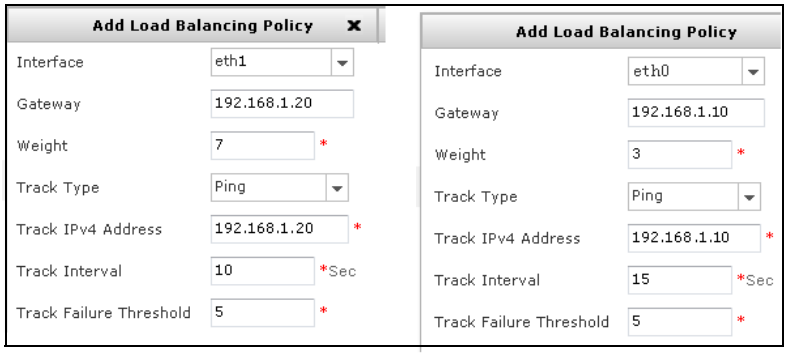
The internal network of a company is connected to the Internet through two service providers. Because ISP A has a better bandwidth and service quality than ISP B, the company wants to configure FGX to appropriately distribute the traffic to the two providers by assigning a weight of 7 to ISP A and a weight of 3 to ISP B. The company also wants to probe the links to the two providers, so traffic can still be forwarded through the other link when one link fails.



1. Choose **Network > Routing > Default Routing**.
2. Click **New** to create a default IPv4 route.



3. In **Load Balancing Policy List**, click **Add** to add the following two load balancing policies:



4. Click **OK**.Click .

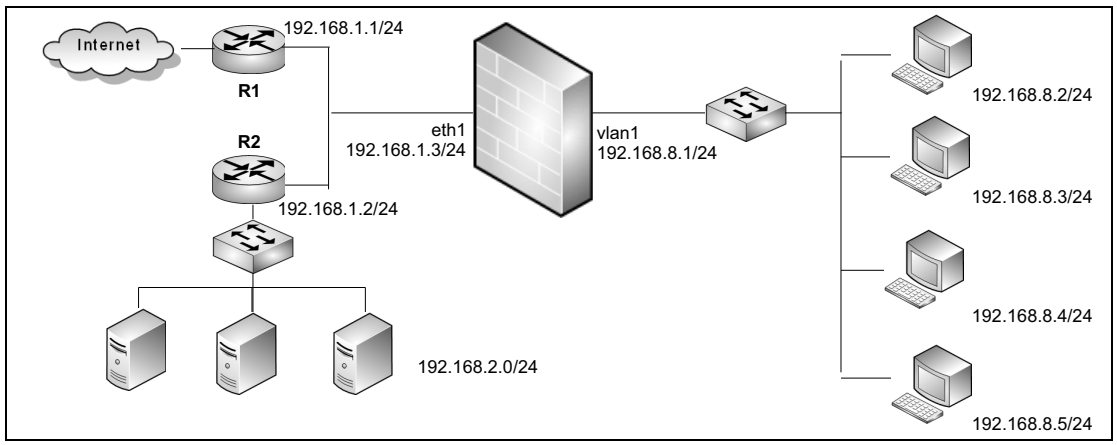
CLI

```
FGX@root> configure mode override
FGX@root-system] route 0.0.0.0 0.0.0.0 load-balancing interface eth1
gateway 192.168.1.20 7 ip-track ping 192.168.1.20 10 5 1
FGX@root-system] route 0.0.0.0 0.0.0.0 load-balancing interface eth1
gateway 192.168.1.10 3 ip-track ping 192.168.1.10 15 5 1
FGX@root-system] exit
FGX@root> save config
```

Example 2: L3 Unicast: Policy-based routes

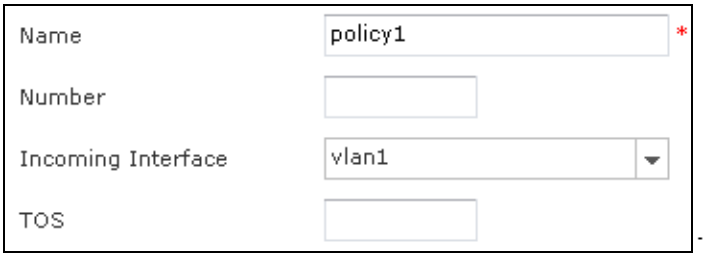
Four hosts in an internal network are connected to the Internet and another internal network through FGX.

- The two hosts at 192.168.8.2/24 and 192.168.8.3/24 are allowed to access any network;
- 192.168.8.4/24 and 192.168.8.5/24 can access the internal server only for TCP 80 services.

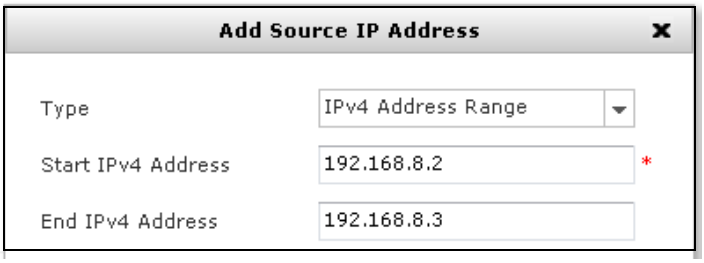


To create routing policies for the first two hosts:

1. Choose **Network > Routing > Policy-Based Routing**.
2. Click **New** to set policy name and interface receiving packets.

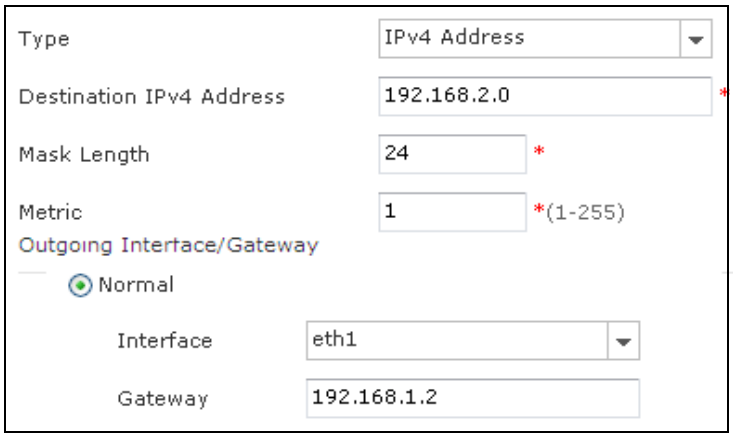


3. In the **Source IP Address** area, click **Source IP Address List** and click **Add** to add an IPv4 address range. Then click **OK**.

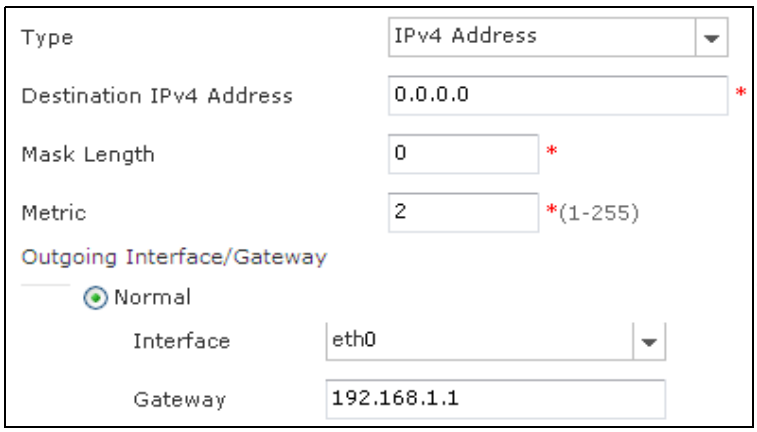


4. In the **Service** area, click **Any**.

5. Click **OK**.
6. Click "**policy1 Routing Table**" and click **New** to create a normal static route.



7. Click **OK**.
8. Click **New** to create a normal default route.



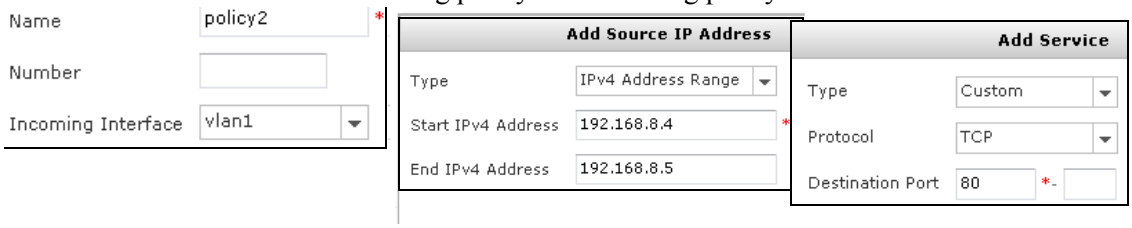
9. Click **OK**.Click  .

CLI

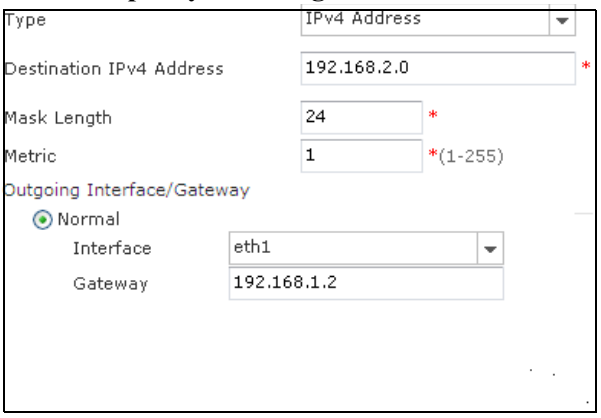
```
FGX@root> configure mode override
FGX@root-system] policy route policy1 enable
FGX@root-system-routepolicy-policy1] matching input-interface vlan1
FGX@root-system-routepolicy-policy1] matching sip 192.168.8.2
192.168.8.3
FGX@root-system-routepolicy-policy1] matching protocol any
FGX@root-system-routepolicy-policy1] route 192.168.2.0 255.255.255.0
interface eth1 gateway 192.168.1.2 1
FGX@root-system-routepolicy-policy1] route 0.0.0.0 0.0.0.0 interface
eth1 gateway 192.168.1.1 2
FGX@root-system-routepolicy-policy1] exit
FGX@root> save config
```

To create a routing policy for the other two hosts:

1. Choose **Network > Routing > Policy-Based Routing**.
2. Click **New** to create the following policy-based routing policy:



3. Click **OK**.
4. Click "**policy2 Routing Table**" and click **New** to create a normal static route.



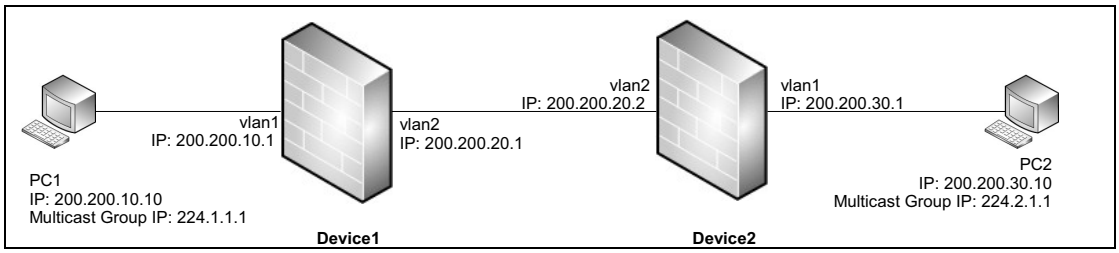
5. Click **OK**.Click .

CLI

```
FGX@root> configure mode override
FGX@root-system] policy route policy2 enable
FGX@root-system-routepolicy-policy2] matching input-interface vlan1
FGX@root-system-routepolicy-policy2] matching sip 192.168.8.4
192.168.8.5
FGX@root-system-routepolicy-policy2] matching protocol tcp 80
FGX@root-system-routepolicy-policy2] route 192.168.2.0 255.255.255.0
interface eth1 gateway 192.168.1.2 1
FGX@root-system-routepolicy-policy2] end
FGX@root> save config
```

Example 3: L3 multicast dynamic (DVMRP)

Users at PC1 and PC2 want to hold a video meeting. PC1 plays the video using multicast group IP address 224.1.1.1, and PC2 using 224.2.1.1. The TTL value of multicast packets is 3. You can configure DVMRP on Device1 and Device2 so that the two users can hold a video meeting.

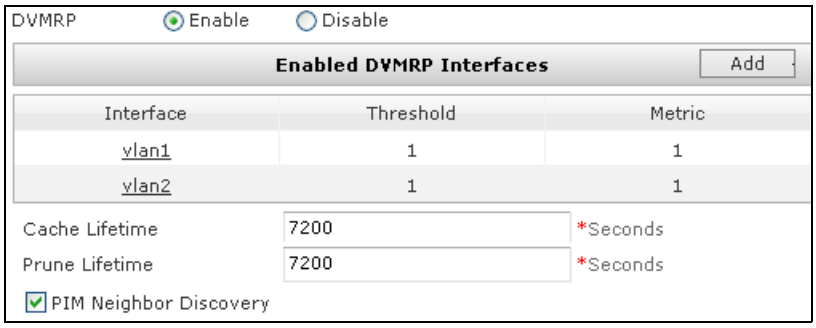


Do the following on Device1 and Device2:

- Create an access policy to permit inter-zone access on each FGX device. See Example 2. Create Access Policy.
- Create a multicast policy to permit multicast traffic to be forwarded. See 8.2.4 Create Multicast Policy.

Device1

1. Choose **Network > Multicast > DVMRP**.
2. Click **Enable** to enable the DVMRP function.
3. Click **Add** and configure DVMRP interfaces as follows:
   a. Choose the interface vlan1 for forwarding multicast packets.
   b. Set the threshold of vlan1 = 1. Multicast packets with TTL = 3 can be forwarded.
   c. Set the metric of vlan1 as 1 for route exchange and update.
   d. Click **OK**.
   Set vlan2 the same way.



4. Set the cache lifetime of the DVMRP route learned from Device2 as 7,200 seconds. The route stays in Device1 cache for 2 hours. If not used during the 2 hours, route is removed.
5. Set the prune lifetime of Device1 as 7,200 seconds.
   - During this period, Device1 prunes multicast packets to Device2;
   - After this period, Device1 resumes forwarding packets to Device2.
6. (Optional) Check **PIM Neighbor Discovery** so DVMRP on Device1 can support PIM neighbor discovery.
7. Click **OK**.Click .

To monitor dynamic multicast routes or DVMRP neighbors, choose **Monitor > Route** or **Monitor > Multicast > DVMRP Neighbors**. For information, see 14.15.1 DVMRP Neighbors.

CLI

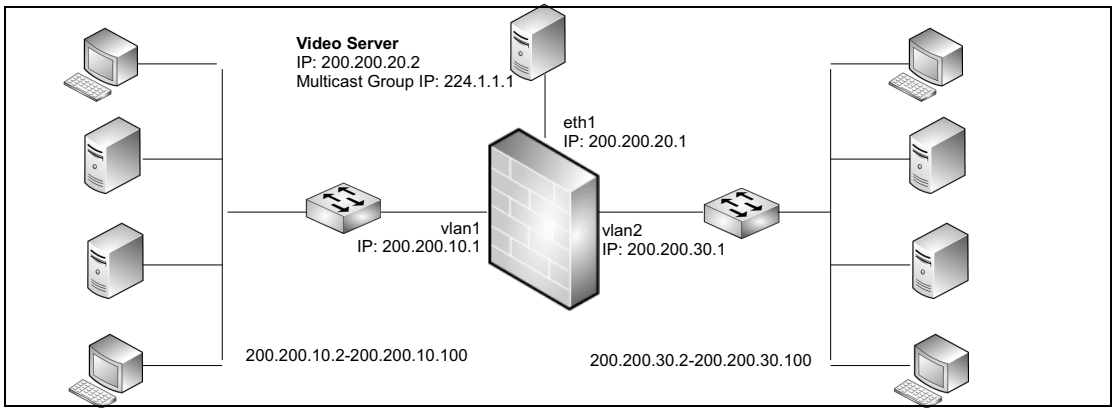
```
FGX@root> configure mode
FGX@root-system] dvmrp enable
FGX@root-system] vlan 1
FGX@root-system-vlan1] dvmrp on
FGX@root-system-vlan1] vlan 2
FGX@root-system-vlan2] dvmrp on
FGX@root-system-vlan2] exit
FGX@root-system] dvmrp cache-lifetime 7200
FGX@root-system] dvmrp pim enable
FGX@root-system] policy default inter-zone access permit
FGX@root-system] exit
FGX@root> save config
```

Device2

Configure the same way. After you complete all configurations, the two users at PC1 and PC2 can hold a video meeting.

Example 4: L3 multicast static

The video server plays programs using the multicast group IP address 224.1.1.1. The TTL value of the multicast packets is 5. You configure FGX so that hosts in vlan1 and vlan2 can watch the video programs played on the video server.

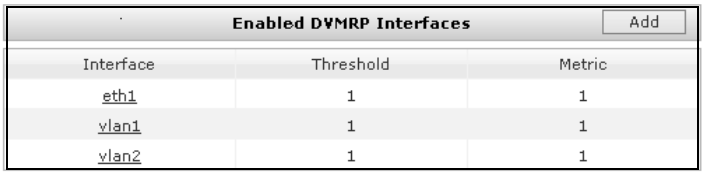


Create in advance a multicast policy to permit multicast traffic to be forwarded among different interfaces. See 8.2.4 Create Multicast Policy.

Configure DVMRP

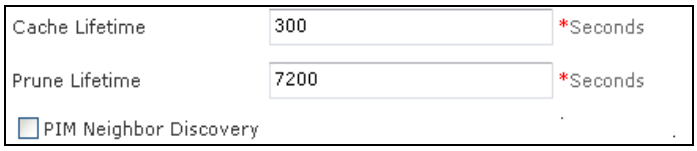
1. Choose **Network > Multicast > DVMRP**.
2. Click **Enable** to enable DVMRP on FGX. Only after you enable DVMRP can multicast routing take effect.

3. In the **Enabled DVMRP Interfaces** list, add the following interfaces:



The threshold and metric do not take effect in static routing.

4. For other 3 global parameters, keep default values. They have no effect in static routing.



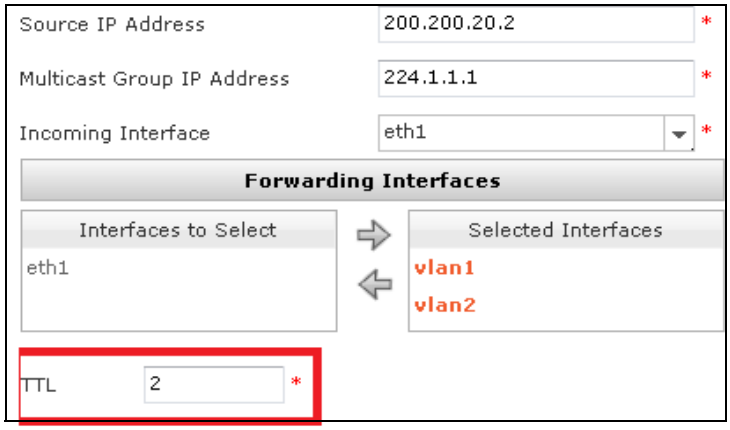
5. Click **OK**. Click .

CLI

```
FGX@root> configure mode
FGX@root-system] dvmrp enable
FGX@root-system] vlan 1
FGX@root-system-vlan1] dvmrp on
FGX@root-system-vlan1] interface ethernet 1
FGX@root-system-if-eth1] dvmrp on
FGX@root-system-if-eth1] vlan 2
FGX@root-system-vlan2] dvmrp on
FGX@root-system-vlan2] exit
FGX@root-system] dvmrp pim disable
FGX@root-system] exit
FGX@root> save config
```

Create Static Multicast Route

1. Click the **Multicast Routing** hyperlink.
2. Click **New** to create the following static multicast route:



Because the TTL value of multicast packets is 5, to allow FGX to forward multicast packets, you need to set the TTL of the static multicast route less than 5 (in this example, 2).

3. Click **OK**.Click .

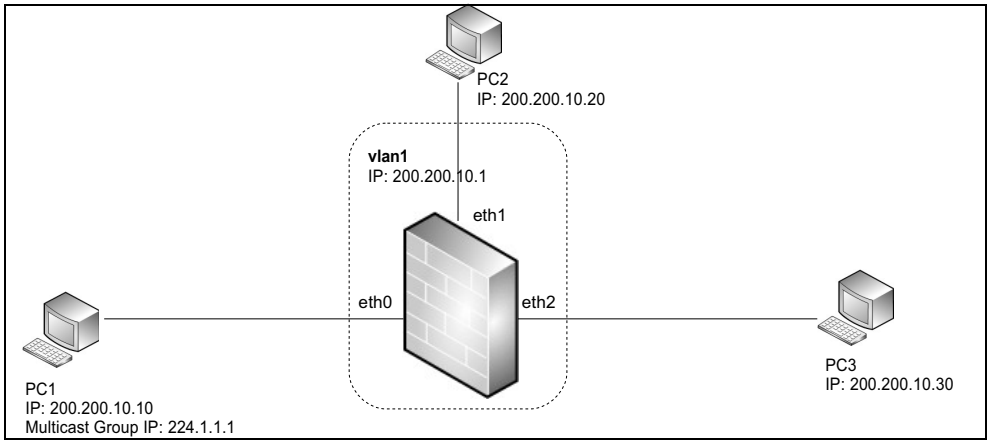
CLI

```
FGX@root> configure mode
FGX@root-system] dvmrp route 200.200.20.2 224.1.1.1 input eth1
forwarding vlan1,vlan2 threshold 2
FGX@root-system] exit
FGX@root> save config
```

Example 5: L2 multicast dynamic (IGMP Snooping)

vlan1 includes three Layer 2 Ethernet interfaces eth0, eth1, and eth2. PC1 serves as a multicast source and plays video programs through the multicast group IP address 224.1.1.1.

Configure IGMP snooping for vlan1. When PC2/PC3 users order programs, PC2/PC3 send IGMP membership reports to 224.1.1.1. FGX snoops the reports, creates dynamic CAM entries, and PC2/PC3 receive the multicast. If either user closes the program, the user's PC sends a leave group message, FGX can delete the corresponding dynamic CAM entry.



Create multicast policy to permit multicast traffic forwarding. See 8.2.4 Create Multicast Policy.

1. Choose **Network > Multicast > IGMP Snooping** and click corresponding to vlan1.
2. Click **On** in the **Active** field to enable IGMP snooping and set as follows:

3. Click **OK**.Click .

To monitor IGMP snooping state, click the **IGMP Snooping State** hyperlink or choose **Monitor > Multicast > IGMP Snooping State**. For information, see 14.15.2 IGMP Snooping State.

After dynamic CAM entries are created, you can choose **Monitor > CAM** to monitor them.

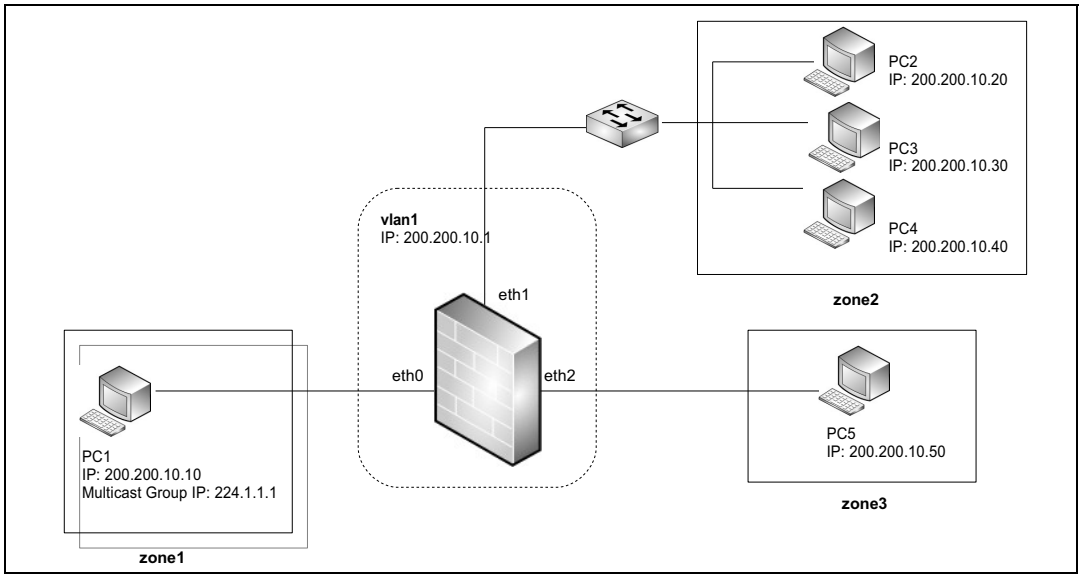
CLI

```
FGX@root> configure mode override
FGX@root-system] vlan 1
FGX@root-system-vlan1] igmp-snooping on
FGX@root-system-vlan1] igmp-snooping version ethernet 0 v2
FGX@root-system-vlan1] igmp-snooping version ethernet 1 v2
FGX@root-system-vlan1] igmp-snooping version ethernet 2 v2
FGX@root-system-vlan1] igmp-snooping interface-flags ethernet 0 host
FGX@root-system-vlan1] igmp-snooping interface-flags ethernet 1 host
FGX@root-system-vlan1] igmp-snooping interface-flags ethernet 2 host
FGX@root-system-vlan1] end
FGX@root> save config
```

Example 6: L2 multicast static

The VLAN interface vlan1 includes three Layer 2 Ethernet interfaces eth0, eth1, and eth2. PC1 serves as a multicast source and plays video programs through the multicast group IP address 224.1.1.1.

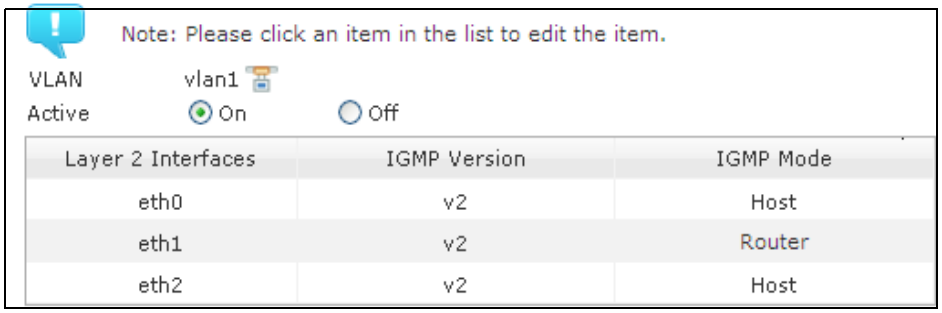
You configure IGMP snooping for vlan1. Create a static multicast CAM entry so that PC2, PC3, and PC4 can always receive multicast video traffic. The user at PC5 can receive multicast video traffic only after the user order the programs.



Create in advance a multicast policy to permit multicast traffic forwarding among the three zones. See Example 3. Apply Multicast Policy Among Zones.

Configure IGMP Snooping for vlan1

1. Choose **Network > Multicast > IGMP Snooping** and click corresponding to vlan1.
2. Click **On** in the **Active** field to enable IGMP snooping and set the IGMP versions and modes of Layer 2 interfaces as follows:



3. Click **OK**.Click .

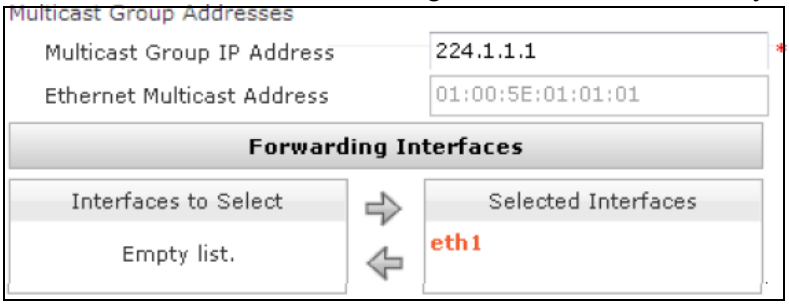
To monitor IGMP snooping state, click the **IGMP Snooping State** hyperlink or choose **Monitor > Multicast > IGMP Snooping State**. For information, see 14.15.2 IGMP Snooping State.

CLI

```
FGX@root> configure mode override
FGX@root-system] vlan 1
FGX@root-system-vlan1] igmp-snooping on
FGX@root-system-vlan1] igmp-snooping version ethernet 0 v2
FGX@root-system-vlan1] igmp-snooping version ethernet 1 v2
FGX@root-system-vlan1] igmp-snooping version ethernet 2 v2
FGX@root-system-vlan1] igmp-snooping interface-flags ethernet 0 host
FGX@root-system-vlan1] igmp-snooping interface-flags ethernet 1
multicast-router
FGX@root-system-vlan1] igmp-snooping interface-flags ethernet 2 host
FGX@root-system-vlan1] end
FGX@root> save config
```

Create Static Multicast CAM Entry

1. Choose **Network > Multicast > IGMP Snooping**.
2. Click the **Multicast CAM table of vlan1** hyperlink.
3. Click **New** to create the following static multicast CAM entry:



4. Click **OK**.Click  .

To monitor static and dynamic multicast CAM entries, choose **Monitor > CAM**. For information, see 14.7 CAM.

CLI

```
FGX@root> configure mode override
FGX@root-system] vlan 1
FGX@root-system-vlan1] multicast cam-table 224.1.1.1 eth1
FGX@root-system-vlan1] end
FGX@root> save config
```

6.5.Parameter Reference

This section describes parameters used when configuring routing and multicasting functions:

- 6.5.1 L3 Unicast Route Parameters
- 6.5.2 L3 Unicast Policy Parameters
- 6.5.3 L3 multicast dynamic (DVMRP) Parameters
- 6.5.4 L3 multicast Static Parameters
- 6.5.5 L2 multicast dynamic (IGMP Snooping) Parameters
- 6.6. L2 multicast Static (CAM Entry) Parameters

6.5.1 L3 Unicast Route Parameters

Parameter	Description
Type	Type of an IP address. FGX supports IPv4 and IPv6 addresses.
Destination IPv4 Address/Destination IPv6 Address	The IP address of the destination host or network that packets are sent to. The destination IPv4 and IPv6 addresses of a default route are 0.0.0.0 and "::".
Mask Length/Prefix	The mask length of a destination IPv4 address or the prefix length of a destination IPv6 address. The mask length or prefix length of a default route is 0. The mask length range is 0-32, prefix length range is 0-128.
Metric	Indicates the priority of a route. The metric range is 1-255. The smaller the metric, the higher the priority.
Outgoing Interface/ Gateway	Set an outgoing interface or a gateway address or both for a static route. You are required to set either a static route with or without load balancing.
Normal	Configure a static route without load balancing. You are required to set at least one of the following: • **Interface—**the Layer 3 interface through which packets are forwarded out. If you choose the null interface, packets will be dropped and you cannot configure a gateway. • **Gateway—**the IP address of a next-hop routing device when a remote network cannot be reached directly.
Load Balancing	Configure a static route with load balancing. You can configure the following parameters for a load balancing policy: • **Interface—**the Layer 3 interface through which packets are forwarded out. • **Gateway—**IP address of a next-hop routing device when a remote network cannot be reached directly. • **Weight—**the session proportion that a next-hop routing device can get. The greater the weight, the more sessions the routing device can get. The weight range is 1-255. It is 1 by default. • **Track Type—**the method used for tracking an IP address. FGX supports ARP Ping, Ping, TCP Ping, and NS Ping. You can set the track type as None, meaning that FGX does not perform IP tracking. None is the default track type. ARP Ping can track only IPv4 addresses in internal networks of FGX, and NS Ping can track only IPv6 addresses. • **Track IPv4 Address/Track IPv6 Address—**the IPv4 or IPv6 address of the routing device to be tracked. • **Track Port—**the port of a routing device to be tracked when TCP Ping is used. Range is 1-65535. • **Track Interval—**the interval in seconds between two link probes. Range is 1-30,000 secs. Default = 3. • **Track Failure Threshold—**the maximum number of consecutive failures allowed when FGX tracks an IP address. If the number of track failures reaches the threshold and no replies are received within a specified period of time, the link is considered to have failed. Range is 1-999. It is 3 by default. You can configure up to 8 load balancing policies for a static route.

6.5.2 L3 Unicast Policy Parameters

Table 140 Parameters of Policy-Based Routing Policies

Parameter	Description
Number	Indicates the priority of a policy-based routing policy. The lower the number, the higher the priority. If you do not specify a number for a new policy-based routing policy, the priority of the policy will be the lowest automatically.
Name	The unique identifier of a policy-based routing policy. It can be composed of 1-15 UTF-8 characters. Cannot contain ? , " ' \ < > & # or spaces.
Incoming Interface	The Layer 3 interface through which packets are received. It can also be any available Layer 3 interface.
TOS	Define a delivery service for packets in terms of throughput, delay, reliability, and monetary cost. The TOS value range is 0-15, among which: • 0 requires no services. • 1 requires a minimum latency. • 2 requires a maximum throughput. • 4 requires a maximum reliability. • 8 requires a minimum cost.
Source IP Address	The IP address from which packets are sent. A source IP address can be one of the following types: • **Any—**includes all IPv4 and IPv6 addresses. • **Any IPv4 Address—**includes all IPv4 addresses. • **Any IPv6 Address—**includes all IPv6 addresses. • **Use the Following List—**includes IP address objects, object groups, IPv4 addresses, IPv4 address ranges, IPv4 addresses and mask lengths, IPv6 addresses, IPv6 address ranges, and IPv6 addresses and prefix lengths. You can configure up to 32 source IP address entries.
Service	Type of transport layer service used by packets. A service type can be either of the following: • **Any—**includes all types of protocols. • **Use the Following List—**includes objects, object groups, and custom protocols. Custom protocols include ICMP, ICMPv6, TCP, UDP, and other protocols. •When you set ICMP protocol, you can choose any of the following types: ECHO_and_ECHOREPLY, INFO_REQUEST_and_INFO_REPLY, TIMESTAMP_and_TIMESTAMPREPLY, ADDRESS_and_ADDRESSREPLY, ROUTER_ADVERTISEMENT, ROUTER_SOLICITATION, DEST_UNREACH, SOURCE_QUENCH, REDIRECT, TIME_EXCEEDED, PARAMETERPROB, and Any (representing any ICMP types). •When you set ICMPv6 protocol, you can choose any of the following types: DEST_UNREACH, PACKET_TOO_BIG, TIME_EXCEEDED, PARAMETERPROB, ECHO_and_ECHOREPLY, and Any (representing any ICMPv6 types). •The destination port number range of TCP or UDP is 1-65535. Other protocol number range is 1-255. You can configure up to 32 service entries.
Routing Table	The routing table to which a policy-based routing policy corresponds.

6.5.3 L3 multicast dynamic (DVMRP) Parameters

Table 141 Parameters of DVMRP

Parameter	Description
DVMRP	Enables or disables DVMRP on a FGX device. Disabled by default.
Enabled DVMRP Interfaces	Layer 3 interfaces (except loopback interfaces and tunnel interfaces) on which you enable DVMRP. Only DVMRP interfaces can handle and forward multicast data. • **Interface—**Layer 3 interface name. You can choose up to 32 interfaces. • **Threshold—**set for a DVMRP interface to control whether multicast packets are forwarded out of this interface. The threshold is used only in dynamic multicast routing. Only multicast packets with a TTL value > the threshold value of the receiving DVMRP interface can be forwarded through the interface. The threshold range is 1-255, and it is 1 by default. The packet TTL value (in hops) is the maximum routing devices that the packet can pass through. When the packet passes through a DVMRP routing device, its TTL value is reduced by 1. If its TTL value is = 0, the packet will be dropped. • **Metric—**set for a DVMRP interface and used for multicast route exchange and update. Metric is used only in dynamic multicast routing. The metric range is 1-32, and it is 1 by default.
Cache Lifetime	The length of time that a multicast route learned dynamically can stay in the cache. It must be a multiple of 5. Its range is 60-7,200 seconds. It is 300 seconds by default. When the cache lifetime of an unused dynamic route entry is exceeded, FGX deletes it.
Prune Lifetime	The length of time in which FGX should hold a prune state. It must be a multiple of 5. Its range is 120-7,200 seconds. It is 7,200 seconds by default. When the prune lifetime is exceeded, FGX resumes the forwarding of multicast packets to its downstream routers.
PIM Neighbor Discovery	If enabled, FGX can listen to PIM messages and establish neighbor relationships with multicast routers running PIM. Disabled by default.

6.5.4 L3 multicast Static Parameters

Table 142 Parameters of Static Multicast Routes

Parameter	Description
Source IP Address	The IP address from which multicast packets are sent.
Multicast Group IP Address	The IP address of a destination multicast group: 224.0.0.0-239.255.255.255.
Incoming Interface	The DVMRP interface through which multicast packets are received. The incoming interface cannot be the same as any of the forwarding interfaces.
Forwarding Interfaces	The DVMRP interfaces through which multicast packets are forwarded out.
TTL	Controls whether multicast packets are forwarded out of the DVMRP interfaces. It is actually the same as DVMRP threshold. For more information, see Table 141 Parameters of DVMRP for the threshold explanation.

6.5.5 L2 multicast dynamic (IGMP Snooping) Parameters

All VLANs can support IGMP snooping. You must enable IGMP snooping on a VLAN if you want the VLAN to support multicast and have the IGMP snooping function. Otherwise, packets will be forwarded out through all interfaces in the VLAN.

Table 143 Parameters of IGMP Snooping

Parameter	Description
VLAN	VLAN interface name. You can configure IGMP snooping only for VLANs. IGMP snooping supports up to 1,024 VLANs.
Active	Enables or disables IGMP snooping on a VLAN: • **On—**enables IGMP snooping. • **Off—**disables IGMP snooping. IGMP snooping is disabled by default. After you enable IGMP snooping, it will take effect after 255 seconds.
Layer 2 Interfaces	Layer 2 interfaces included in a VLAN. Each VLAN supports up to 32 interfaces.
IGMP Version	IGMP version used by the Layer 2 interfaces in a VLAN: • **Auto—**the interface can dynamically identify IGMP version through analyzing received messages. **Auto** is chosen by default. • **v1—**IGMPv1. FGX cannot process IGMPv2-specific messages, such as leave group messages. • **v2—**IGMPv2. FGX can process both IGMPv1 and IGMPv2 messages. Routing devices on the same network segment must use the same IGMP versions.
IGMP Mode	The type of network connected to the Layer 2 interface in a VLAN: • **Auto—** the interface can dynamically identify network types through analyzing received messages. **Auto** is chosen by default. • **Router—**the device connected to the interface is a multicast router. • **Host—**the device connected to the interface is a host.

6.6.L2 multicast Static (CAM Entry) Parameters

Table 144 Parameters of Multicast CAM Tables

Parameter	Description
Multicast Group IP Address	The IP address of a destination multicast group. Multicast group IP address range is 224.0.0.0-239.255.255.255.
Ethernet Multicast Address	The MAC address corresponding to the multicast group IP address. The system automatically calculates the MAC address depending on the IP address.
Forwarding Interfaces	The interfaces through which multicast packets are forwarded in a VLAN. You are required to choose at least one forwarding interface for a static multicast CAM entry. If a chosen interface is not active, multicast packets will not be forwarded to it. You can choose up to 32 forwarding interfaces for a multicast CAM entry.

7 Quality of Service

This chapter describes FGX Quality of Service (QoS) functionality.

- 7.1. Basic Concepts. Describes QoS concepts and fundamentals.
- 7.2. Basic configuration steps. Describes basic configuration steps and the UI dialogs. Your scenario will not require all of these steps.
- 7.3. Example. Gives detailed step-by-step examples.
- 7.4. Parameter reference. Describes in detail all QoS parameters.

7.1. Basic Concepts

Quality of Service (QoS) is the capability of a network to provide better service to selected network traffic. Basic QoS concepts:

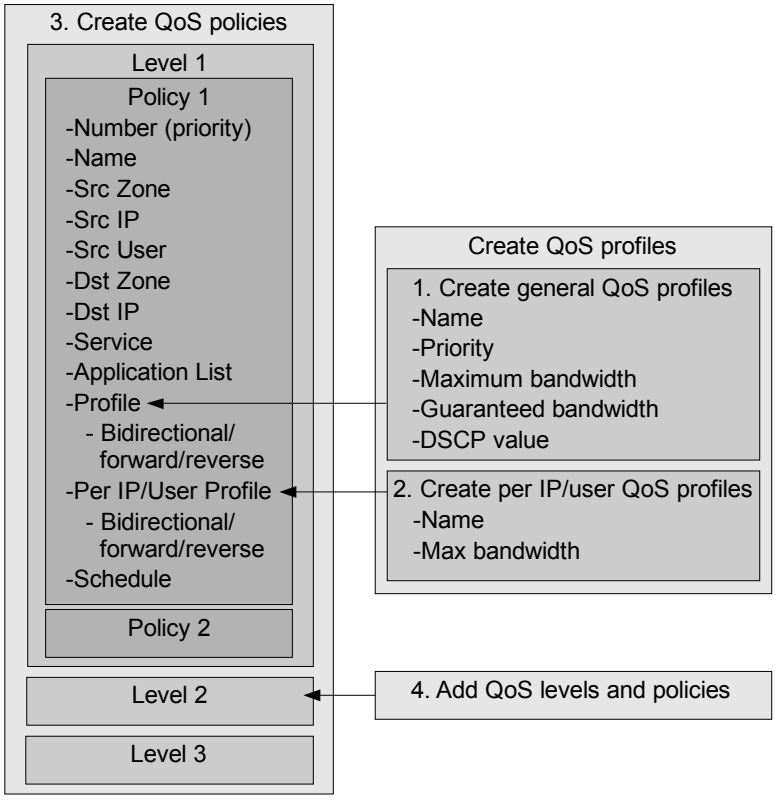
- **Policy number**—priority of a QoS policy.
- **Matching conditions**—includes:
  - Source zone/IPs (can be any)
  - Destination zone/IPs (can be any)
  - Source users (can be any)
  - Service (can be any)
  - Application list
- **General QoS profiles**—specifies the maximum and guaranteed bandwidth, priority, and DSCP value of all traffic.
- **Per IP/user QoS profiles**—specifies the maximum bandwidth of per IP/user traffic.
- **Schedule**—the time a QoS policy takes effect.
- **Multi-level QoS**—inline QoS modules specifying multiple policies. A data flow goes through each level of QoS bandwidth control one by one.

7.2. Basic configuration steps

This section includes:

- 7.2.1 Create general QoS profiles
- 7.2.2 Create per IP/user QoS profiles
- 7.2.3 Create QoS policies

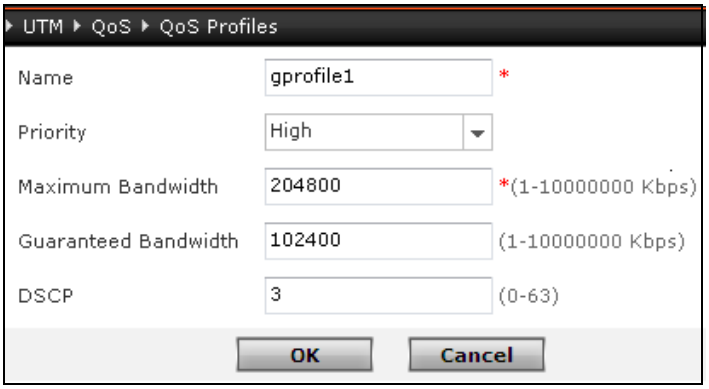
Figure 29 QoS Configuration Steps



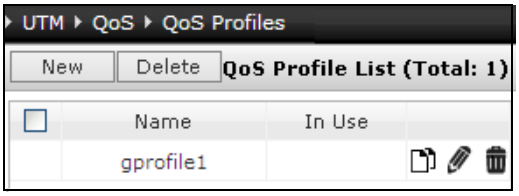
Note: QoS can be configured through the WebUI only.

7.2.1 Create general QoS profiles

1. Choose **UTM > QoS > QoS Profiles**.
2. Click **New** and create a general QoS profile.



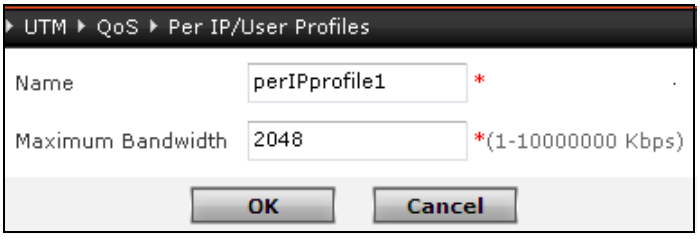
3. Click **OK**.



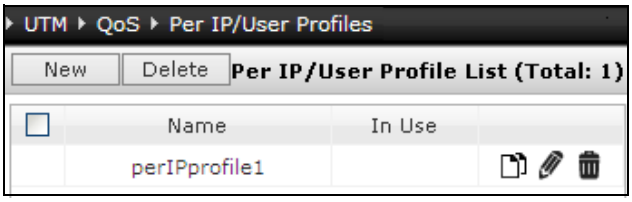
4. Click to clone a profile. If a profile is used by QoS policies, click the corresponding icon under **In Use** to view policies using the profile.

7.2.2 Create per IP/user QoS profiles

1. Choose **UTM > QoS > Per IP/User QoS Profiles**.
2. Click **New** and create a per IP/user QoS profile.



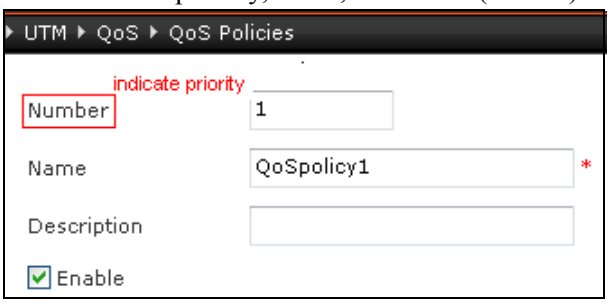
3. Click **OK**.



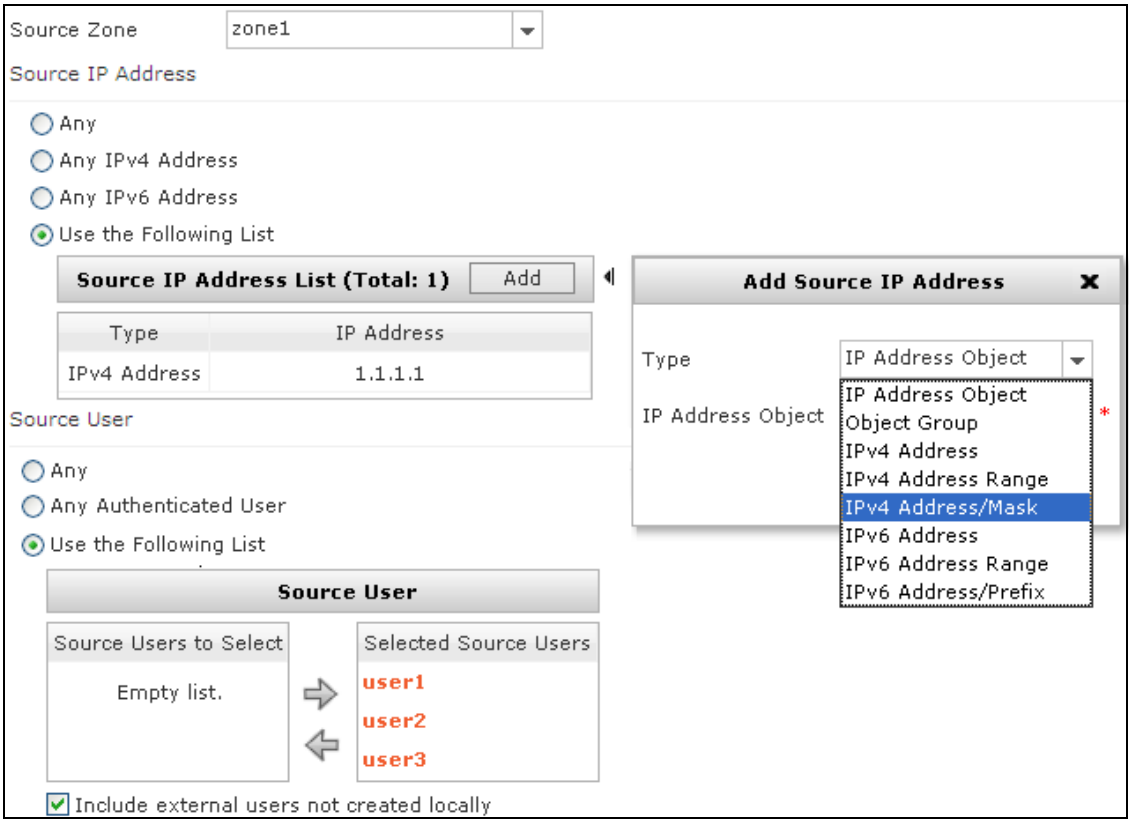
4. Click to clone a profile. If a profile is used by QoS policies, click the corresponding icon under **In Use** to view policies using the profile.

7.2.3 Create QoS policies

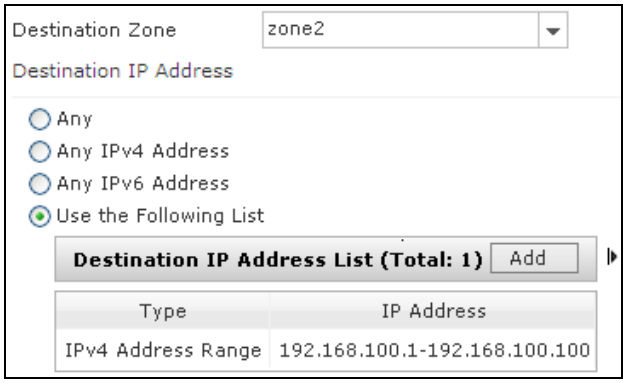
1. Choose **UTM > QoS > QoS Policies**.
2. Click **New** and create a QoS policy.
   a. Set the priority, name, and status (Enable).



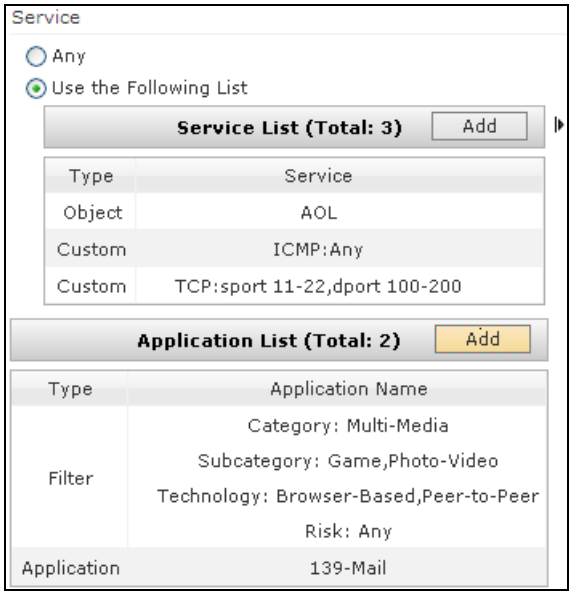
   b. Set the source zone, source IP addresses, and source users.



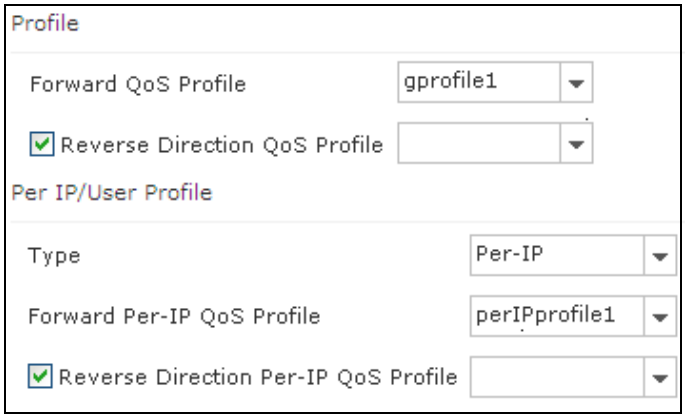
c. Set the destination zone and IP address.



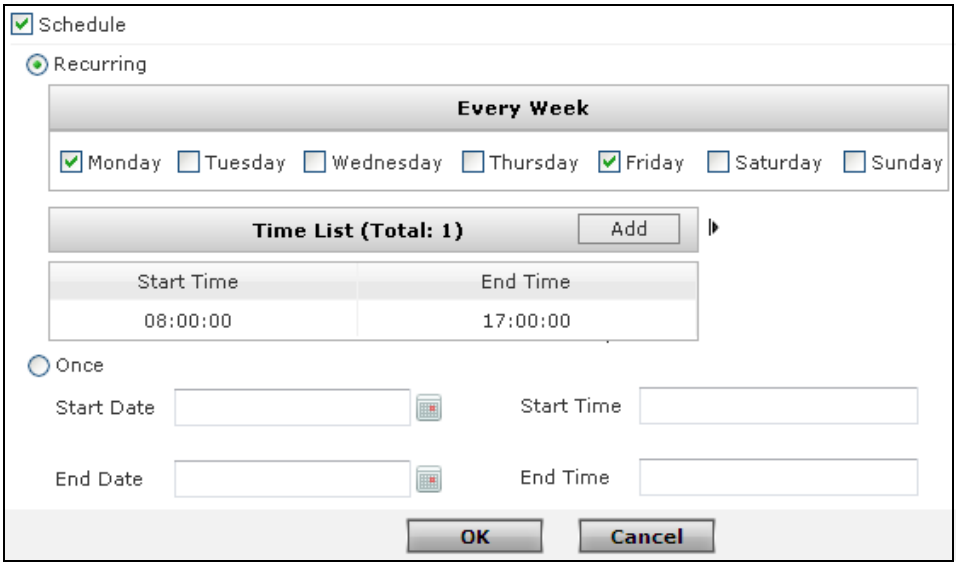
d. Set the service and applications. See 10.2.1.2.3. Create application control profiles for details about how to add applications to the list.



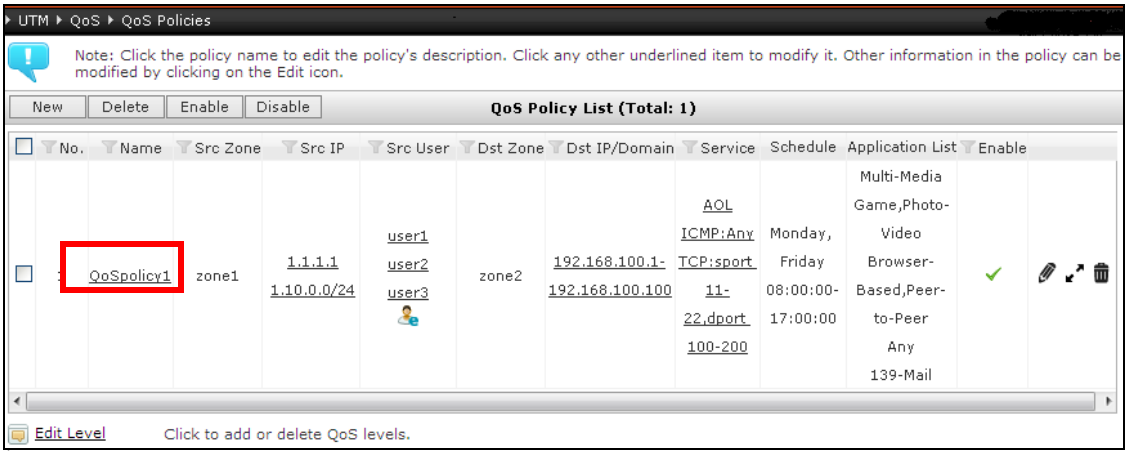
e. Set the general and per IP/user QoS profile.



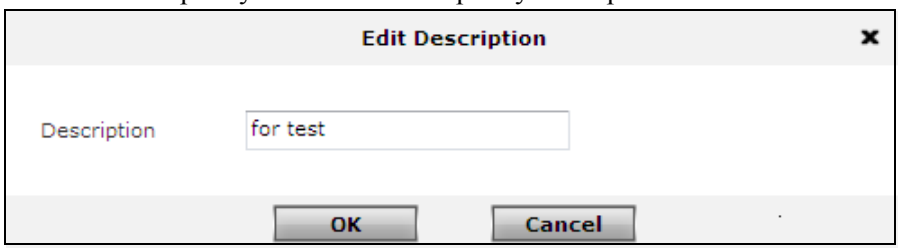
f. Set the schedule.



3. Click **OK**.

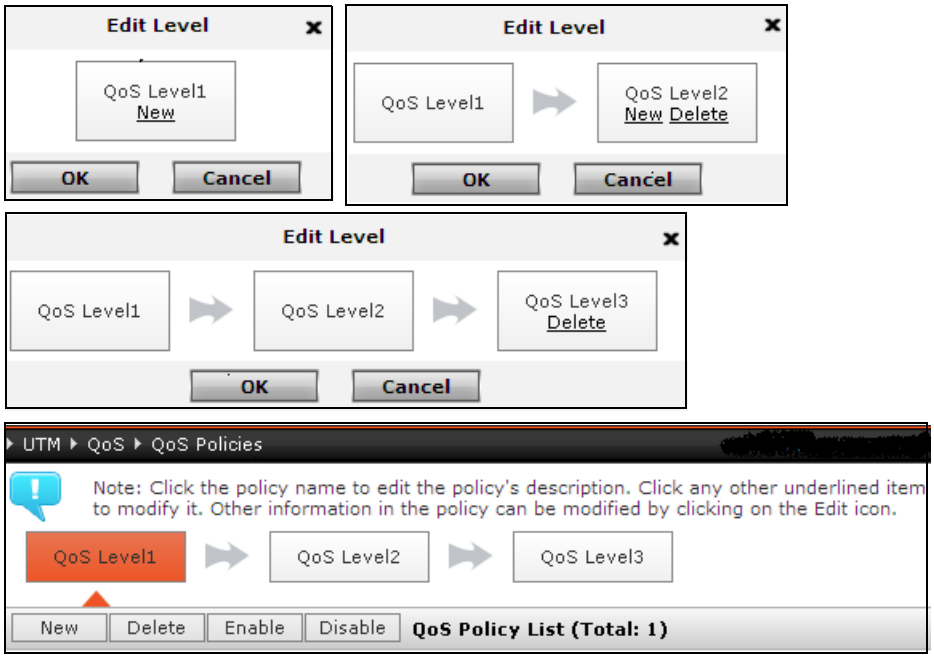


- Click to move a policy to change its priority (within the same level).
- Click to set filters to search for QoS policies.
- Click a policy name to edit the policy description:



- Click the hyperlinks of Src IP, Src User, Dst IP/Domain, and Service to edit the details.

4. To configure multi-level QoS, click the **Edit Level** hyperlink, add QoS levels, and add QoS policies in corresponding levels.



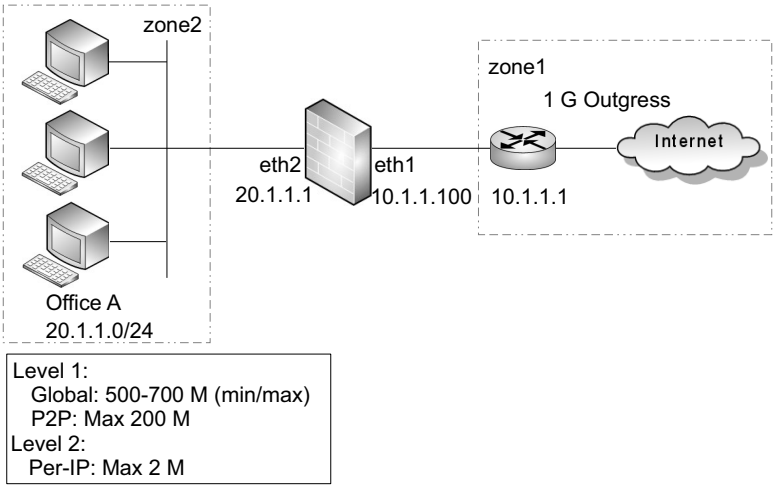
7.3. Example

There are two offices in a department: Office A and Office B. Office A are the development team and require little P2P traffic. Office B are the testing team and require high P2P traffic bandwidth. The network administrator wants to:

- guarantee 500 min and limit to 700 max for overall IP traffic.
- limit the P2P traffic bandwidth no more than 200 M (no min specified) to ensure the P2P traffic bandwidth of the other offices.
- limit per-IP traffic no more than 2 M. (Each employee has only one IP address.)

The network topology is shown in Figure 30.

Figure 30 QoS Example

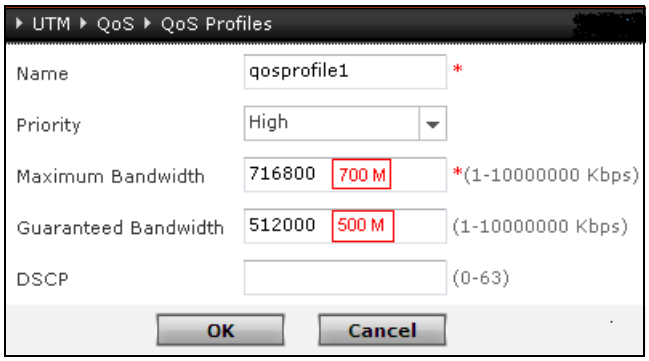


Configuration steps include:

- 7.3.1. Create general QoS profiles (max/min bandwidth)
- 7.3.2. Create per-IP QoS profile (max bandwidth)
- 7.3.3. Edit QoS levels
- 7.3.4. Create multi-level QoS policies

7.3.1. Create general QoS profiles (max/min bandwidth)

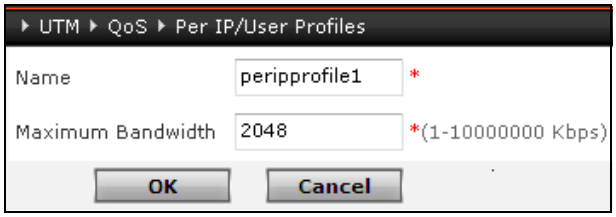
1. Choose **UTM > QoS > QoS Profiles**.
2. Click **New** and create QoS profile qosprofile1 for Office A as follows:



3. Click **OK**.
4. Click **New** and create QoS profile qosprofile2 for Office A. **Maximum Bandwidth** is set as 204800 Kbps (200M).
5. Click  .

7.3.2. Create per-IP QoS profile (max bandwidth)

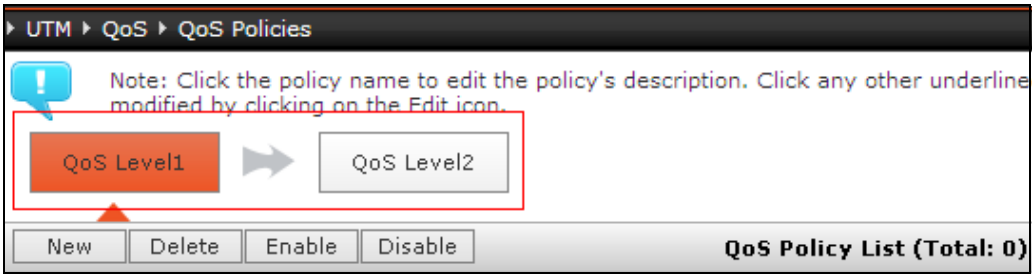
1. Choose **UTM > QoS > Per IP/User Profiles**.
2. Click **New** and create per-IP QoS profile peripprofile1 for Office A as follows:



3. Click  .

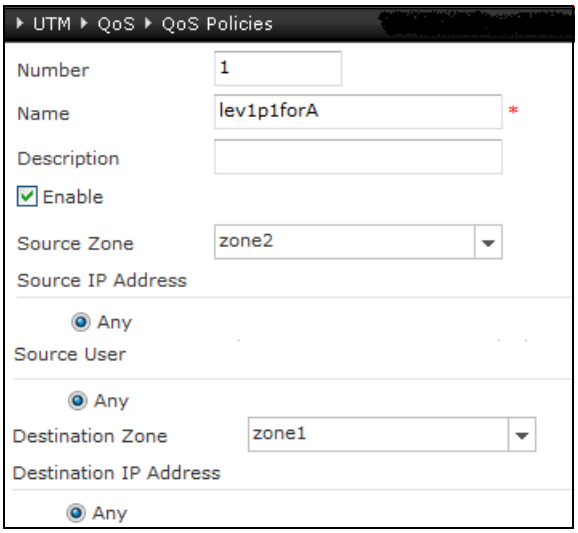
7.3.3. Edit QoS levels

1. Choose **UTM > QoS > QoS Policies**.
2. Click **Edit Level**, click **New**, and click **OK**.



7.3.4. Create multi-level QoS policies

1. Choose **UTM > QoS > QoS Policies**.
2. Click **QoS Level1** and create QoS policy lev1p1forA for Office A as follows:



3. Click **OK**.
4. Click **QoS Level2** and click **New** to create QoS policy lev2p1forA for Office A:

   Source Zone: zone2

   Destination Zone: zone1

   Profile:

   Bidirectional QoS Profile: qosprofile2
5. Click **OK**.
6. Click  .

7.4. Parameter reference

This section describes parameters for:

- 7.4.1. QoS Policies
- 7.4.2. QoS Profiles
- 7.4.3. Per IP/User QoS Profiles

7.4.1. QoS Policies

Table 145 Parameters of QoS Policies

Parameter	Description
No.	QoS policy priority. 1-80,000. 1 is highest priority.
Name	QoS policy name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces.
Src Zone	QoS policy source zone. Any by default.
Src IP	QoS policy source IP address or address range.Each QoS policy can have up to 4,096 source IP addresses or address ranges.
Src User	Can be: • **Any** (default)**—**authenticated or unauthenticated users. • **Any Authenticated User—**any authenticated users. • **Use the Following List—**Can include externally authenticated users not created on FGX. Each QoS policy can have up to 4,096 source users.
Dst Zone	QoS policy destination zone. Any by default.
Dst IP/Domain	Each QoS policy can have up to 4,096 destination IP addresses, address ranges, or domain names.
Service	The source and destination ports of packets matching a QoS policy. Add up to 32 entries (including max of 4,096 port numbers in total) to the service list, and the same entry cannot be added a second time.
Application List	The application(s) to be controlled by a QoS policy.You can add applications by application name or filter.
Schedule	The effective time of a QoS policy, including Recurring and Once.If the schedule is enabled but schedule is not set, it indicates that the policy is effective at any time.
Enable	A QoS policy is enabled by default.
Description	The description of a QoS policy. 0-255 UTF-8 characters. It cannot contain ? ” ' \ < > or &.
(General) Profile	A QoS profile used by a QoS policy to define the maximum bandwidth, guaranteed bandwidth, traffic priority, and DSCP value of the overall traffic. In a QoS policy, you can set one or two of the following types of QoS profiles: • **Bidirectional QoS Profile—**controls bandwidth of bidirectional traffic. • **Forward QoS Profile—**controls bandwidth of the traffic from the source to the destination. It is available only when reverse direction QoS profile is enabled. • **Reverse Direction QoS Profile—**controls the traffic from the destination to the source. A QoS profile can be used by multiple QoS policies.
Per IP/User Profile	A QoS profile used by a QoS policy to define the maximum bandwidth per IP or user. In a QoS policy, you can set the following information about a per IP/user QoS profile: • **Profile Type—**includes Per-IP and Per-User. • **Bidirectional Per IP/User QoS Profile**—controls bandwidth of bidirectional traffic per IP or user. • **Forward Per IP/User QoS Profile**—controls bandwidth of the per IP/user traffic from the source to the destination. It is available only when reverse direction per IP/user QoS profile is enabled. • **Reverse Direction Per IP/User QoS Profile—**controls the bandwidth of each IP or user’s traffic sent from the destination to the source.

7.4.2. QoS Profiles

Table 146 Parameters of (General) QoS Profiles

Parameter	Description
Name	General QoS profile name. 1-63 UTF-8 characters. It cannot contain ? , ” ' \ < > & # or spaces.
In Use	Click to view QoS policies using a general QoS profile. A general QoS profile can be used by multiple QoS policies. Profiles in use cannot be deleted.
Priority	Traffic forwarding priority. Traffic of services with higher priorities are forwarded first. When traffic reaches the maximum limit (as set in the QoS policy), lowest priority traffic is not forwarded. The highest 3 levels are high/medium/low guaranteed. The lowest 3 levels are high/medium/low non-guaranteed.
Maximum Bandwidth	Maximum bandwidth allowed. The specified service cannot occupy a bandwidth greater than this threshold. When this threshold value is greater than the system throughput, FGX will try its best to forward traffic.
Guaranteed Bandwidth	FGX makes sure the specified bandwidth is available as required. The guaranteed bandwidth must be smaller than or equal to the maximum bandwidth.
DSCP	A tag added to packets passing through FGX to indicate that those tagged packets are going to go through QoS control on subsequent network devices. For more information about DSCP (Differentiated Services Code Point), see RFC 2474.

7.4.3. Per IP/User QoS Profiles

Table 147 Parameters of Per IP/User QoS Profiles

Parameter	Description
Name	Per IP/user QoS profile name. 1-63 UTF-8 characters. It cannot contain ? , ” ' \ < > & # or spaces.
In Use	Click to view the QoS policies using a per IP/user QoS profile. A per IP/user QoS profile can be used by multiple QoS policies. Profiles in use cannot be deleted.
Maximum Bandwidth	Maximum bandwidth allowed for each IP or user.

8 Policies

Policies control the traffic passing through FGX. The main goal of FGX access control is to prevent unauthorized access.

This chapter describes:

- 8.1. Overview. Describes concepts and fundamentals.
- 8.2. Basic Configuration Steps. Describes basic configuration steps and the UI dialogs.
- 8.3. Examples. Describes how to configure IP-MAC binding, access, multicast, and session policies.
- 8.4. Parameter Reference. Describes in detail all parameters.

8.1. Overview

This section describes FGX policy concepts and fundamentals.

- 8.1.1 IP-MAC Binding
- 8.1.2 Access Policies
- 8.1.3 Default Access Policies
- 8.1.4 Multicast Policies
- 8.1.5 Session Policies

8.1.1 IP-MAC Binding

IP-MAC binding binds the IP address(es) of a host to the MAC address of the host's NIC, thus preventing IP address spoofing. This section includes:

- 8.1.1.1 IP-MAC Binding Policies
- 8.1.1.2 Policy Matching Order

8.1.1.1 IP-MAC Binding Policies

You must create an IP-MAC binding policy binding IPv4 or IPv6 address(es) with a MAC address; otherwise, FGX does not check whether the source IP address of a packet matches its source MAC address.

8.1.1.2 Policy Matching Order

1. Drop the packet if the source IP address matches that in an IP-MAC binding policy but the source MAC address does not match that in the policy.
2. Drop the packet if the source IP address does not have a match in an IP-MAC binding policy but the source MAC address has a match.
3. Drop the packet if neither the source IP address nor the source MAC address has a match in IP-MAC binding policies and the default action of IP-MAC binding is Deny.

8.1.2 Access Policies

Configure criteria in a policy for packets from specific sources to specific destinations.

8.1.2.1 Policy Content

In an access policy, you can set:

- Basic elements: Number (priority), name, description, state (enabled or disabled), and logging.
- Selection criteria: Source zone/user(s)/IP(s), destination zone/IP(s), service(s), and schedule(s).
- Actions for handling packets: Permit/deny, VPN tunneling, and transparent DNS proxy.
- Specific timeouts.

8.1.2.2 How a Policy Is Enforced

When receiving a packet,

- If it belongs to an existing session, perform stateful inspection on the packet and forward it if the packet session state matches that in the session table.
- If it belongs to no existing sessions, match it against all enabled access policies according to the priority from the highest to the lowest.
  - If the packet matches a policy and the policy action is Permit, save the packet session information in the session table and forward it. (If user authentication is also required, determine whether to forward the packet according to user permission.)

    If the action is Deny, drop the packet.
  - If the packet does not match any policy, apply the default inter-zone or intra-zone access policy to the packet.

8.1.3 Default Access Policies

Default access policies include:

- Default inter-zone policies: Permit/deny IP traffic between different zones. If there are no zones, all traffic is considered inter-zone traffic. The default action is Deny.
- Default intra-zone policies: Permit/deny IP traffic among different FGX interfaces within a zone. The default action is permit.

A default access policy has a lower priority than existing access policies.

8.1.4 Multicast Policies

On FGX, you can set multicast policies to control the forwarding of multicast data flow and multicast control flow. FGX forwards only the multicast packets that match all conditions specified in a multicast policy. On FGX, multicast policies permit the forwarding and routing of multicast packets from specific sources to destinations.

If you configure a multicast route without configuring a multicast policy for it, FGX will not forward packets of this route.

8.1.5 Session Policies

Session policies prevent session table flooding through limiting the number of sessions. A session policy specifies one of the following traffic limit types:

- **Source IP based session limit—**limits the number of concurrent sessions from each source IP address.
- **Destination IP based session limit—**limits the number of concurrent sessions to each destination IP address.
- **Source and destination IP (“policy based”)based session limit**—limits the number of concurrent sessions for the entire group (not each) of specified source and destination IP addresses.

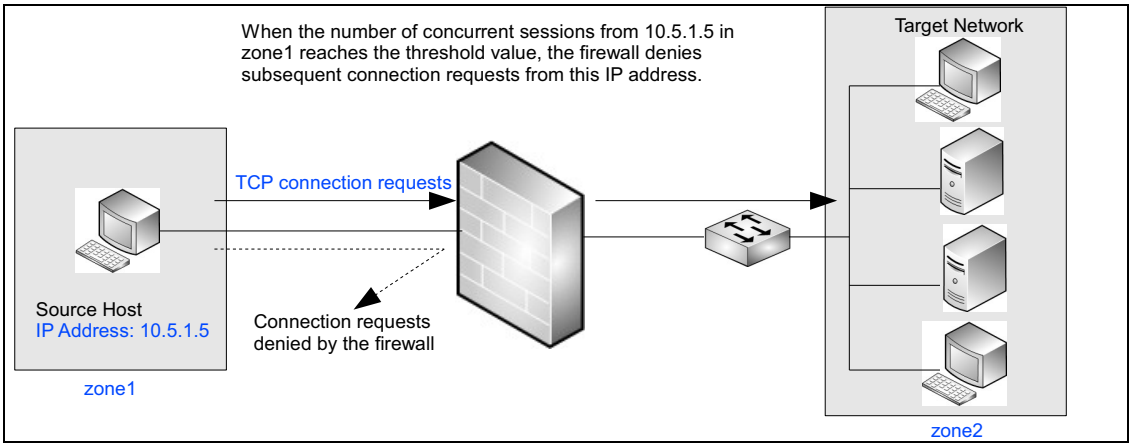
8.1.5.1 Source IP Based Session Limit

As shown in Figure 31, when sessions from a source IP address match the following defined in a source IP based session policy:

- Source IP address
- Source & destination zones
- Service

and the number of concurrent sessions from the source IP address reaches the maximum number (threshold) allowed, FGX denies subsequent connection requests from this IP address.

Figure 31 Source IP Based Session Limit



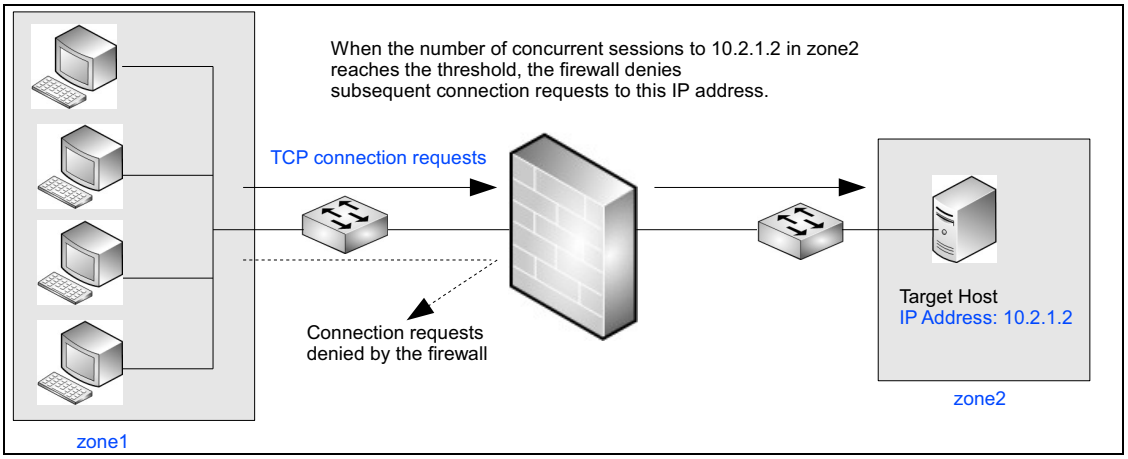
8.1.5.2 Destination IP Based Session Limit

As shown in Figure 32, when sessions to a destination IP address match the following defined in a destination IP based session policy:

- Destination IP address
- Source & destination zones
- Service

and the number of concurrent session requests to the destination reaches the maximum number (threshold) allowed, FGX denies subsequent connection requests to this IP address.

Figure 32 Destination IP Based Session Limit



8.1.5.3 Policy-Based Session Limit

When sessions from a source IP address to a destination IP address match the following defined in a policy-based session policy:

- Source & destination IP addresses
- Source & destination zones
- Services

and the number of concurrent session requests reaches the maximum number (threshold) allowed, FGX denies subsequent connection requests matching the policy.

8.2. Basic Configuration Steps

This section describes the basic configuration procedure.

- 8.2.1 Configure IP-MAC Binding
- 8.2.2 Create Access Policy
- 8.2.3 Configure Default Access Policies
- 8.2.4 Create Multicast Policy
- 8.2.5 Create Session Policy

Create in advance:

- Zone, choose **Network** > **Zones**.
- User, choose **System** > **Authentication** > **Users**.
- IP address object or object group, choose **System** > **Objects** > **IP Addresses** > **IP Address Objects/IP Address Object Groups**.

  Note: IPv4 and IPv6 IP addresses cannot be set for the same policy except the IP-MAC binding policies.

- Service object or object group, choose **System** > **Objects** > **Services** > **Service Objects/ Service Object Groups**.

8.2.1 Configure IP-MAC Binding

IP-MAC binding configuration includes:

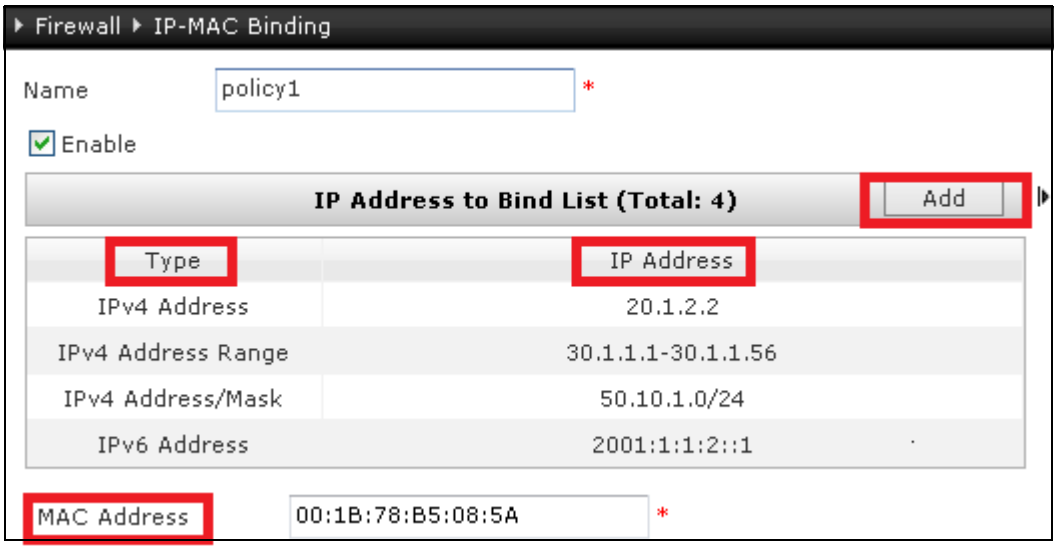
- 8.2.1.1 Create IP-MAC Binding Policy
- 8.2.1.2 Set Default Action

8.2.1.1 Create IP-MAC Binding Policy

Choose **Firewall** > **IP-MAC Binding** > **New**.

1. Set policy name.
2. Add the source IP address from which packets are sent.

3. Set the source MAC address from which packets are sent.

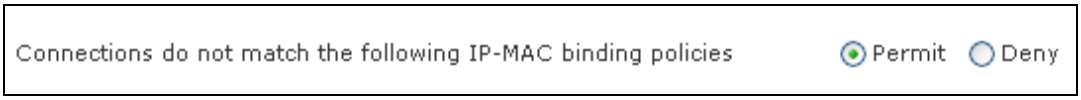


Note: An IP-MAC binding policy includes only one MAC address and multiple IP addresses or address ranges.

8.2.1.2 Set Default Action

When a packet matches none of the IP-MAC binding policies, it will be processed according to the default action.

Choose **Firewall** > **IP-MAC Binding** and click **Permit** or **Deny**:



Caution: Before you set the action as Deny, make sure you have configured an IP-MAC binding policy that binds the IP address and the MAC address of the administrative host and the IP-MAC binding policy is enabled. Otherwise, it will cause network connection failure.

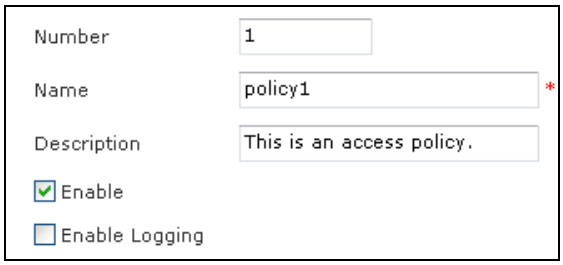
Table 148 IP-MAC Binding Policy Commands

policy ip-mac *policy_name*	Adds an IP-MAC binding policy.
policy default ip-mac {**permit** | **deny**}	Modifies the default action.
unset policy ip-mac [*policy_name*]	Deletes IP-MAC binding policies.
show policy ip-mac	Displays IP-MAC binding policy information.

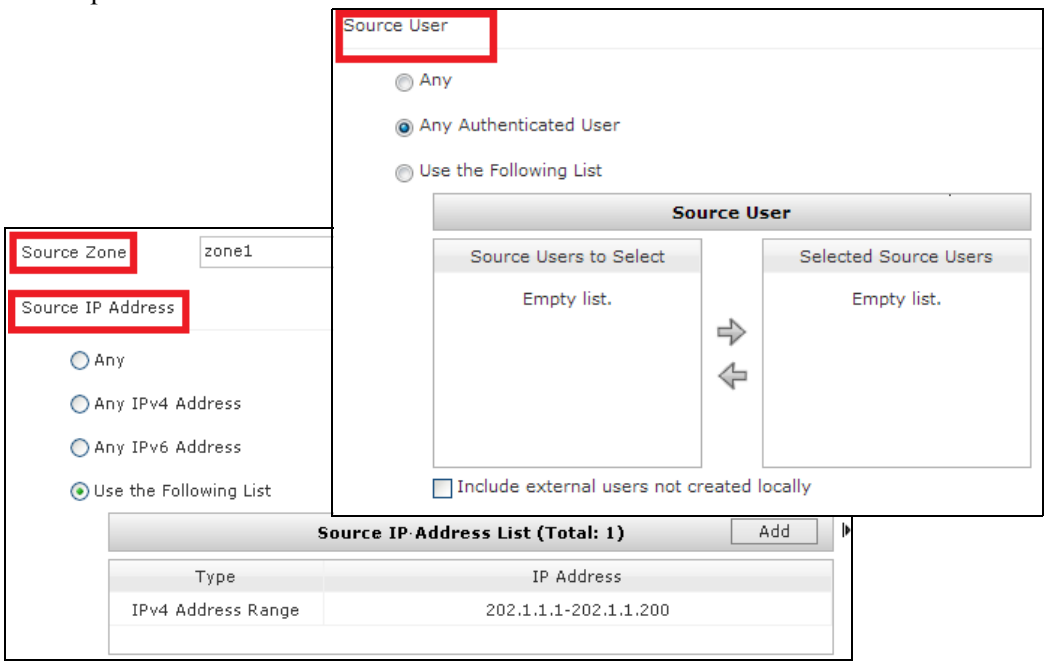
8.2.2 Create Access Policy

Choose **Firewall** > **Access Policies** > **New**.

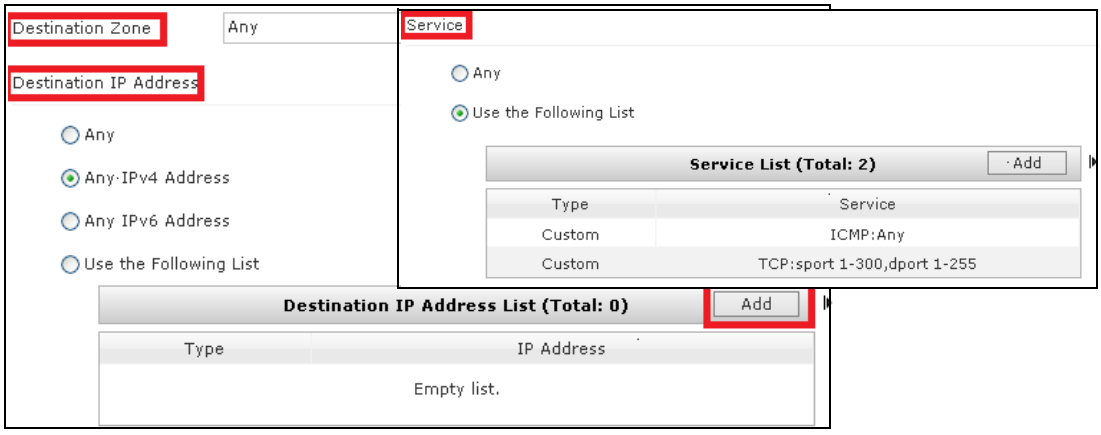
1. Set basic elements.



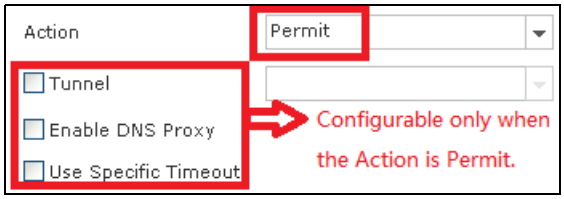
2. Set packet sources.



3. Set packet destinations and services that packets use.

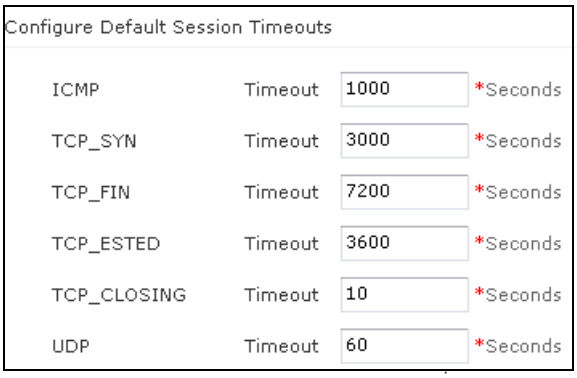


4. Set actions for handling packets matching the policy.



- Check **Tunnel** and choose a tunnel or tunnel group to which FGX forwards packets.
- Check **Enable DNS Proxy** to enable the transparent DNS proxy function.
- Check **Use Specific Timeout** to set timeout values for different states of TCP sessions and simulated sessions of ICMP and UDP.

Note: Choose **Firewall** > **Default Policy Settings**. Set default values for timing out sessions.



5. Set schedules during which the policy takes effect.

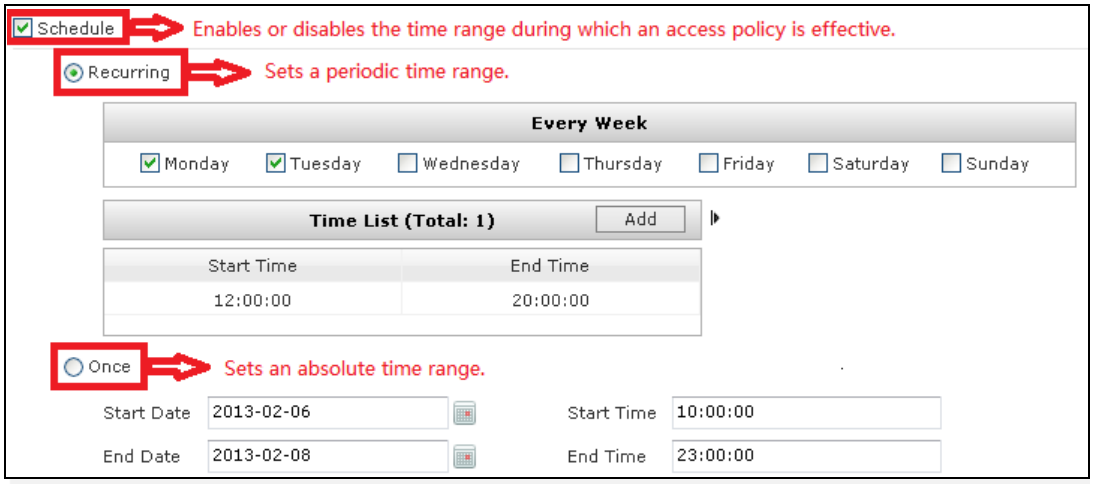


Table 149 Acess Policy Commands

policy access *policy_name*	Adds an access policy.
policy access *policy_name* **description**	Sets a comment.
policy access *policy_name* **log** {**on** | **off**}	Enables or disables the logging function.
policy access *policy_name* **number** *pri*	Modifies policy priority.

Table 149 Acess Policy Commands (*continued*)

policy access *policy_name* **protocol**	Add services.
policy access *policy_name* **schedule**	Sets a schedule.
policy access *policy_name* **sourceip**	Adds source IP addresses.
policy access *policy_name* **desip**	Adds destination IP addresses.
policy access *policy_name* **timeout**	Sets session timeouts.
policy access *policy_name* **tunnel**	Sets a VPN tunnel.
policy access *policy_name* [**user** *user_list*]	Adds source users.
unset policy access [*policy_name*]	Deletes access policies.
show policy access	Displays access policy information.
timeout	Sets default timeout values.
timeout reset	Sets the all timeouts to their default settings.

8.2.3 Configure Default Access Policies

Choose **Firewall** > **Default Policy Settings**. Set an action for default inter- and intra-zone policies.

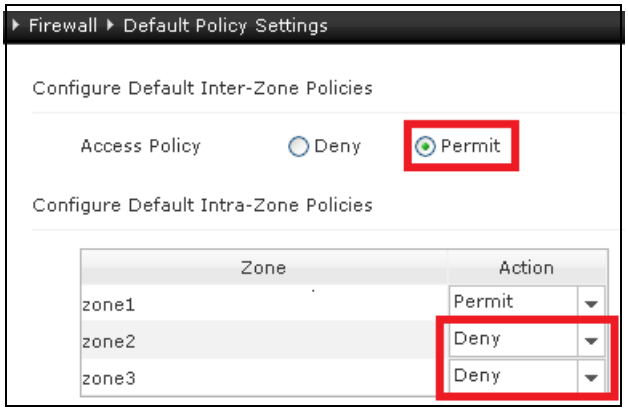


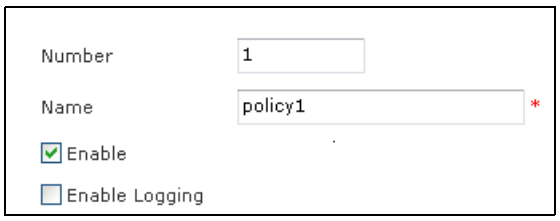
Table 150 Default Access Policy Commands

policy default inter-zone access {**permit** | **deny**}	Sets an action for the default inter-zone access policy
policy default intra-zone *zone_name* {**permit** | **deny**}	Sets an action for the default intra-zone policy.
show policy default	Displays default policy information.

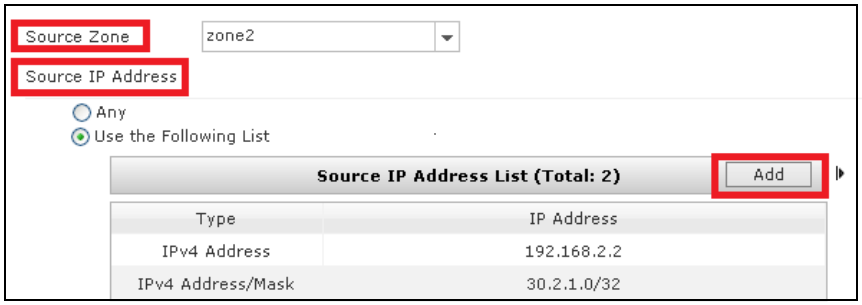
8.2.4 Create Multicast Policy

Choose **Firewall** > **Multicast Policies** > **New**.

1. Set basic elements.



2. Set packet sources.



3. Set packet destination multicast group IP's and zones in which multicasting is allowed.

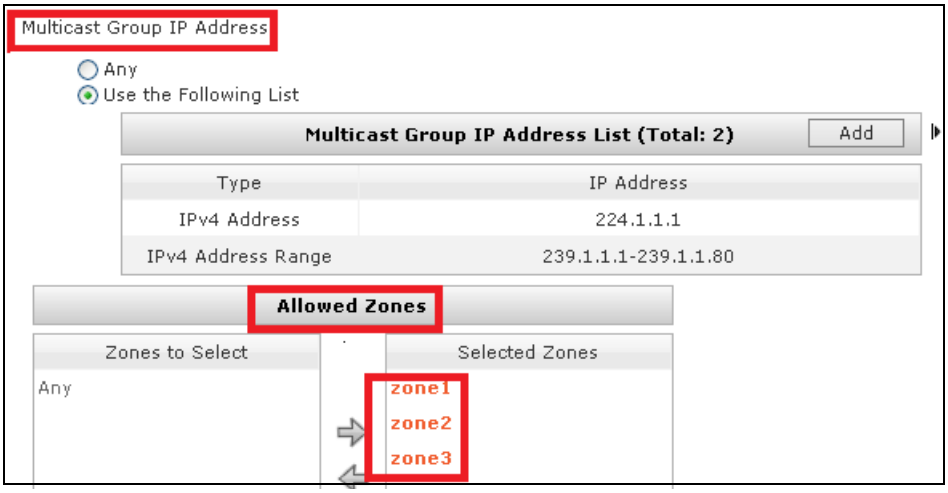


Table 151 Multicast Policy Commands

policy multicast *policy_name*	Adds a multicast policy.
policy multicast *policy_name* **groupip**	Adds multicast group IP addresses.
policy multicast *policy_name* **log {on | off}**	Enables or disables the logging function.
policy multicast *policy_name* **sourceip**	Adds source IP addresses.
policy multicast *policy_name* **allowedzone**	Adds destination zones.
policy multicast *policy_name* **{enable | disable}**	Enables or disables a multicast policy.
policy multicast *policy_name* **number** *pri*	Changes policy priority.

Table 151 Multicast Policy Commands (*continued*)

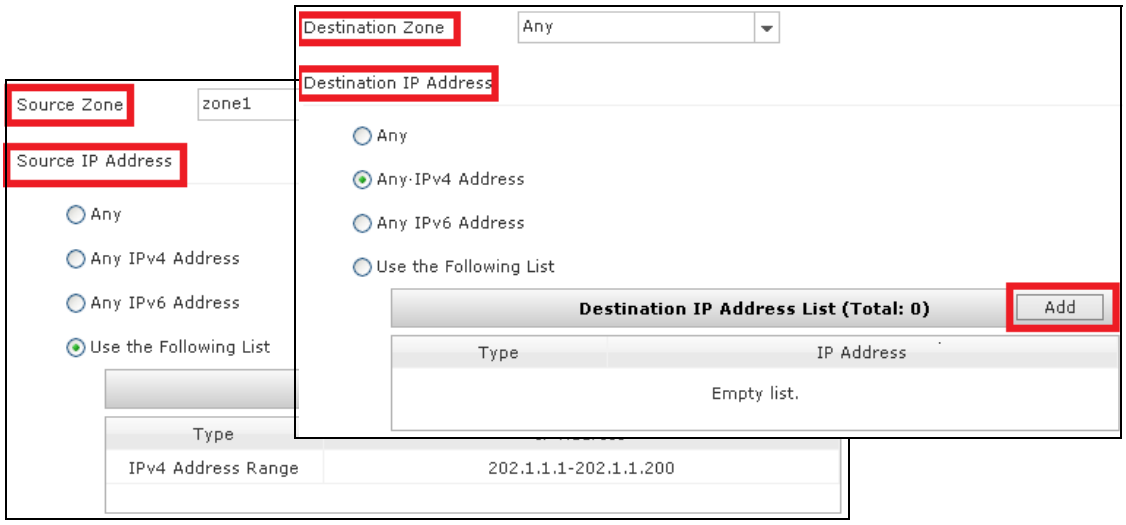
show policy multicast [*policy_name*]	Displays policy information.
unset policy multicast [*policy_name*]	Deletes policies.

8.2.5 Create Session Policy

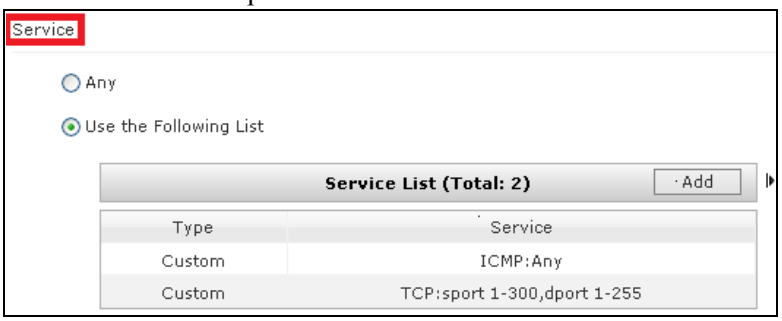
Choose **Firewall** > **Session Policies** > **New**.

1. Set basic elements.

2. Set packet sources and destinations.



3. Set services that packets use.



4. Set a session policy type, maximum number of connections allowed, and actions.

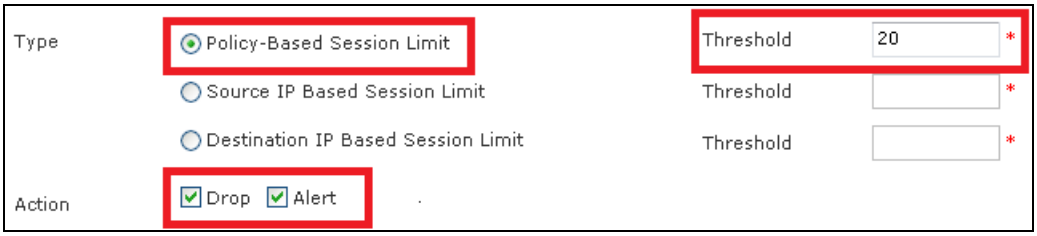


Table 152 Session Policy Commands

policy session *policy_name*	Adds a session policy.
policy session *policy_name* **sourceip**	Adds source IP addresses for session policies.
policy session *policy_name* **desip**	Adds destination IP addresses for session policies.
policy session *policy_name* {**enable** | **disable**}	Enables or disables session policies.
policy session *policy_name* **protocol**	Adds services for session policies.
policy session *policy_name* **type**	Sets the session policy type and threshold value.
show policy session [*policy_name*]	Displays session policy information.
unset policy session [*policy_name*]	Deletes session policies.

8.3. Examples

This section gives the following examples about how to configure policies:

- Example 1. Create IP-MAC Binding Policy
- Example 2. Create Access Policy
- Example 3. Apply Multicast Policy Among Zones
- Example 4. Create Destination IP-Based Session Policy

For each scenario, you must do the following in advance:

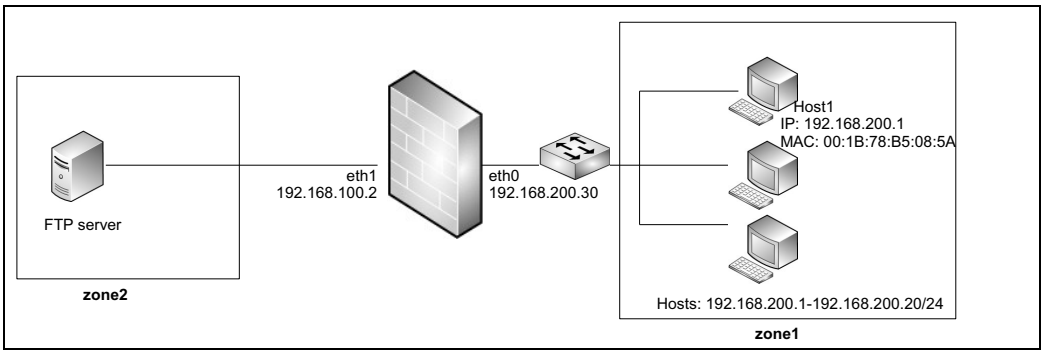
- Choose **Network** > **Interfaces** to configure FGX interfaces. See 4.2.3 Example: Ethernet Interface.
- If zones are needed, choose **Network** > **Zones** > **New** to create them. See 4.12.3 Example: Zone Application.
- If users are needed, choose **System** > **Authentication** > **Users** > **New** to create them. See 3.14 Users.
- If objects and object groups s are needed, choose **System** > **Objects** to create them.
- Choose **Firewall** > **Default Policy Settings** to configure the default inter-zone policy action as Permit or choose **Firewall** > **Access Policies** to create an access policy permitting any traffic. See 8.2.2 Create Access Policy.

Example 1. Create IP-MAC Binding Policy

In this example, an FTP server is deployed in zone2. To prevent the FTP server from being attacked by IP address spoofing, create an IP-MAC binding policy, which:

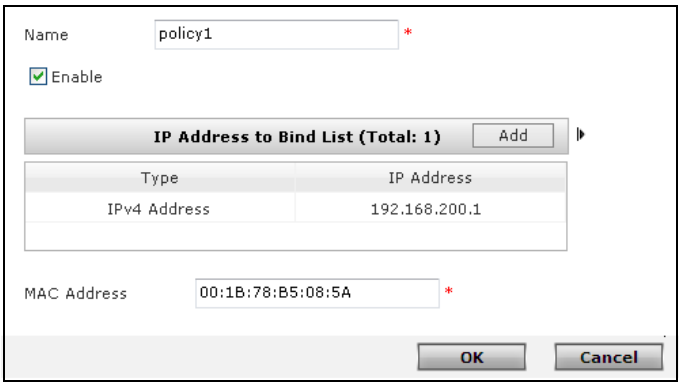
- Binds the IP address 192.168.200.1 with the MAC address 00:1B:78:B5:08:5A of Host1 to allow only the host with this MAC in zone1 to access the FTP server.
- Blocks any host when it tries to access the FTP server and neither the IP address nor the MAC address of the host matches any IP-MAC binding policies.

Figure 33 Network Topology

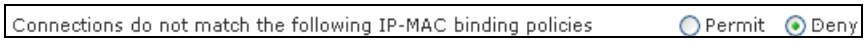


WebUI

1. Choose **Firewall** > **IP-MAC Binding** > **New** to create the following policy:

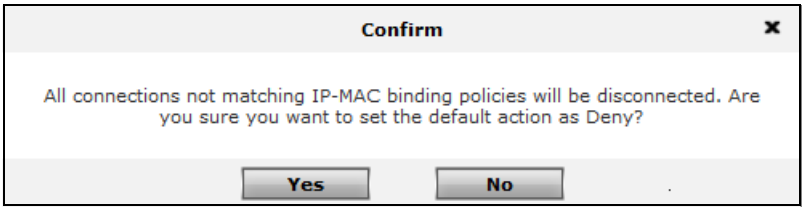


2. Click **OK**.
3. Click **Deny** to set the default action.



Caution: Make sure you have configured an IP-MAC binding policy that binds the IP address and the MAC address of the administrative host and the IP-MAC binding policy is enabled. Otherwise, it will cause network connection failure.

4. Click **Yes** in the following dialog box.



5. Click  .

CLI

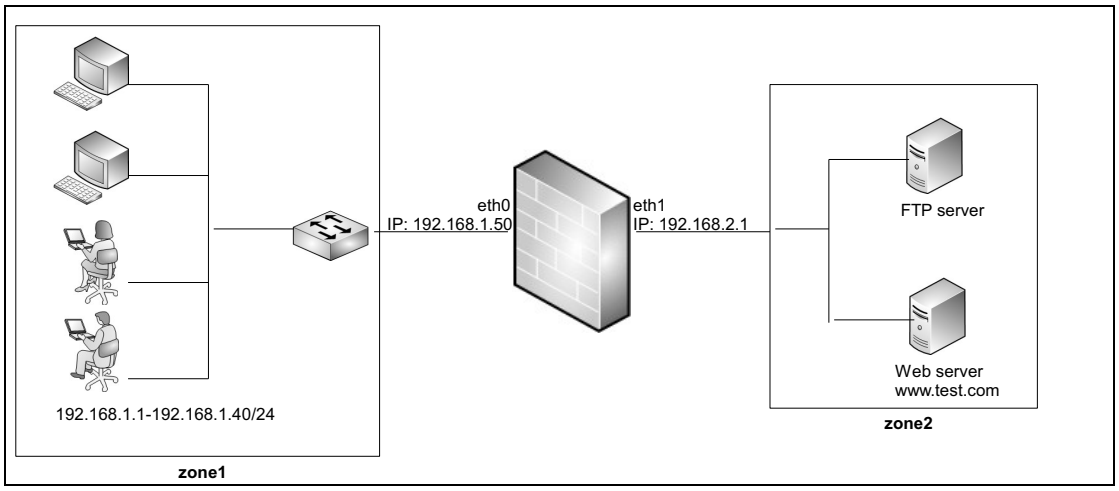
```
FGX@root> configure mode override
FGX@root-system] policy ip-mac policy1 192.168.200.1 00:1B:78:B5:08:5A enable
FGX@root-system] policy default ip-mac deny
FGX@root-system] exit
FGX@root> save config
```

Example 2. Create Access Policy

In this example, you deploy a Web server (with a domain name www.sina.com) and an FTP server in zone2. You require FGX to control access from zone1 to zone2 as follows:

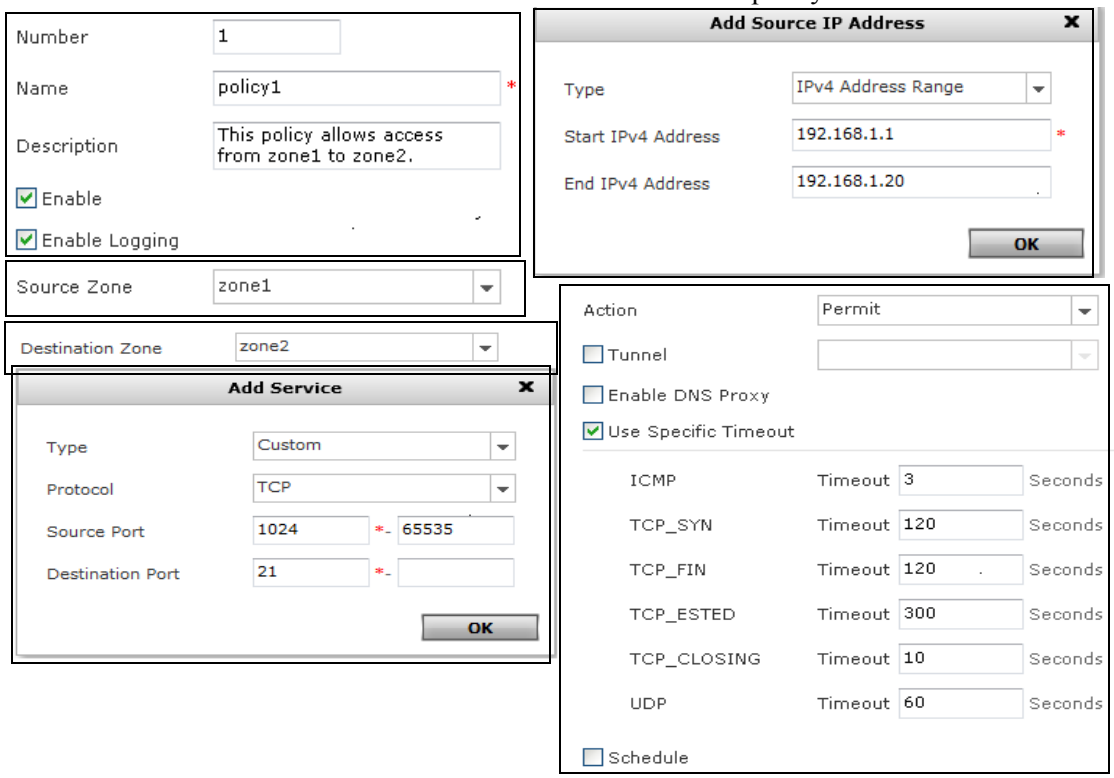
- Permit host in 192.168.1.1-192.168.1.20 in zone1 to access the FTP server in zone2 and log access. To prevent the number of FTP server connections from growing too large, an established FTP session will be terminated if no operation is performed within 300 seconds.
- Block user1 and user2 in 192.168.1.21-192.168.1.40 in zone1 and all external users from accessing the Web server in zone2 during work hours (08:30:00-17:30:00, Monday through Friday).

Figure 34 Network Topology



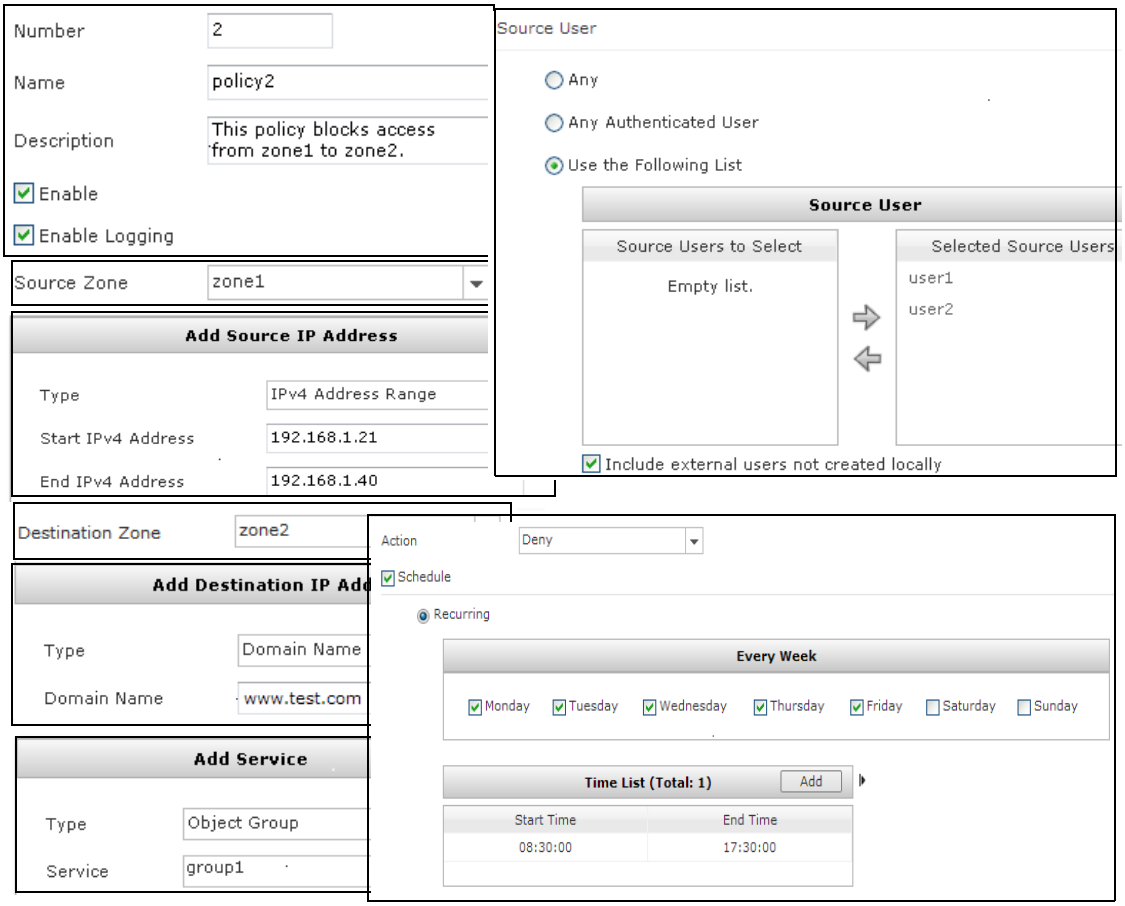
WebUI

1. Choose **Firewall** > **Access Policies** and click **New** to create policy1:



2. Click **OK**.
3. Click  .

4. Click **New** to create policy2.



The service group group1 comprises service objects DNS, HTTP, and HTTPS:

5. Click **OK**.
6. Click  .

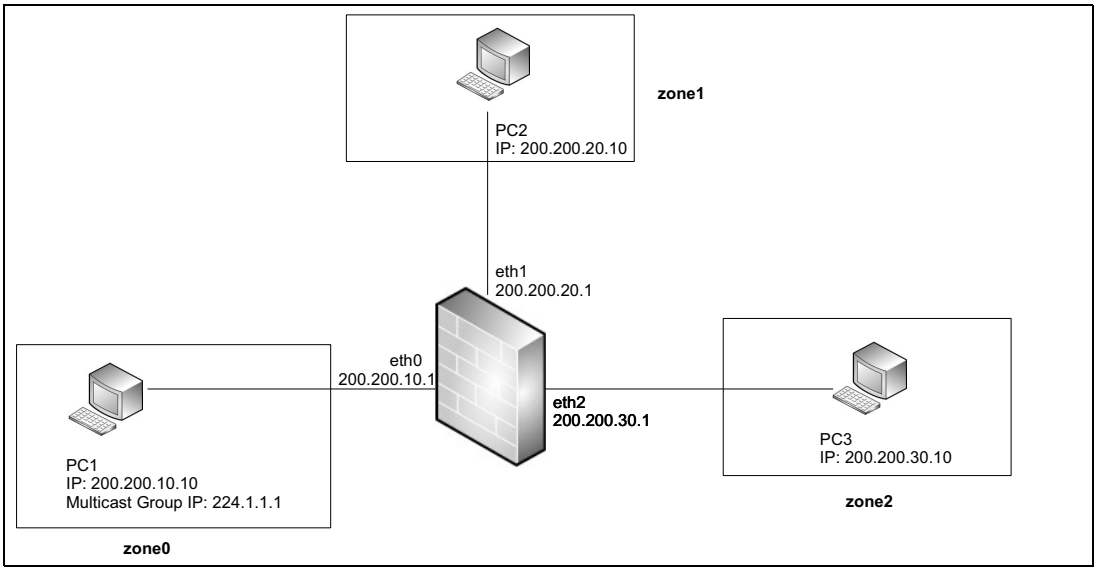
CLI

```
FGX@root> configure mode override
FGX@root-system] policy access policy1 zone1 192.168.1.1-192.168.1.20 zone2 any tcp 1024-65535 21 any permit enable 1
FGX@root-system] policy access policy1 timeout tcp ested 300
FGX@root-system] policy access policy1 log on
FGX@root-system] policy access policy2 zone1 192.168.1.21-192.168.1.40 zone2 DomainName www.sina.com protocol-group group1 user user1,user2 include-external-users deny enable 2
FGX@root-system] policy access policy2 schedule start-week 1 end-week 5 08:30:00-17:30:00
FGX@root-system] exit
FGX@root> save config
```

Example 3. Apply Multicast Policy Among Zones

In this example, PC1 serves as a multicast source, and multicast flow is transmitted through the multicast group IP address 224.1.1.1 to PC1 and PC2. Figure 35 shows the network topology. You create a multicast policy which allows only PC2 to receive multicast flow from PC1.

Figure 35 Network Topology



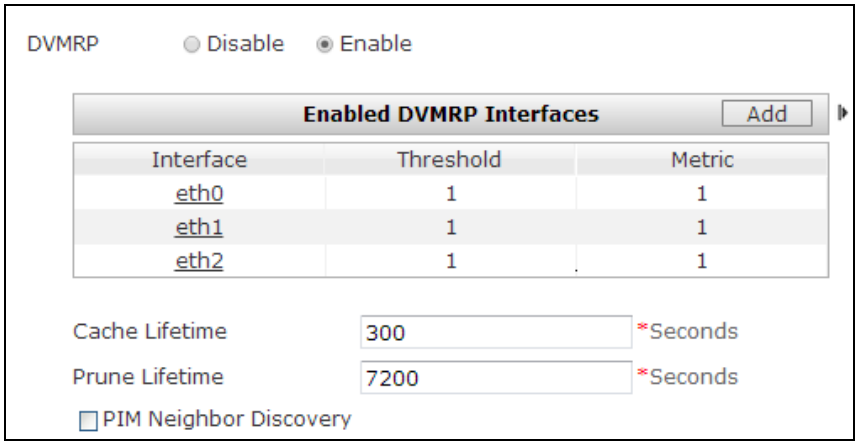
Configuration steps are as follows:

- 3.1 Enable DVMRP
- 3.2 Create Static Multicast Route
- 3.3 Create Multicast Policy

3.1 Enable DVMRP

WebUI

1. Choose **Network** > **Multicast** > **DVMRP** and configure DVMRP as follows:



2. Click **OK**.
3. Click  .

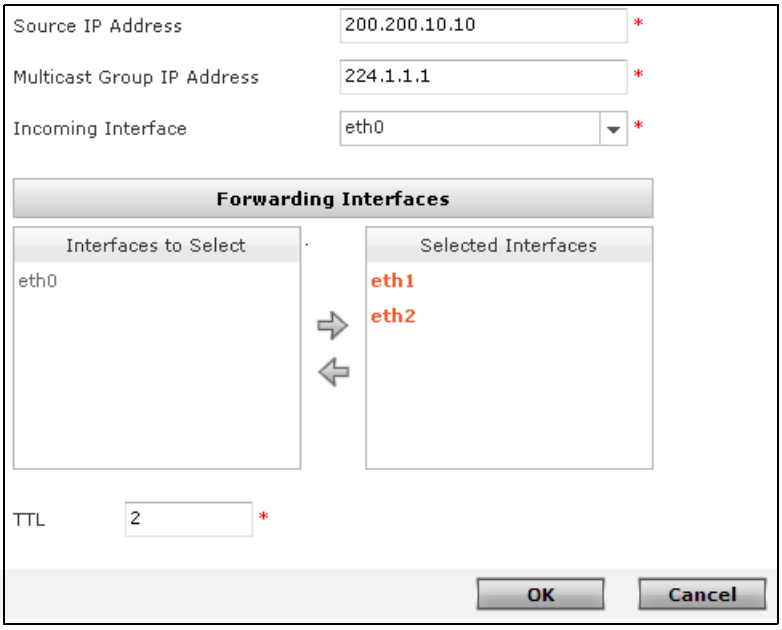
CLI

```
FGX@root>configure mode
FGX@root-system]dvmrp enable
FGX@root-system]interface ethernet 0
FGX@root-system-if-eth0]dvmrp on
FGX@root-system-if-eth0]dvmrp metric 1
FGX@root-system-if-eth0]dvmrp threshold 1
FGX@root-system-if-eth0]exit
FGX@root-system]interface ethernet 1
FGX@root-system-if-eth1]dvmrp on
FGX@root-system-if-eth1]dvmrp metric 1
FGX@root-system-if-eth1]dvmrp threshold 1
FGX@root-system-if-eth1]exit
FGX@root-system]interface ethernet 2
FGX@root-system-if-eth2]dvmrp on
FGX@root-system-if-eth2]dvmrp metric 1
FGX@root-system-if-eth2]dvmrp threshold 1
FGX@root-system-if-eth2]exit
FGX@root-system]dvmrp cache-lifetime 300
FGX@root-system]dvmrp prune-lifetime 7200
FGX@root-system]dvmrp pim disable
FGX@root-system] exit
FGX@root> save config
```

3.2 Create Static Multicast Route

WebUI

1. Click **Multicast Routing** on the **DVMRP** page or choose **Network** > **Routing** > **Multicast**. Click **New** to create the following static multicast route:



2. Click **OK**.
3. Click  .

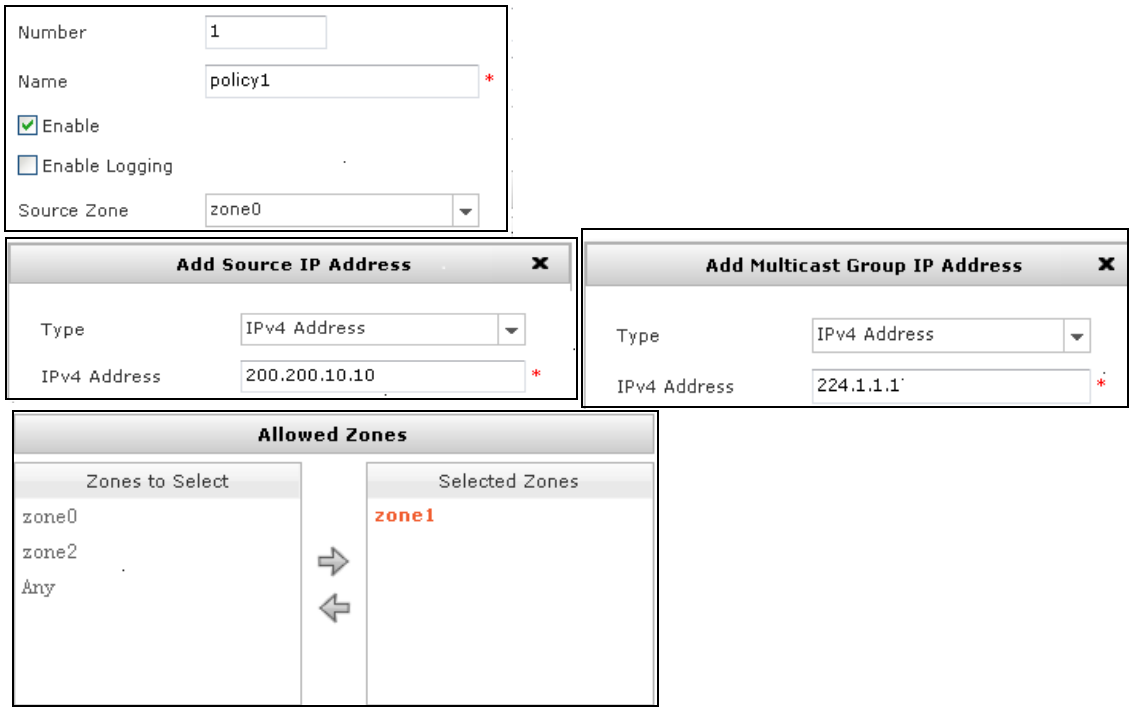
CLI

```
FGX@root>configure mode
FGX@root-system]dvmrp route 200.200.10.10 224.1.1.1 input eth0
forwarding eth1,eth2 threshold 2
FGX@root-system]exit
FGX@root>save config
```

3.3 Create Multicast Policy

WebUI

1. Choose **Firewall** > **Multicast Policies** and click **New** to create policy1 which allows PC2 to receive multicast flow from PC1:



2. Click **OK**.
3. Click .

CLI

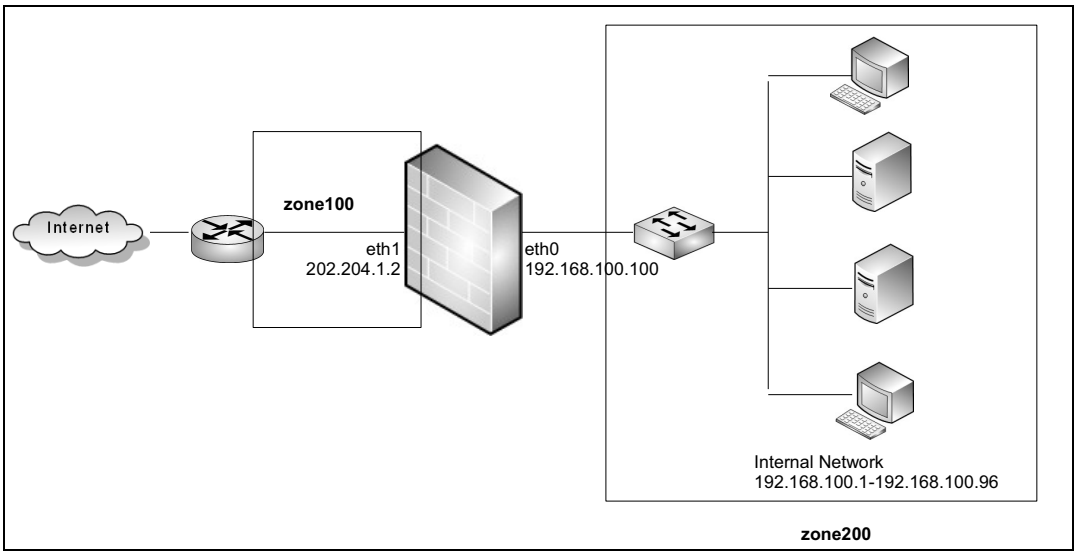
```
FGX@root> configure mode override
FGX@root-system] policy multicast policy1 zone0 200.200.10.10
224.1.1.1 zone1 enable 1
FGX@root-system] end
FGX@root> save config
```

Example 4. Create Destination IP-Based Session Policy

In this example, protected servers of a company are flooded by excessive and useless TCP connections. Figure 36 shows the network topology. To prevent DoS attacks, you require FGX drops packets satisfying the following conditions and sends alerts:

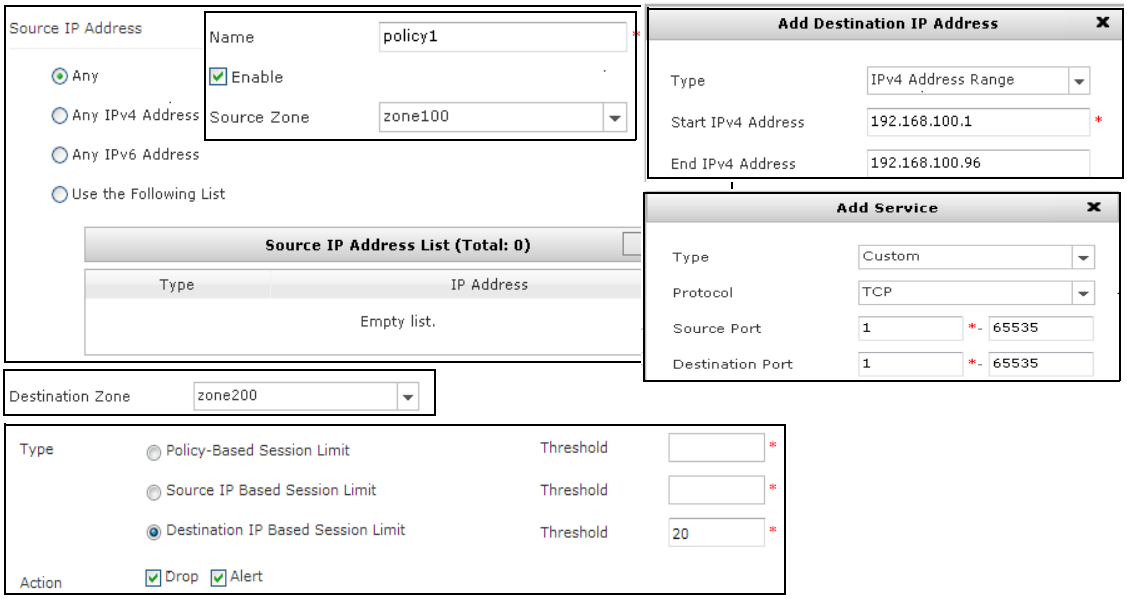
- The packets are from zone100.
- The maximum number of concurrent sessions of the packets to a destination IP address in 192.168.100.1-192.168.1.96 in zone200 exceeds 20.
- The service used by the packets is TCP with port numbers in 1-65535.

Figure 36 Network Topology



WebUI

1. Choose **Firewall** > **Session Policies** and click **New** to create the following session policy:



2. Click **OK**.
3. Click  .

CLI

```
FGX@root> configure mode override
FGX@root-system] policy session policy1 zone100 zone200 any
192.168.100.1-192.168.100.96 tcp 1-65535 1-65535 20 type dstip
enable drop alert
FGX@root-system] end
FGX@root> save config
```

8.4. Parameter Reference

This section describes parameters used when configuring policies:

- 8.4.1 IP-MAC Binding Policy Parameters
- 8.4.2 Access Policy Parameters
- 8.4.3 Multicast Policy Parameters
- 8.4.4 Session Policy Parameters

8.4.1 IP-MAC Binding Policy Parameters

Table 153 Parameters of IP-MAC Binding Policies

Name	Description
Name	IP-MAC binding policy name. 1-63 UTF-8 characters. It cannot contain ? , ” ' \ < > & # or spaces. IP-MAC binding policy names must be unique within a virtual system.
Enable	Used to enable or disable an IP-MAC policy. An IP-MAC policy is enabled by default.
IP Address to Bind List	Used to set the source IP address or addresses from which packets are sent. An IP address can be one of the following: • IP address object • Object group • IPv4 address • IPv4 address range • IPv4 address/mask length • IPv6 address • IPv6 address range • IPv6 address/prefix length IP Address Object is chosen by default. You can add a maximum of 4,096 IP addresses to IP Address to Bind List. All entries must be unique.
MAC Address	The source MAC address from which packets are sent. You can configure only one MAC address for an IP-MAC binding policy, and IPv4 and IPv6 addresses in IP Address to Bind List are bound to this MAC address.

8.4.2 Access Policy Parameters

Basic elements include number, name, description, and state. The conditions for matching access policies include source zone, source IP address, source user, destination zone, destination IP address, service, and schedule. Action elements include permitting/denying, logging, VPN tunneling, and transparent DNS proxy. Basic elements also include specific timeout..

Table 154 Parameters of Access Policies

Parameter	Description
Number	Access policy priority. Integer in 1-80,000. The lower the number, the higher the priority. If you do not specify a number for a new policy, the policy number will be the highest automatically. If the number of an existing policy is specified for a new policy, the number of the existing policy will be increased by 1.
Name	Access policy name. 1-63 UTF-8 characters. It cannot contain ? , ” ' \ < > & # or spaces. Access policy names must be unique within a virtual system.
Description	Access policy description. 0-255 UTF-8 characters. It cannot contain ? ,” ' \ < > & or spaces.
Enable	Used to enable or disable an access policy. An access policy is enabled by default.
Enable Logging	Used to set whether to generate logs about packets that match an access policy. Disabled by default.
Source Zone	The zone from which packets are sent. It is Any by default, meaning any zones.
Source IP Address	The IP address from which packets are sent. A source IP address can be one of the following types: • **Any—**includes all IPv4 and IPv6 addresses. Any is chosen by default. • **Any IPv4 Address—**includes all IPv4 addresses. • **Any IPv6 Address—**includes all IPv6 addresses. • **Use the Following List—**includes IP address objects, object groups, IPv4 addresses, IPv4 address ranges, IPv4 addresses and mask lengths, IPv6 addresses, IPv6 address ranges, and IPv6 addresses and prefix lengths. IP Address Object is chosen by default. You can configure up to 4,096 source IP address entries per policy. All entries must be unique.
Source User	The user from whom packets are sent. The user can be one of the following types: • **Any—**includes all users, authenticated or unauthenticated. Any is chosen by default. • **Any Authenticated User**—includes all users who have passed authentication. • **Use the Following List—**includes users you choose. You can also choose whether or not to include external users not created on FGX. You can choose up to 4,096 source users per policy. All users must be unique. For more information about users, see 3.14 Users.
Destination Zone	The zone to which packets are sent. It is Any by default, meaning any zones.

Table 154 Parameters of Access Policies (*continued*)

Parameter	Description
Destination IP Address	The IP address to which packets are sent. A destination IP address can be one of the following types: • **Any—**includes all IPv4 and IPv6 addresses. Any is chosen by default. • **Any IPv4 Address—**includes all IPv4 addresses. • **Any IPv6 Address—**includes all IPv6 addresses. • **Use the Following List—**includes IP address objects, object groups, IPv4 addresses, IPv4 address ranges, IPv4 addresses and mask lengths, IPv6 addresses, IPv6 address ranges, IPv6 addresses and prefix lengths, and domain names. IP Address Object is chosen by default. The length range of a domain name is 2-255 characters. You can configure up to 4,096 destination IP address entries per policy. All entries must be unique.
Service	Type of transport layer service used by packets. A service type can be either of the following: • **Any—**includes all types of protocols. Any is chosen by default. • **Use the Following List—**includes service objects, service object groups, and custom protocols. Object AOL is chosen by default. Custom protocols include ICMP, ICMPv6, TCP, UDP, and other protocols. When you set ICMP protocol, you can choose any of the following types: ECHO_and_ECHOREPLY, INFO_REQUEST_and_INFO_REPLY, TIMESTAMP_and_TIMESTAMPREPLY, ADDRESS_and_ADDRESSREPLY, ROUTER_ADVERTISEMENT, ROUTER_SOLICITATION, DEST_UNREACH, SOURCE_QUENCH, REDIRECT, TIME_EXCEEDED, PARAMETERPROB, and Any (representing any ICMP types). When you set ICMPv6 protocol, you can choose any of the following types: DST_UNREACH, PACKET_TOO_BIG, TIME_EXCEEDED, PARAM_RPROB, ECHO_and_ECHOREPLY, and Any (representing any ICMPv6 types). The source and destination port number ranges of TCP or UDP are 1-65535. Other protocol number range is 1-255. You can configure up to 32 service entries (including a maximum of 4,096 port numbers in total) to the service list. All entries must be unique.
Action	Indicates how FGX processes the packets that match access policies: • **Permit—**FGX forwards packets and updates the session states of the packets. Permit is the default action. • **Deny—**FGX drops packets and cancels the sessions of the packets.
Tunnel	When the action is Permit, you can enable or disable the VPN tunneling function. Disabled by default. When enabled, you can choose a VPN tunnel or tunnel group through which packets are forwarded.
Enable DNS Proxy	When the action is Permit, you can enable or disable transparent DNS proxy. Disabled by default. For more information about transparent proxy, see 4.14 DNS Proxy.

Table 154 Parameters of Access Policies (*continued*)

Parameter	Description
Use Specific Timeout	When the action is Permit, you can enable or disable specific timeouts. Disabled by default. When enabled, you can set timeout values for different states of TCP sessions and simulated sessions of ICMP and UDP. The timeout value range is 1-99,999,999 seconds. When disabled, FGX will use the default state timeouts provided by the system.

Schedule	Used to enable or disable the time range during which an access policy is effective. Disabled by default.
	If you do not set a schedule for an enabled access policy, the policy is effective at all times.
	• **Recurring—**used to set a periodic time range. During a recurring time range, an access policy is effective on specified days each week.
	  • **Every Week—**you can choose the days from Sunday through Monday.
	  • **Time List—**you can enter a daily start time and end time. The valid time format is HH:MM:SS; range is 00:00:00-23:59:59. You can add up to eight time ranges to the time list. Time ranges can overlap but cannot be the same.
	• **Once—**used to set an absolute time range. An access policy is effective only during the set period of time. The valid date format is YYYY-MM-DD; range is 1970-01-01 through 2037-12-31. You are required to set one start date and time and one end date and time.

FGX filters packets of TCP, UDP, ICMP, and other protocols. The filter policies are called access policies. You can create zones and assign interfaces with the same requirements to the same zone and then apply access policies to different zones. Thus, you do not need to configure a policy for each interface. For more information about zones, see 4.12 Zones.

FGX supports stateful inspection based on sessions rather than on packets. For the connection-oriented TCP protocol, a session is a TCP connection. Each packet in the same TCP session has the same session information. For connectionless protocols, such as UDP, ICMP, and other protocols, FGX processes packets by maintaining simulated sessions like those of the TCP protocol. Each simulated session starts with the first request packet. When a session is idle for a period of time longer than the predefined timeout, the session is terminated. Stateful inspection packet filtering is performed on sessions rather than on packets, which conserves system resources.

The following table shows a comparison of session information among the protocols mentioned above.

Table 155 Comparison of Session Information

Type & Information	TCP & UDP	ICMP	Other
Source IP	The source IP address of a packet		
Destination IP	The destination IP address of a packet		
Source Port	The source port of a packet	The ICMP type and code value	0
Destination Port	The destination port of a packet	echo.id in ICMP implementation	0
Service	The protocol type of a packet		

When a new session request is permitted by an access policy, FGX adds the session information to the session table. It also adds information such as the translated IP address, zone, session state, and timeout. When the session is terminated or times out, all its information will be removed from the session table.

To clearly describe the events that occur when initiating and terminating sessions and transmitting data, the TCP protocol defines several states and dictates that a TCP session must remain in the same state until another event occurs. FGX checks the validity of the state for each TCP packet. For example, a session in the state of transmitting data has been recorded in a session table (session established). If a packet with the same session information as those in the existing session requests to establish a new session, FGX will consider this packet as invalid and drop it. For UDP, ICMP, and other protocols, the stateful inspection of simulated sessions is similar to that of TCP sessions. Sessions of those protocols are much easier to process since they have only one state.

8.4.3 Multicast Policy Parameters

Table 156 Parameters of Multicast Policies

Parameter	Description
Number	Indicates the priority of a multicast policy. Integer in 1-80,000. The lower the number, the higher the priority. If you do not specify a number for a new policy, the policy number will be the highest automatically. If the number of an existing policy is specified for a new policy, the number of the existing policy will be increased by 1.
Name	Multicast policy name. 1-63 UTF-8 characters. It cannot contain ? , ” ' \ < > & # or spaces. Multicast policy names must be unique within a virtual system.
Enable	Used to enable or disable a multicast policy. A multicast policy is enabled by default.
Enable Logging	Used to set whether to generate logs about packets that match a multicast policy. Disabled by default.
Source Zone	The zone from which FGX receives multicast packets. It is Any by default, meaning any zones.
Source IP Address	The IP address from which multicast packets are sent. A source IP address can be one of the following types: • **Any—**includes all IPv4 addresses. Any is chosen by default. • **Use the Following List—**includes IP address objects, object groups, IPv4 addresses, IPv4 address ranges, and IPv4 addresses and mask lengths. IP Address Object is chosen by default. You can configure up to 4,096 source IP address entries per policy. All entries must be unique.

Table 156 Parameters of Multicast Policies (*continued*)

Parameter	Description
Multicast Group IP Address	The IP address of the destination multicast group to which multicast packets are forwarded. A multicast group IP address can be one of the following types: • **Any—**includes all IPv4 addresses. Any is chosen by default. • **Use the Following List—**includes IP address objects, object groups, IPv4 addresses, IPv4 address ranges, and IPv4 addresses and mask lengths. IP Address Object is chosen by default. You can configure up to 4,096 multicast group IP address entries per policy. All entries must be unique.
Allowed Zones	The zones through which multicast packets are sent out. It is Any by default, meaning any zones.

8.4.4 Session Policy Parameters

Table 157 Parameters of Session Policies

Parameter	Description
Name	Session policy name. 1-63 UTF-8 characters. It cannot contain ? , ” ' \ < > & # or spaces. Session policy names must be unique within a virtual system.
Enable	Used to enable or disable a session policy. A session policy is enabled by default.
Source Zone	The zone from which packets are sent. It is Any by default, meaning any zones.
Destination Zone	The zone to which packets are sent. It is Any by default, meaning any zones.
Source IP Address	The IP address from which packets are sent. A source IP address can be one of the following types: • **Any—**includes all IPv4 and IPv6 addresses. Any is chosen by default. • **Any IPv4 Address—**includes all IPv4 addresses. • **Any IPv6 Address—**includes all IPv6 addresses. • **Use the Following List—**includes IP address objects, object groups, IPv4 addresses, IPv4 address ranges, IPv4 addresses and mask lengths, IPv6 addresses, IPv6 address ranges, and IPv6 addresses and prefix lengths. IP Address Object is chosen by default. You can configure up to 4,096 source IP address entries per policy. All entries must be unique.

Table 157 Parameters of Session Policies (*continued*)

Parameter	Description
Destination IP Address	The IP address to which packets are sent. A destination IP address can be one of the following types: • **Any—**includes all IPv4 and IPv6 addresses. Any is chosen by default. • **Any IPv4 Address—**includes all IPv4 addresses. Any is chosen by default. • **Any IPv6 Address—**includes all IPv6 addresses. • **Use the Following List—**includes IP address objects, object groups, IPv4 addresses, IPv4 address ranges, IPv4 addresses and mask lengths, IPv6 addresses, IPv6 address ranges, and IPv6 addresses and prefix lengths. IP Address Object is chosen by default. You can configure up to 4,096 destination IP address entries per policy. All entries must be unique.
Services	Type of transport layer service used by packets. A service type can be either of the following: • **Any—**includes all types of protocols. Any is chosen by default. • **Use the Following List—**includes objects, object groups, and custom protocols. Object AOL is chosen by default. Custom protocols include ICMP, ICMPv6 TCP, UDP, and other protocols. When you set ICMP protocol, you can choose any of the following types: ECHO_and_ECHOREPLY, INFO_REQUEST_and_INFO_REPLY, TIMESTAMP_and_TIMESTAMPREPLY, ADDRESS_and_ADDRESSREPLY, ROUTER_ADVERTISEMENT, ROUTER_SOLICITATION, DEST_UNREACH, SOURCE_QUENCH, REDIRECT, TIME_EXCEEDED, PARAMETERPROB, and Any (representing any ICMP types). When you set ICMPv6 protocol, you can choose any of the following types: DST_UNREACH, PACKET_TOO_BIG, TIME_EXCEEDED, PARAM_RPROB, ECHO_and_ECHOREPLY, and Any (representing any ICMPv6 types). The destination port number range of TCP or UDP is 1-65535. Other protocol number range is 1-255. You can configure up to 32 service entries (including a maximum of 4,096 port numbers in total) to the service list. All entries must be unique.
Type	Types of session policies: • Policy-Based Session Limit • Source IP Based Session Limit • Destination IP Based Session Limit Policy-Based Session Limit is chosen by default.
Threshold	The maximum number of concurrent sessions allowed by a session policy. The value range is 1-99,999,999.
Action	Indicates how FGX will process the packets matching a certain session policy: • **Alert—**FGX generates alert. • **Drop—**FGX drops attack packets. The action is Alert + Drop by default.

9 Attack Defense

This chapter describes zone-level attack detection and defense mechanisms.

- 9.1. Basic Concepts. Describes attack defense concepts and fundamentals.
- 9.2. Attack Types / Tactics / Countermeasures. Describes common attack types and the corresponding measures taken in FGX.
- 9.3. Basic Configuration Steps. Describes basic configuration steps and the UI dialogs.
- 9.4. Parameter Reference. Describes in detail all parameters.

9.1. Basic Concepts

This section describes:

- 9.1.1. Attack Goals
- 9.1.2. Attack Types
- 9.1.3. Countermeasures

9.1.1. Attack Goals

Attack goals include:

- Access secure data
- Access information about the host system
- Damage the target system

9.1.2. Attack Types

Attacks can be generalized as:

- DoS attack
- Reconnaissance attack
- TCP evasion control
- IP option check
- ICMP attack

Columns 1/2 in Table 158 Attack types / tactics / countermeasures describe attack types.

9.1.3. Countermeasures

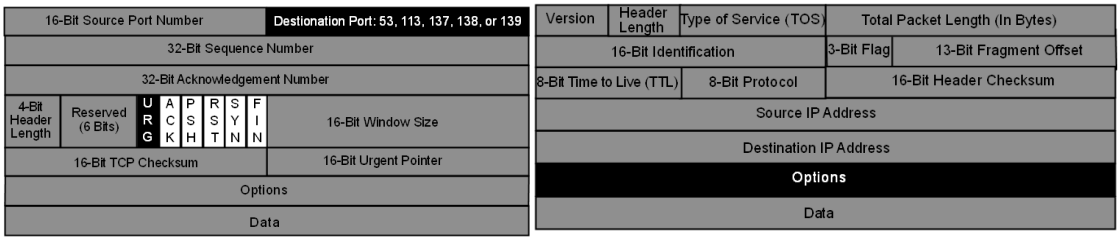
You can specify countermeasures in **Firewall** > **Attack Defense.**
Most countermeasures have a threshold parameter used to determine when an attack is occurring (for example, the number of packets sent within a time period).
Column 3 in Table 158 Attack types / tactics / countermeasures describes FGX countermeasures, which include:

- **Drop—**drop attack packets.
- **Alert—**an event will be generated informing administrator that an attack occurs. It includes:
  - Attack Type
  - Source/ destination IP address and port of the attack packet
  - Vsys that the attack packet belongs to
  - Protocol
  - Source/ destination zone (only displayed in policy-level defense)

9.2. Attack Types / Tactics / Countermeasures

Table 158 lists the common attack types and the countermeasures taken on FGX. TCP / IP packet header fields are shown in Figure 37 .

Figure 37 TCP / IP Packet Headers



.

Table 158 Attack types / tactics / countermeasures

Attack type	Attack tactic	FGX countermeasures
DoS / ICMP flood	Send many ICMP echo request packets to the victim host in a short period, exhausting host resources.	Limit number (threshold) of ICMP echo packets allowed to pass per second.
DoS / UDP flood	Send many UDP packets to the victim host in a short period, exhausting host resources.	Limit number (threshold) of UDP packets allowed to pass per second.
DoS / DNS flood	Send many DNS requests to the victim host in a short period, exhausting host resources.	Limit number (threshold) of UDP-based DNS requests allowed from a zone per second.
DoS / TCP SYN flood	Send many TCP SYN packets with false source IP addresses to the victim host in a short period, causing the victim host to send back a mass of SYN-ACK packets to hosts that usually do not exist or cannot be reached. The victim receives no ACK replies and TCP connections cannot be established. The victim host becomes overwhelmed with uncompleted connections.	Limiting the number (threshold) of TCP SYN packets allowed to pass through per second.
DoS / TCP SYN cookie		TCP SYN cookies enable FGX (instead of the server) to process SYN requests and protect from TCP SYN flood attacks. FGX can identify the validity of a three-way-handshake by checking the ACK sequence number without keeping the connection state information, dramatically saving system resources.
DoS / LAND	Send many TCP SYN packets with the same source and destination IP addresses of the victim host within a short period. Useless connections exhaust victim host resources.	Check TCP SYN packet source and destination IP addresses. If same, perform specified action.

Table 158 Attack types / tactics / countermeasures (*continued*)

Attack type	Attack tactic	FGX countermeasures
DoS / Smurf	Broadcast a large number of ICMP echo request packets using the source IP address of a victim host. Other hosts send reply packets, overwhelming the victim host or network.	When FGX receives an ICMP echo request packet, it checks whether the destination IP address is a broadcast address. If it is, FGX will consider the packet as an attack packet and process it according to the specified action.
DoS / TCP RST	Send many forged TCP RST packets to the target host to terminate normal connections, causing a service interruption.	If the packet does not belong to an existing session, FGX then classifies it as an attack packet and perform the specified action.
DoS / WinNuke	Send TCP URG packets to ports 53, 113, 137, 138, or 139, leading to a NetBIOS fragment overlap and Windows host crash.	Classify such packets as an WinNuke attack and perform the specified action.
DoS / Ping of Death	The maximum length of IP packets is 65,535 bytes. An IP packet larger than 65,535 bytes may make the host unable to work, no matter which operating system it is running. To launch a Ping of Death attack, attackers fragment an oversized IP packet and send the fragments to the victim host. After receiving the fragments, the victim host reassembles them into one IP packet. When the reassembled packet is oversized, the victim system may crash.	FGX reassembles the IP fragments. If the reassembled IP packet is larger than 65,535 bytes, FGX will consider this a Ping of Death attack and drop the fragments.
DoS / Teardrop	A large IP packet is fragmented into small pieces (IP fragments) for transmitting. In the header of each IP fragment, there is an offset field, indicating the starting position of the fragment in the original unfragmented packet. When the target host receives these IP fragments, it reassembles them into the original IP packets according to the offset values. If an IP packet fragment overlaps the previous one, reassembly may cause unexpected results (restart, crash, etc), especially on some earlier operating systems. Attackers launch a Teardrop attack by changing the offset fields, which leads to the IP fragments overlapping. Reassembly of these IP fragments may cause a system crash and therefore cause a denial of service.	When FGX receives an IP fragment, it checks the offset value and data length against those of the adjacent fragments to identify whether the fragments overlap. If they do overlap, FGX will delete the overlapping part and reassemble the fragments.
Reconnaissance / IP address sweep	Broadcast a large number of ICMP echo request packets. Hosts send reply packets are considered as active and can be easily located for further attacks.	IP address sweep occurs when more than 10 ICMP echo request packets sent from a host to different hosts are detected within the specified time period (threshold). Classify such packets as an attack and perform the specified action.

Table 158 Attack types / tactics / countermeasures (*continued*)

Attack type	Attack tactic	FGX countermeasures
Reconnaissance / TCP SYN port scan	Send TCP SYN packets to different ports of the same target host within a short period. Attackers can then identify which ports are open and which services are available for further attacks by the responses from these ports.	A TCP SYN port scan occurs when a host sends TCP SYN packets to more than 16 ports on the same destination host within a specified interval (threshold). Classify such packets as an attack and perform the specified action.
Reconnaissance / TCP NULL scan	Send TCP packets with no flags set to a port on the victim host. The port is open unless an RST packet is sent back. A TCP packet with no flags set is an anomaly. Different operating systems respond in different ways to such anomalies, so attackers can identify which operating system the target host is running by the way it responds.	FGX considers any TCP packet with no flags set as an attack packet and processes it according to the specified action.
Reconnaissance / TCP XMAS scan	Send TCP packets with the FIN, URG, and PSH flags set to a port on the victim host. The port is open unless an RST packet is sent back. This kind of TCP packet is an anomaly. Different operating systems respond with different RST packets, so attackers can identify which operating system the target host is running by the way it responds.	FGX considers any TCP packet with the FIN, URG, and PSH flags set as an attack packet and processes it according to the specified action.
Reconnaissance / TCP FIN scan	Send TCP FIN packets to a port on the victim host. The port is open unless an RST packet is sent back. Different operating systems respond with different packets to TCP FIN packets, so attackers can identify which operating system the target host is running by the way it responds.	FGX considers any TCP FIN packet that does not belong to an existing session as an attack packet and processes it according to the specified action.
Reconnaissance / TCP SYN&FIN flags	The SYN and FIN flags cannot be set in the same TCP packet simultaneously because they serve mutually exclusive purposes. A TCP packet with both SYN and FIN flags set is an anomaly. Different operating systems respond with different packets to such anomalies. Therefore, by sending packets with the SYN and FIN flags set to the target host, attackers can identify which operating system the target host is running by the way it responds.	FGX considers any TCP packet with the SYN and FIN flags set as an attack packet and drops it.
Reconnaissance / TCP FIN flag / no ACK	Normally, a TCP packet with the FIN flag has the ACK flag; otherwise, it is an anomaly. Different operating systems respond in different ways to such anomalies. By sending this kind of TCP packet to the target host, attackers can identify which operating system the host is running by the way it responds, for example, some hosts will drop the packet directly and some will return an RST packet.	FGX considers any TCP packet with the FIN flag but without the ACK flag as an attack packet and drops it.

Table 158 Attack types / tactics / countermeasures (*continued*)

Attack type	Attack tactic	FGX countermeasures
Reconnaissance / Non-SYN flag	The first packet initiating a session should be an SYN packet; otherwise, it is an anomaly. Before a session is initiated, attackers send such anomalous packets to a certain port on the victim host, and then they identify whether the port is open by its response. The port is open unless an RST packet is sent back.	When FGX receives a packet, it first performs a session lookup in the session table. If the packet belongs to an existing session, FGX will update this session and forward the packet. If not, FGX will check whether the packet has the SYN flag. If it does, FGX will create a new session and forward the packet. If not, FGX will consider the packet as an attack packet and drop it.
Reconnaissance / IP spoofing	Attackers can insert a forged source address in the packet header to gain access to a restricted area of a target network as a legitimate user. This technique is called IP spoofing.	FGX provides two IP spoofing detection methods. One is to check the route, and the other is to bind IP and MAC addresses. When interfaces on FGX are operating in routing or NAT mode, the detection of IP spoofing relies on checking the route of the packet with the route entry. When a packet reaches an interface and its IP address does not correspond with the source IP address in the route entry, FGX considers this as IP spoofing. When interfaces on FGX are operating in transparent mode, IP spoofing detection depends on the binding of the IP address to the MAC address. When a packet arrives and does not have correctly bound IP and MAC addresses, FGX considers this as IP spoofing.
TCP evasion / Spoofed reset	A TCP RST packet is used to reset erroneous connections. When a host receives such a packet, it will clear all established connections in the cache. If the host wants to continue to send packets, it has to establish a new connection. Attackers send a large number of TCP RST packets with spoofed source IP addresses to the target host, which disconnects normal connections, resulting in data loss and service interruption.	Limit the maximum number (threshold) of RST packets allowed to pass per connection within a specified period. When the threshold is exceeded, FGX performs the specified action.

Table 158 Attack types / tactics / countermeasures (*continued*)

Attack type	Attack tactic	FGX countermeasures
TCP evasion / Small PMTU	The maximum transmission unit (MTU) refers to the size (in bytes) of the largest protocol data unit that can be sent over the network. The smallest MTU in a path is the path MTU (PMTU). The PMTU between two hosts can be learned through PMTU discovery to determine the size of packets for transmission. Normally a host sends an IP packet based on its own MTU value and marks that the packet cannot be fragmented during transmission. When the packet in transit crosses a link of which MTU is smaller than the packet size, the router on the link will reply the source host with a "Destination Unreachable" ICMP message, allowing the host to modify its own MTU value appropriately. In a Small PMTU attack, attackers send intentionally forged ICMP messages to the victim host specifying an excessively low value for the connection's PMTU. Then the victim host sends a large number of small-sized packets (smaller than the real PMTU), which consumes a lot of system resources and potentially makes the victim host unable to respond.	FGX compares the next-hop MTU in each returned "Destination Unreachable" ICMP message with the user-specified minimum MTU. If the user-specified MTU is larger, FGX will drop the ICMP message to prevent hosts from sending packets with excessively low MTU values and thus avoid Small PMTU attacks.
TCP evasion / TCP control bit anomaly	TCP control bits check is used to check the packet control bits, SYN, ACK, or FIN when establishing and closing TCP connections. The control bit of a packet has different states during these processes. When a client wants to establish a TCP connection with a server, it will send an SYN packet as a connection request to the server. When the server receives this packet, it will reply to the client with an SYN/ACK packet. Finally, the client will send an ACK packet to finish the three-way handshake. If the client wants to terminate the connection, it will send an FIN packet to the server.	Check the control bit in the header of a packet when a TCP connection is established or closed. If there are any errors in the control bit, FGX will block this connection, thus preventing malicious attacks and connection disruption.
TCP evasion / TCP data overlap	Data in packets may overlap when errors or modifications occur during TCP packet transmission, causing the host system receiving these packets to crash.	Check the data in packets, and remove the repeated parts in the packets.
TCP evasion / TCP protection	The TCP protocol has some intrinsic vulnerabilities that attackers may take advantages.	FGX provides security protection for protocol applications by checking TCP sequence numbers and TCP checksums. **Check TCP checksums—**checks whether the checksums of a TCP packet are valid. TCP packets with invalid checksums will be dropped. **Check TCP sequence numbers—** checks the sequence number of a TCP packet against the TCP connection state. TCP packets of specified state with invalid sequence number will be dropped.

Table 158 Attack types / tactics / countermeasures (*continued*)

Attack type	Attack tactic	FGX countermeasures
IP Option Check / IP record route option	The record route option records the IP addresses of network devices an IP packet passes through. When the host receives an IP packet with the record route option set, it can gain the routing information of the packet. In case that attackers gain access to a compromised host and send the host IP packets with the record route option set, they can then obtain the routing information as well as the topology and addressing scheme of the target network for further attack.	When FGX receives an IP packet with the record route option set, it processes the packet according to the specified action. If the packet is permitted to pass, FGX will check the format of the option. If the format is correct, FGX will record the IP address of the outgoing interface in the record route option of the packet and then forward it. Otherwise, it will drop the packet.
IP Option Check / IP timestamp option	The timestamp option records the time a router spends to process a packet and is usually used to trace routers during network debugging. When a host receives a packet with the timestamp option set, it obtains the IP addresses of the routers that the packet passes through and the time taken to traverse between routers. Attackers can take advantage of the IP timestamp option. If they have managed to gain access to a compromised host and send the host IP packets with the timestamp option set, they can then obtain the routing information as well as the topology and addressing scheme of the target network.	When FGX receives an IP packet with the timestamp option set, it processes the packet according to the specified action. If the packet is permitted to pass, FGX will check the format of the option. If the format is correct, FGX will record the time it takes to process the packet in the packet timestamp option and then forward it. Otherwise, it will drop the packet.
IP Option Check / IP strict source route option	The strict source route option specifies the route of a packet when it is transmitted across a network, so senders can choose routes —the route with the shortest delay, the route with the best throughput, or a safer and more reliable route. Packets with the strict source route set must pass through all the routers specified in the packet header and cannot pass through routers not specified. If these packets pass through a router not specified or do not pass through all the specified routers, they will be dropped. Using this, attackers can hide the real source of attack packets by specifying routes and can thereby gain access to protected networks.	When FGX receives an IP packet with the strict source route option set, it processes the packet according to the specified action. If the packet is permitted to pass, FGX will check the format of the option. If the format is correct, FGX will use the IP address of the outgoing interface to replace that specified in the option and forward the packet. Otherwise, it will drop the packet.
IP Option Check / IP loose source route option	The IP loose source route option works in a way similar to the IP strict source route option, but it offers an extended context for packets to select routers on the network. IP packets with the loose source route option set must pass through all specified routers in order, but they are permitted to pass through routers that are not specified. Attackers often use the IP loose source route option to get access to protected networks. With the loose source route option, they can hide the real source of attack packets by specifying routes.	When FGX receives an IP packet with the loose source route option set, it processes the packet according to the specified action. If the packet is permitted to pass, FGX will check the format of the option. If the format is correct, FGX will use the IP address of the outgoing interface to replace that specified in the option and forward the packet. Otherwise, it will drop the packet.

Table 158 Attack types / tactics / countermeasures (*continued*)

Attack type	Attack tactic	FGX countermeasures
IP Option Check / IP traceroute option	The IP Traceroute option is used to trace a packet from source to destination. If a source host sends an ICMP echo request packet to the destination host with the IP Traceroute option set, all the routers the packet passes through will reply to the source host with an ICMP Traceroute packet. If there are *x* routers from source to destination, the source host will receive *x* ICMP Traceroute packets from the routers and an ICMP reply packet from the destination host. In this way, the source host manages to trace the route. If the ICMP reply packet from the destination host has the IP Traceroute option set, the destination host can trace all the routers the packet has passed through. Attackers often use the IP Traceroute option to obtain the topology and addressing scheme of the target network.	When FGX receives an IP packet with the Traceroute option set, it processes the packet according to the specified action. If the packet is permitted to pass, FGX will check the format of the option. If the format is correct, FGX will send back an ICMP Traceroute message to the source host and then forward the packet. Otherwise, it will drop the packet.
IP Option Check / Other IP options	In addition to the IP option attacks described above, FGX can detect other IP option attacks and defend against them.	When FGX receives an IP packet with other IP options set, it processes the packet according to the specified action. If the packet is allowed to pass, FGX will check the format of the option. If the format is correct, FGX will forward the packet. Otherwise, it will drop the packet.
IP Fragmentation & Reassembly	Attackers launch an IP packet fragmentation attack by making use of the vulnerabilities in packet fragment reassembly codes. They send the target host IP fragments comprising malicious information, which makes the target host unable to process the fragments correctly, causing anomalies or even a crash on the host system.	FGX provides an IP fragmentation and reassembly function. When it receives IP fragments, it first checks whether they are valid. If they are, FGX will reassemble them into a packet. If not, FGX will drop them.
ICMP Attack / ICMP ISS Pinger	Internet Security Scanner (ISS), scans for host information and system vulnerabilities.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP L3retriever Ping	Finds out the states of hosts on a network through ICMP echoes.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Nemesis v1.1 Echo	Sends ICMP echo requests through Nemesis v1.1.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Ping NMAP	Network Mapper (NMAP) scan, quickly scans large networks and individual hosts to get the running information of hosts on the network.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Icmpenum v1.1.1	Scans the IP addresses of target hosts.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Redirect Host	Redirects the routes of a host by modifying its routing table.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Redirect Net	Redirects routes on a network.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Superscan Echo	Checks the states of hosts within a network through Superscan echo requests.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Traceroute IPOPTs	Sends ICMP packets and records their paths.	Classify such action as an attack and perform the specified action.

Table 158 Attack types / tactics / countermeasures (*continued*)

Attack type	Attack tactic	FGX countermeasures
ICMP Attack / ICMP Webtrends Scanner	Scans hosts on a network and gets information about their running states.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Source Quench	A kind of flow control mechanism that attackers can take advantage of to cause low bandwidth and initiate DoS attacks.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Broadscan Smurf Scanner	Sends a specific ICMP packet to scan active hosts on a network.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Ping Speedera	Consumes host resources on a network using Speedera ping.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP TJPingPro1.1Build 2 Windows	Obtains the route to a target host on a network.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Ping Whatsup Gold Windows	Obtains information such as user names and IP addresses on a network.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Ping CyberKit 2.2 Windows	Checks network connections and records routes.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Ping Sniffer Pro/ NetXRay Network Scan	Detects active hosts on a network through ping.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Destination Unreachable-Communication Administratively Prohibited	Makes destination IP addresses unreachable.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Destination Unreachable-Communication with Destination Host Administratively Prohibited	Makes destination hosts unreachable.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Destination Unreachable-Communication with Destination Network Administratively Prohibited	Makes destination networks unreachable.	Classify such action as an attack and perform the specified action.

Table 158 Attack types / tactics / countermeasures (*continued*)

Attack type	Attack tactic	FGX countermeasures
ICMP Attack / ICMP Digital Island Bandwidth Query	Collects information on connected network bandwidth.	Classify such action as an attack and perform the specified action.
ICMP Attack / ICMP Path MTU Denial of Service	Finds out MTUs and then initiates DoS attacks.	Classify such action as an attack and perform the specified action.

9.3. Basic Configuration Steps

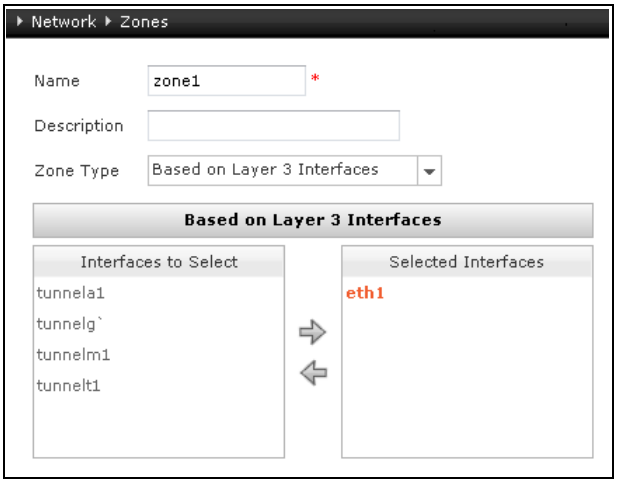
This section describes the basic configuration procedure, providing both WebUI operation and CLI.

- 9.3.1. Create a Zone
- 9.3.2. Apply Attack Defense

9.3.1. Create a Zone

On FGX, attack defense can only be applied to a zone, so the devices that need to be protected should be allocated to a zone first.

1. In **Network** > **Zone**, click **New** and create a zone.



2. Click **OK**.
3. Click  .

Table 159 Creating a zone

zone *zone_name*	Creates a zone.
zone *zone_name* **based-layer2 vlan** *vlan_id* [*l2_interface_name*]	Configures a zone based on Layer 2 interfaces.
zone *zone_name* **based-layer3** *l3_interface_name*	Configures a zone based on Layer3 interfaces.

9.3.2. Apply Attack Defense

- 9.3.2.1. DoS Defense
- 9.3.2.2. Reconnaissance Defense
- 9.3.2.3. TCP Evasion Control
- 9.3.2.4. IP Option Check
- 9.3.2.5. ICMP Attack Defense

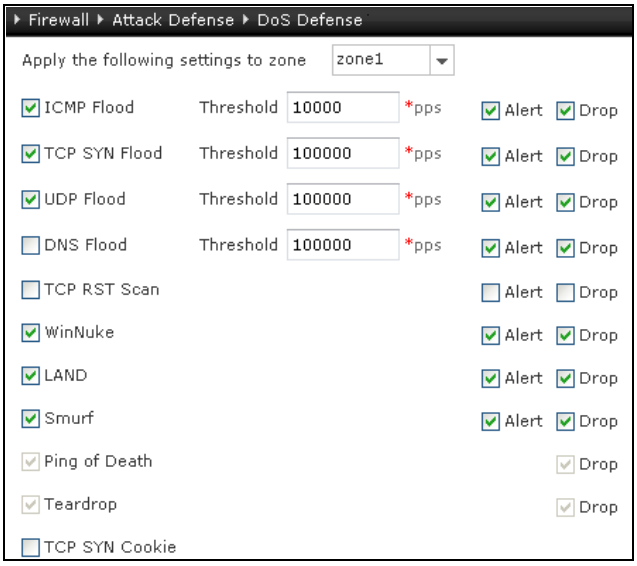
The following commands can be used to enable a certain type of defense and set its threshold:

Table 160 Common Commands

attack-defense *zone_name attack_name* **active** {**on** {**alert** [**drop**] **| drop** [**alert**]} **| off** [**alert** [**drop**] **| drop** [**alert**]]}	Sets defense against a specified attack in a specified zone. If defense against the attack is enabled, when an attack is detected by FGX, the attack packets will be processed according to the preset actions.
attack-defense *zone_name attack_name* **threshold**	Sets threshold for a specified defense to judge an attack in a specified zone.
show attack-defense	Displays all attack defense settings in a specified zone.

9.3.2.1. DoS Defense

1. Choose **Firewall > Attack Defense > DoS Defense** and configure the related settings.



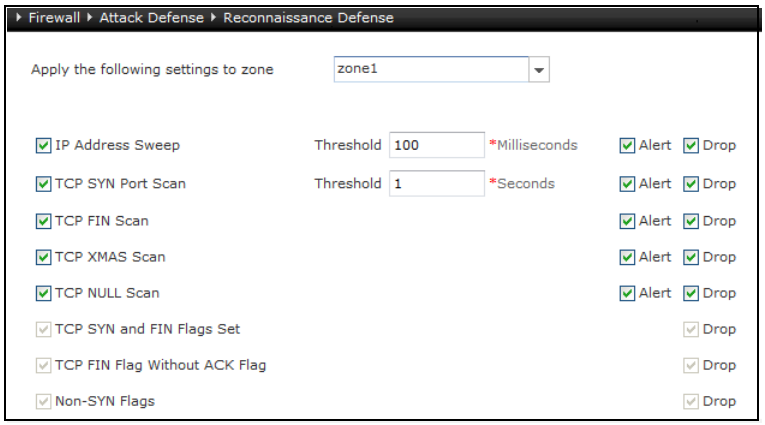
2. Click **OK**.
3. Click .

Table 161 DoS Defense Commands

attack-defense *zone_name* **tcp-syn-cookie active** {**on** | **off**}	Enables or disables SYN Cookie defense in a specified zone.

9.3.2.2. Reconnaissance Defense

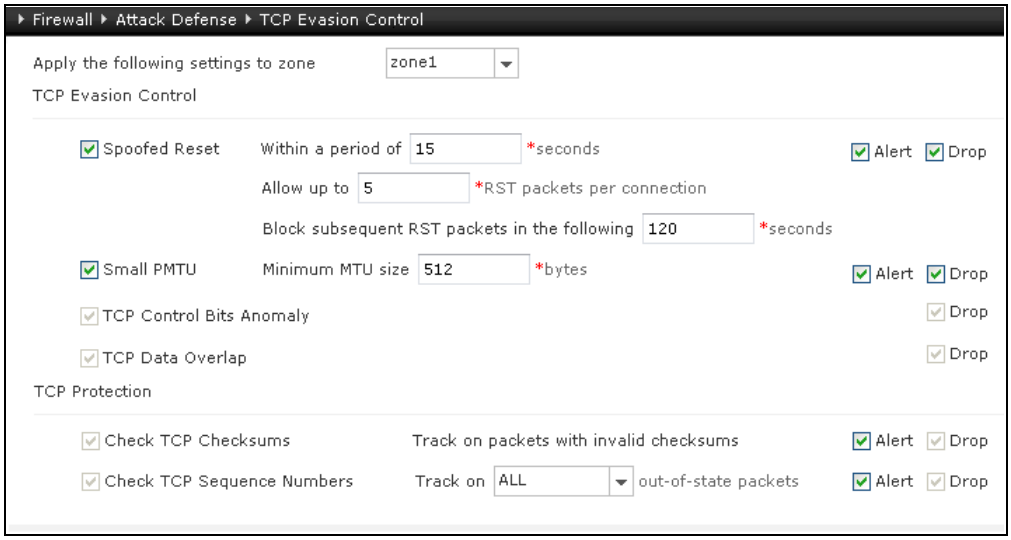
1. Choose **Firewall > Attack Defense > Reconnaissance Defense** and configure the related settings.



2. Click **OK**.
3. Click .

9.3.2.3. TCP Evasion Control

1. Choose **Firewall > Attack Defense > TCP Evasion Control** and configure the related settings.



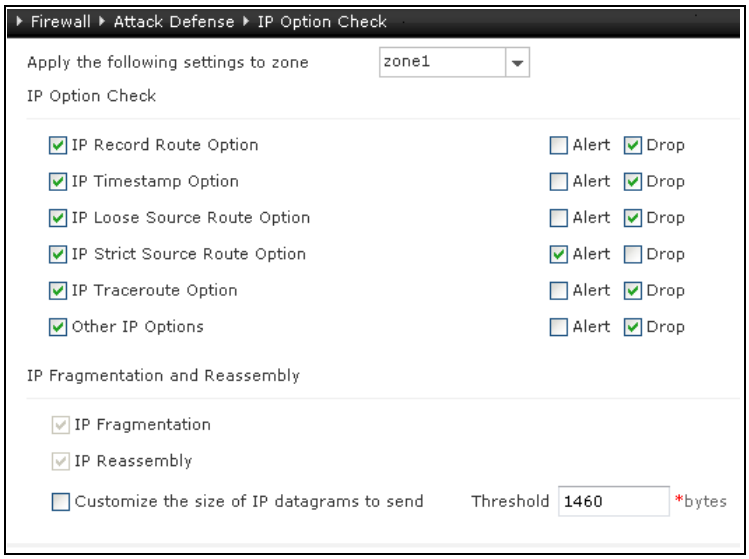
2. Click **OK**.
3. Click .

Table 162 TCP Evasion Control-Specific Commands

attack-defense *zone_name* **spoofed-reset**	Sets the threshold for the spoofed TCP reset protection of TCP evasion control.
attack-defense *zone_name* **small-pmtu parameter** *threshold_value*	Sets the minimum MTU for TCP evasion control to protect a host from pmtu attack by avoiding packets with extremely small MTU values.
attack-defense *zone_name* **tcp-checksum** [**alert**]	Enables or disables alerts against packets with invalid checksums.
attack-defense tcp-sequence-track	Sets the TCP sequence check function.

9.3.2.4. IP Option Check

1. Choose **Firewall > Attack Defense > IP Option Check** and configure the related settings.



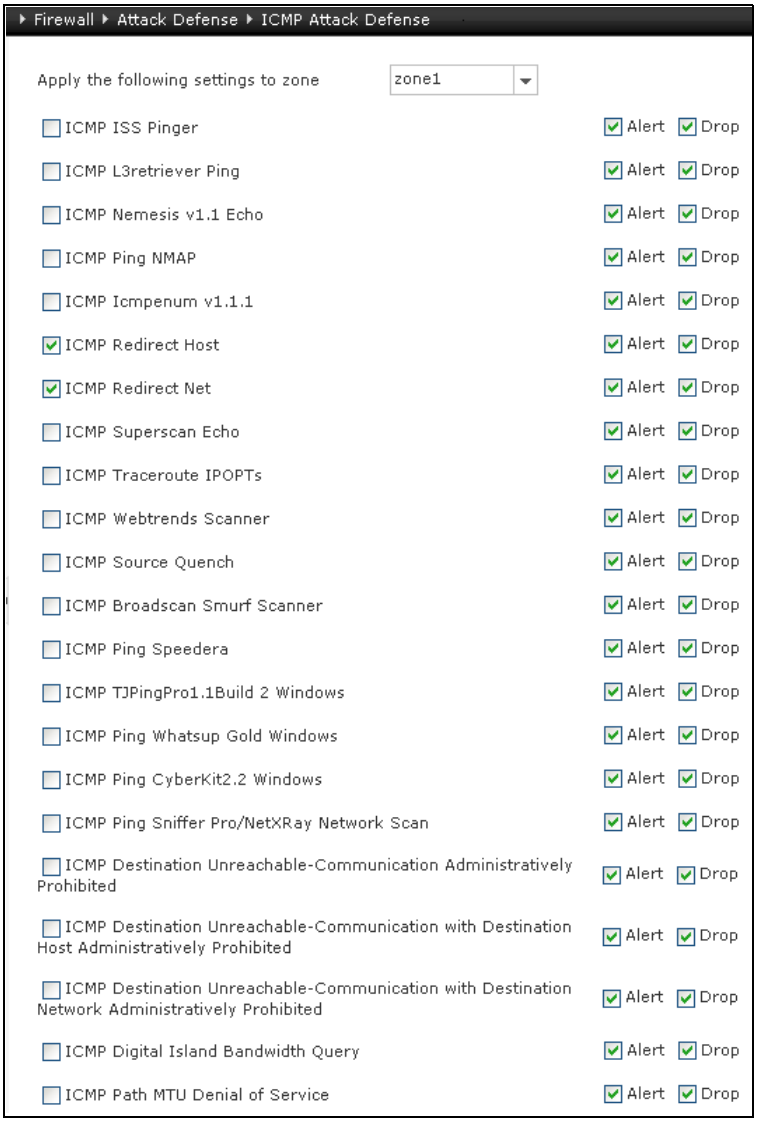
2. Click **OK**.
3. Click .

Table 163 IP Option Check-Specific Commands

customize-the-size-of-IP-datagrams-to-send active {**on** | **off**} **threshold** *threshold_ip_datagram*	Enables or disables the function of customizing the size of reassembled packets to send per time and to set the threshold.
show customize-the-size-of-IP-datagrams-to-send	Displays the settings of customizing the size of reassembled packets to send.

9.3.2.5. ICMP Attack Defense

1. Choose **Firewall > Attack Defense > ICMP Attack Defense** and configure the related settings.



2. Click **OK**.
3. Click  .

9.4. Parameter Reference

- 9.4.1. DoS Defense Parameters
- 9.4.2. ICMP Attack Defense Parameters
- 9.4.3. IP Option Check Parameters
- 9.4.4. Reconnaissance Defense
- 9.4.5. TCP Evasion Control Parameters

9.4.1. DoS Defense Parameters

Table 164 Parameters of DoS Defense

Attack defense function	Enable	Alert	Drop	Threshold range / default	Other parameters
ICMP Flood	Y/N	Y/N	Y/N	1 - 1,000,000 pps / 10,000	
TCP SYN Flood	Y/N	Y/N	Y/N	1 - 1,000,000 pps / 100,000	
UDP Flood	Y/N	Y/N	Y/N	1 - 1,000,000 pps / 100,000	
DNS Flood	Y/N	Y/N	Y/N	1 - 1,000,000 pps / 100,000	
TCP RST Scan	Y/N	Y/N	Y/N		
WinNuke	Y/N	Y/N	Y/N		
LAND	Y/N	Y/N	Y/N		
Smurf	Y/N	Y/N	Y/N		no broadcast addresses in IPv6, so there is no Smurf defense in IPv6
Ping of Death	Y		Y		
Teardrop	Y		Y		
TCP SYN Cookies	Y/N				

9.4.2. ICMP Attack Defense Parameters

Table 165 Parameters of ICMP Attack Defense

Attack defense function	Enable	Alert	Drop	Threshold range / default	Other parameters
ICMP ISS Pinger	Y/N	Y/N	Y/N		
ICMP L3retriever Ping	Y/N	Y/N	Y/N		
ICMP Nemesis v1.1 Echo	Y/N	Y/N	Y/N		
ICMP Ping NMAP	Y/N	Y/N	Y/N		
ICMP Icmpenum v1.1.1	Y/N	Y/N	Y/N		
ICMP Redirect Host	Y/N	Y/N	Y/N		
ICMP Redirect Net	Y/N	Y/N	Y/N		
ICMP Superscan Echo	Y/N	Y/N	Y/N		
ICMP Traceroute IPOPTs	Y/N	Y/N	Y/N		
ICMP Webtrends Scanner	Y/N	Y/N	Y/N		
ICMP Source Quench	Y/N	Y/N	Y/N		
ICMP Broadscan Smurf Scanner	Y/N	Y/N	Y/N		
ICMP Ping Speedera	Y/N	Y/N	Y/N		
ICMP TJPingPro1.1Build 2 Windows	Y/N	Y/N	Y/N		
ICMP Ping Whatsup Gold Windows	Y/N	Y/N	Y/N		
ICMP Ping CyberKit 2.2 Windows	Y/N	Y/N	Y/N		
ICMP Ping Sniffer Pro/NetXRay Network Scan	Y/N	Y/N	Y/N		
ICMP Destination Unreachable-Communication Administratively Prohibited	Y/N	Y/N	Y/N		
ICMP Destination Unreachable-Communication with Destination Host Administratively Prohibited	Y/N	Y/N	Y/N		
ICMP Destination Unreachable-Communication with Destination Network Administratively Prohibited	Y/N	Y/N	Y/N		
ICMP Digital Island Bandwidth Query	Y/N	Y/N	Y/N		
ICMP Path MTU Denial of Service	Y/N	Y/N	Y/N		
ICMP Source Quench	Y/N	Y/N	Y/N		

9.4.3. IP Option Check Parameters

Table 166 Parameters of IP Option Check

Attack defense function	Enable	Alert	Drop	Threshold range / default	Other parameters
IP Record Route Option	Y/N	Y/N	Y/N		
IP Timestamp Option	Y/N	Y/N	Y/N		
IP Strict Source Route Option	Y/N	Y/N	Y/N		
IP Loose Source Route Option	Y/N	Y/N	Y/N		
IP Traceroute Option	Y/N	Y/N	Y/N		
Other IP Options	Y/N	Y/N	Y/N		
IP Fragmentation	Y				
IP Reassembly	Y				
Customize size of IP datagrams to send	Y/N			32-1460/ 1400 bytes	

9.4.4. Reconnaissance Defense

Table 167 Parameters of Reconnaissance Defense

Attack defense function	Enable	Alert	Drop	Threshold range / default	Other parameters
IP Address Sweep	Y/N	Y/N	Y/N	100 - 10,000 ms (multiple of 100) / 100	
TCP SYN Port Scan	Y/N	Y/N	Y/N	1 - 7,200 secs / 1	
TCP FIN Scan	Y/N	Y/N	Y/N		
TCP XMAS Scan	Y/N	Y/N	Y/N		
TCP NULL Scan	Y/N	Y/N	Y/N		
TCP SYN & FIN Flags	Y		Y		
TCP FIN Flag Without ACK Flag	Y		Y		
Non-SYN Flags	Y		Y		

9.4.5. TCP Evasion Control Parameters

Table 168 Parameters of TCP Evasion Control

Attack defense function	Enable	Alert	Drop	Threshold range / default	Other parameters
Spoofed Reset	Y/N	Y/N	Y/N	2 - 10,000 / 5	time period = 2 - 10,000 secs / 15 blocking interval = 2 - 10,000 secs/ 120
Small PMTU	Y/N	Y/N	Y/N	68 - 512 bytes / 350	
TCP Control Bits Anomaly	Y		Y		
TCP Data Overlap	Y		Y		
Check TCP checksums	Y	Y/N	Y		
Check TCP sequence numbers	Y	Y/N	Y		FGX checks the sequence number of a TCP packet against the TCP connection state. If a packet matches the state but has an incorrect sequence number, the packet will be dropped. FGX checks the sequence number of the following types of packets: **All—**checks all out-of-state packets and logs every action performed on packets after sequence number verification (includes packets with correct ACK # and incorrect sequence #). **Anomalous—**checks anomalous out-of-state packets and logs only significant events causing packet loss (includes packets with invalid ACK # and invalid sequence #). **Suspicious—**checks suspicious out-of-state packets and logs significant events causing packet loss and potential attacks (includes SYN retransmission with different sequence numbers and SYN/SYN-ACK retransmission with different window scaling).

10 Unified Threat Management

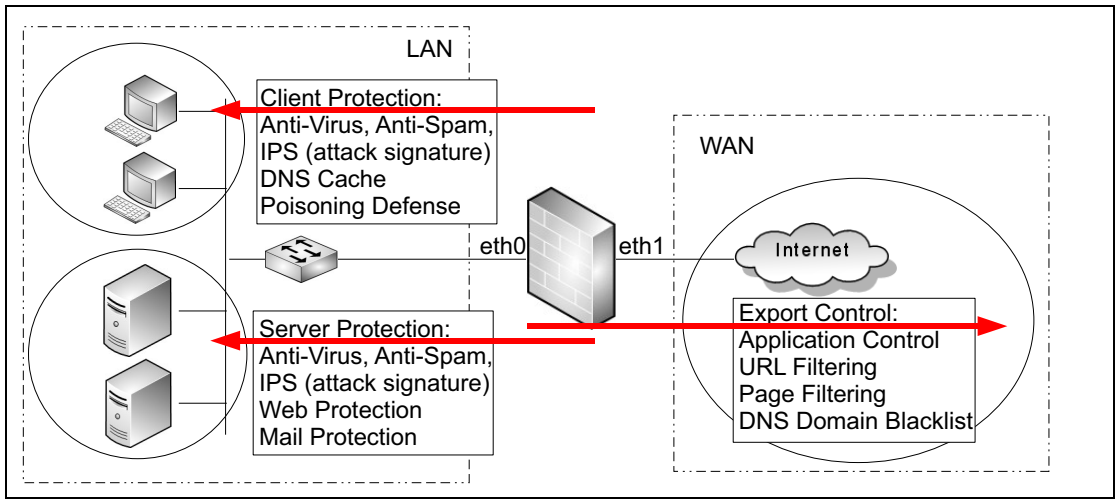
This chapter describes FGX unified threat management (UTM).

- 10.1. Overview. Describes basic UTM concepts.
- 10.2. Basic Configuration. Gives a simplified step-by-step introduction to configuration for all UTM features. Your scenario will not require all of these steps.
- 10.3. Scenarios. Describes real-world threat scenarios.
- 10.4. UTM Examples. Gives detailed step-by-step examples.
- 10.5. Parameter reference. Describes in detail all UTM parameters.

10.1. Overview

The following figure shows the typical application scenario of UTM.

Figure 38 Typical UTM Scenario



UTM offers three kinds of security policies:

- 10.1.1. Export control
- 10.1.2. Client protection
- 10.1.3. Server protection

If a packet matches any of the security policies, it will undergo UTM inspection. UTM inspection performed on packets matching security policies includes:

- Protocol identification.
- Protocol anomaly detection according to RFC specifications.
- Protocol restriction based on user-defined conditions (takes priority over anomaly detection).
- Packet content-level inspection.

UTM inspection for client/server protection includes:

- 10.1.2.3. Anti-Virus
- 10.1.2.4. Anti-Spam
- 10.1.2.2. IPS

UTM also supports:

- Real-time update of the application list, URL categories, anti-virus rules, anti-spam rules, and attack signature rules.
- Notification messages sent to clients when UTM detects viruses, spam, or attacks.
- Monitoring. See Chapter 14, Monitoring.

10.1.1. Export control

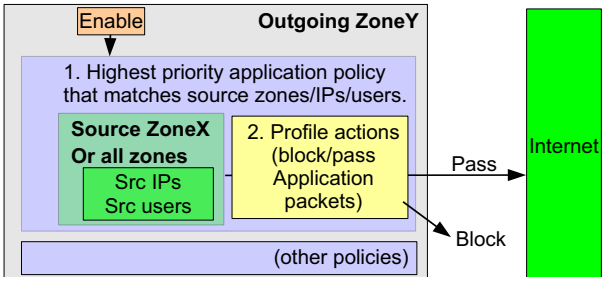
Export control is used to control user traffic on the outgoing zones for security. For each outgoing zone: Block unallowed traffic from multiple incoming zones.

- 10.1.1.1. Application packet processing
- 10.1.1.2. HTTP packet processing
- 10.1.1.3. DNS packet processing

10.1.1.1. Application packet processing

UTM export control provides application control. Application packet processing steps are shown in the diagram below:

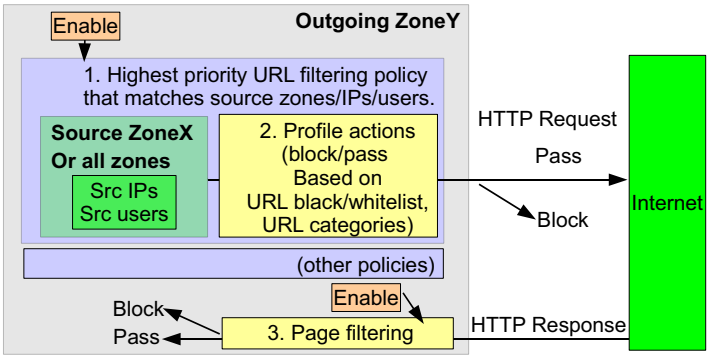
1. Determine highest-priority policy that matches the source zone/IPs/users.
2. Perform application control profile (specified in policy) actions.



10.1.1.2. HTTP packet processing

UTM export control provides URL filtering on HTTP requests and page filtering on HTTP responses. HTTP packet processing steps are shown in the diagram below:

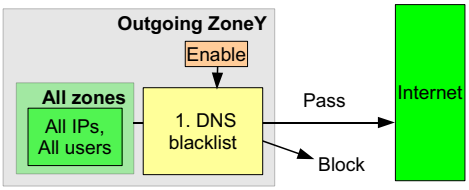
1. Determine highest-priority policy that matches the source zone/IPs/users.
2. Perform URL filtering profile (specified in policy) actions.
3. Perform page filtering.



10.1.1.3. DNS packet processing

UTM export control provides a DNS domain blacklist to filter DNS requests. DNS packet processing steps are shown in the diagram below:

1. Block blacklisted DNS requests.



10.1.2. Client protection

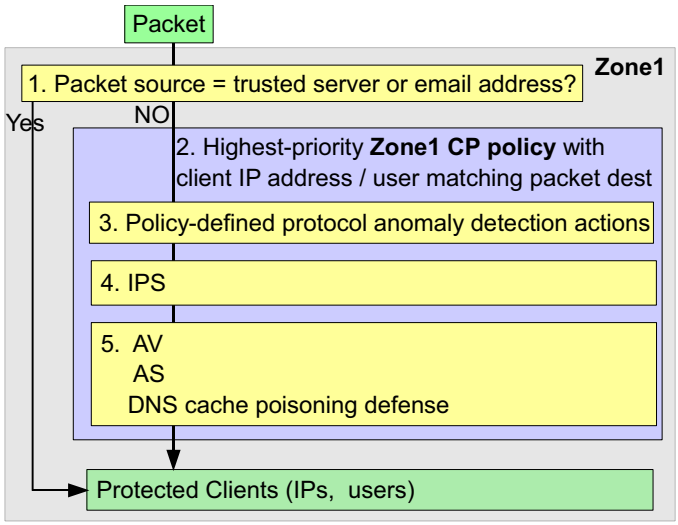
Client protection only inspects the traffic sent from servers to clients, such as download traffic and e-mails, for clients within specified zones. For each client zone: Block unallowed traffic to specified client IPs / users.

- 10.1.2.1. Basic steps
- 10.1.2.2. IPS
- 10.1.2.3. Anti-Virus
- 10.1.2.4. Anti-Spam

10.1.2.1. Basic steps

UTM client protection packet processing steps are shown in the diagram below:

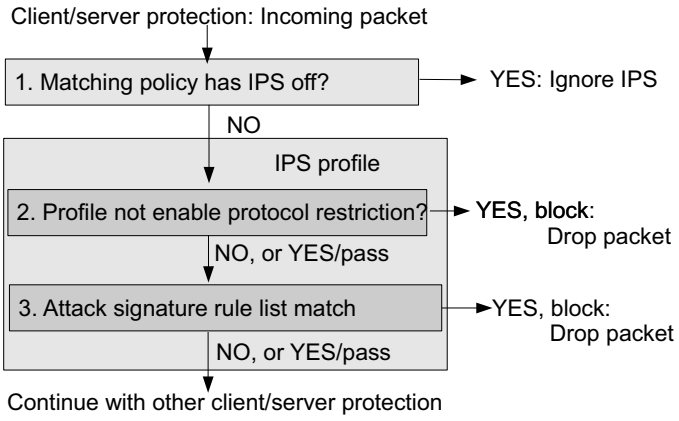
1. If from a trusted server or email address (zone-defined): Pass.
2. Determine highest-priority policy that matches packet client IP address and/or user for the destination zone.
3. Perform protocol anomaly detection actions (policy-defined).
4. Perform IPS inspection (specified in policy-defined IPS profile), including protocol restriction and IPS attack signature detection. See 10.1.2.2. IPS.
5. Perform one or more of the following depending on the packet protocol:
   - For POP3, IMAP, FTP, or HTTP protocol packets, perform AV profile (specified in policy) actions. (If from AV trusted source: Skip AV.) See 10.1.2.3. Anti-Virus.
   - For POP3 protocol packets, perform AS profile (specified in policy) actions. (If AS allowed: Skip AS. If AS blocked: Drop packet. If not AS allowed/blocked, perform AS spam word list actions.) See 10.1.2.4. Anti-Spam.
   - For DNS protocol packets, perform DNS cache poisoning defense (globally defined) actions.



10.1.2.2. IPS

IPS defines attack signature detection and protocol restriction, and it is specified in client/server protection policies. IPS packet processing steps are shown in the diagram below:

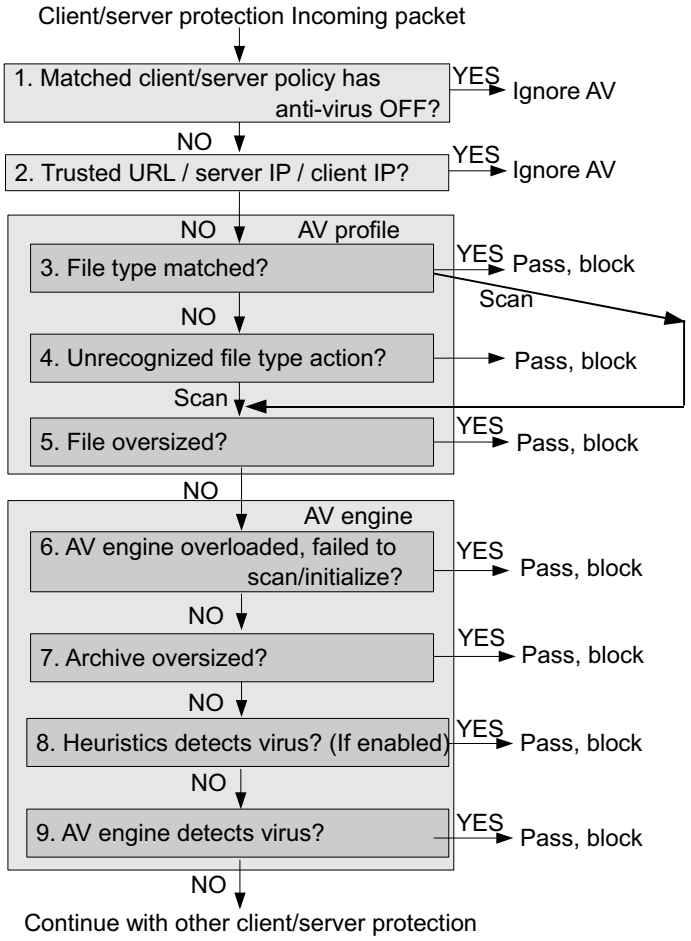
1. Ignore IPS if turned off in policy.
2. If enabled in profile: Perform the type of protocol restriction for the client or server type. If matches restriction, then pass or block (as defined in the protocol restriction level last selected in the UI).
3. If matches attack signature rule list, then pass or block (as defined in profile).



10.1.2.3. Anti-Virus

Anti-virus is provided in client or server protection to detect viruses in files passing through FGX. Anti-virus packet processing steps are shown in the diagram below:

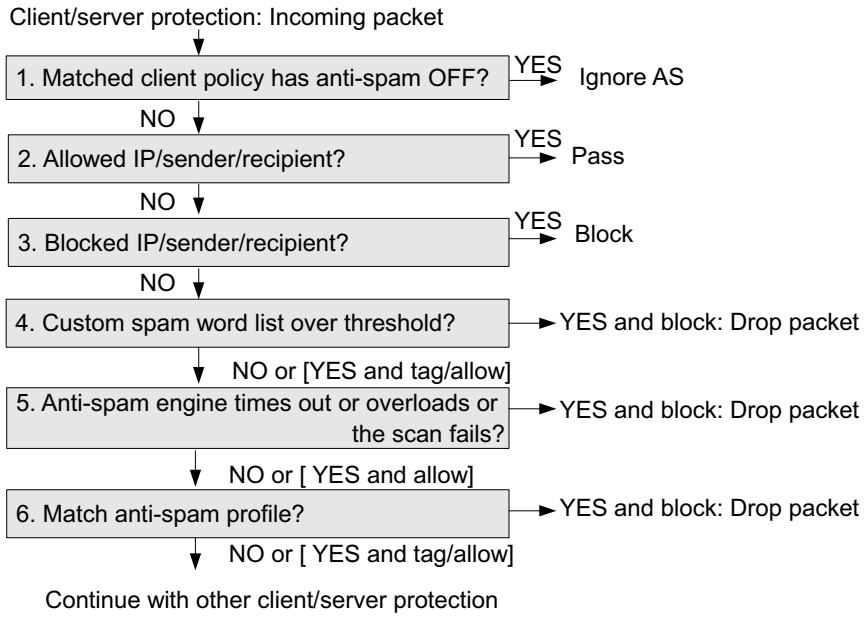
1. Ignore AV if turned off in policy.
2. If from a trusted URL, web server, or client: Pass.
3. If the file type is matched, then pass, block or scan (specified in profile).
4. If the file is unrecognized, then pass, block or scan (specified in profile).
5. If the file is oversized, then pass or block (specified in profile).
6. If AV engine overloaded, failed to scan/initialize, then pass or block file according to scan settings.
7. If archive oversized, then pass or block (archive settings).
8. If heuristics enabled and detects a virus, then pass or block (heuristic scanning settings).
9. If AV engine detects virus, then pass or block (scan settings).



10.1.2.4. Anti-Spam

Anti-spam is provided in client or server protection to detect spam in emails passing through FGX. Anti-spam packet processing steps are shown in the diagram below:

1. Ignore AS if turned off in policy.
2. If matches IP/sender/recipient allow list: Pass.
3. If matches IP/sender/recipient block list: Block.
4. If custom spam word list is matched and over threshold, then block or allow (optionally tag).
5. If anti-spam engine ever times out or overloads or the scan fails, then pass emails without scanning or block.
6. If matches anti-spam profile, then block or allow (optionally tag).



10.1.3. Server protection

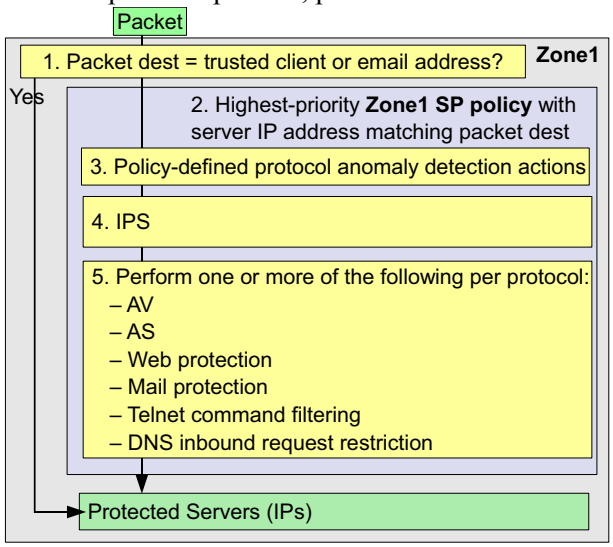
Server protection only protects the server-side traffic, such as upload traffic and emails, for servers within specified zones. For each server zone: Block unallowed traffic to specified server IPs.

- 10.1.2.1. Basic steps
- 10.1.3.2. IPS, AV, AS (same as for Client Protection)

10.1.3.1. Basic steps

UTM server protection packet processing steps are shown in the diagram below.

1. If from a trusted client or email address (zone-defined): Pass.
2. Determine highest-priority policy that matches packet server IP address for the destination zone.
3. Perform protocol anomaly detection actions (policy-defined).
4. Perform IPS inspection (specified in policy-defined IPS profile), including protocol restriction and IPS attack signature detection. See 10.1.2.2. IPS.
5. Perform one or more of the following depending on the packet protocol:
   - For SMTP or FTP protocol packets, perform AV scanning. If from trusted source: Skip AV scanning. Perform AV profile (specified in policy) actions. See 10.1.2.3. Anti-Virus.
   - For SMTP protocol packets, perform AS inspection. If AS allowed: Skip AS inspection. If AS blocked: Drop emails. Perform AS spam word list (globally defined) actions. Perform AS profile (specified in policy) actions. See 10.1.2.4. Anti-Spam.
   - For HTTP protocol packets, perform web protection (globally defined) actions.
   - For SMTP protocol packets, perform mail protection (globally defined) actions.
   - For Telnet protocol packets, perform Telnet command filtering. (policy-defined)
   - For DNS protocol packets, perform DNS inbound request restriction. (policy-defined).



10.1.3.2. IPS, AV, AS

Same as for Client Protection.

10.2. Basic Configuration

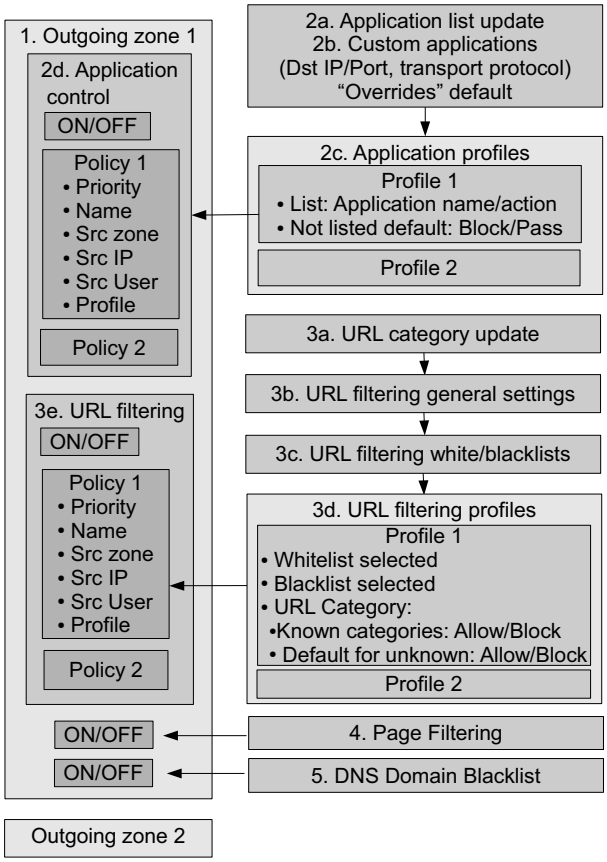
This section includes:

- 10.2.1. Export control
- 10.2.2. Client protection
- 10.2.3. Server protection
- 10.2.4. Notification messages
- 10.2.5. Overview page

Note: UTM can be configured through the WebUI only.

10.2.1. Export control

Figure 39 Export Control Configuration Steps



Non-export-control setup:

- 10.2.1.1. Create zones, access policies, default route, NAT rules.

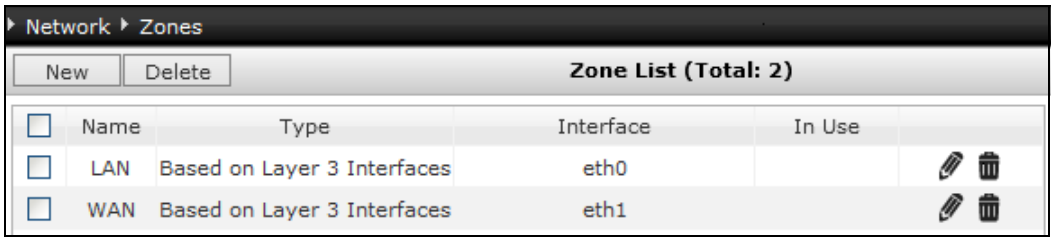
Export control setup:

- 10.2.1.2. Configure application control:
  - 10.2.1.2.1. Update application list.
  - 10.2.1.2.2. Create custom applications.
  - 10.2.1.2.3. Create application control profiles.
  - 10.2.1.2.4. Create application control policies.
- 10.2.1.3. Configure (HTTP request) URL filtering:
  - 10.2.1.3.1. Update URL filtering rule base.
  - 10.2.1.3.2. Configure URL filtering general settings.
  - 10.2.1.3.3. Create URL filtering profiles: Black/white lists.
  - 10.2.1.3.4. Create URL filtering profiles.
  - 10.2.1.3.5. Create URL filtering policies.
- 10.2.1.4. Configure (HTTP response) page filtering.
- 10.2.1.5. Configure DNS domain blacklist.

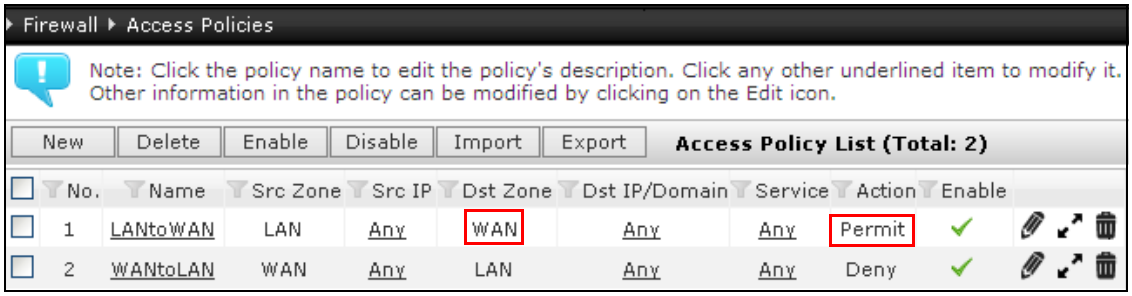
10.2.1.1. Create zones, access policies, default route, NAT rules

Export control will control the traffic between 1 outgoing zone and multiple incoming zones. Create the zones, access policies, default route, and NAT rules if required. For details see sections 4.12 Zones, 8.2.2 Create Access Policy, 6.2.1 L3 Unicast, and 5.2.1. Create SNAT Rule.

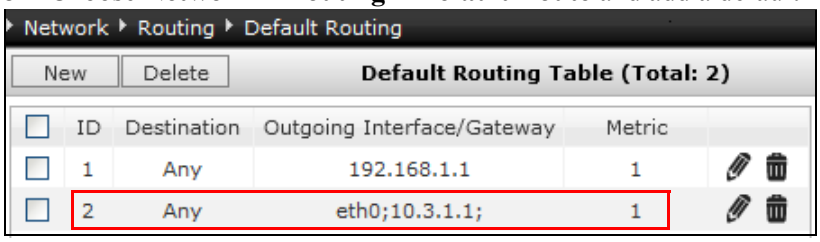
1. Choose **Network > Zones** and create zones (at least one outgoing zone for export control). In the following "LAN" is the incoming zone and "WAN" is the outgoing zone.



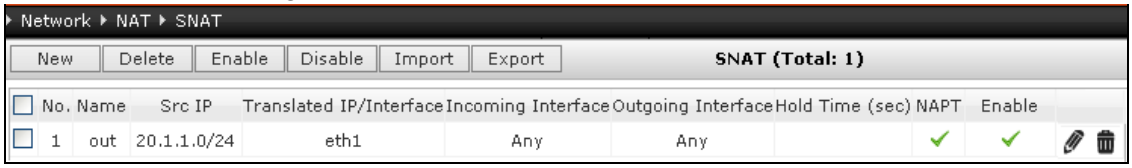
2. Choose **Firewall > Access Policies** and create access policies to allow outgoing traffic from the intranet to the Internet.



3. Choose **Network > Routing > Default Route** and add a default route as required.



4. If FGX works in Routing Mode, choose **Network > NAT > SNAT** and add a SNAT rule, such as the following:



10.2.1.2. Configure application control

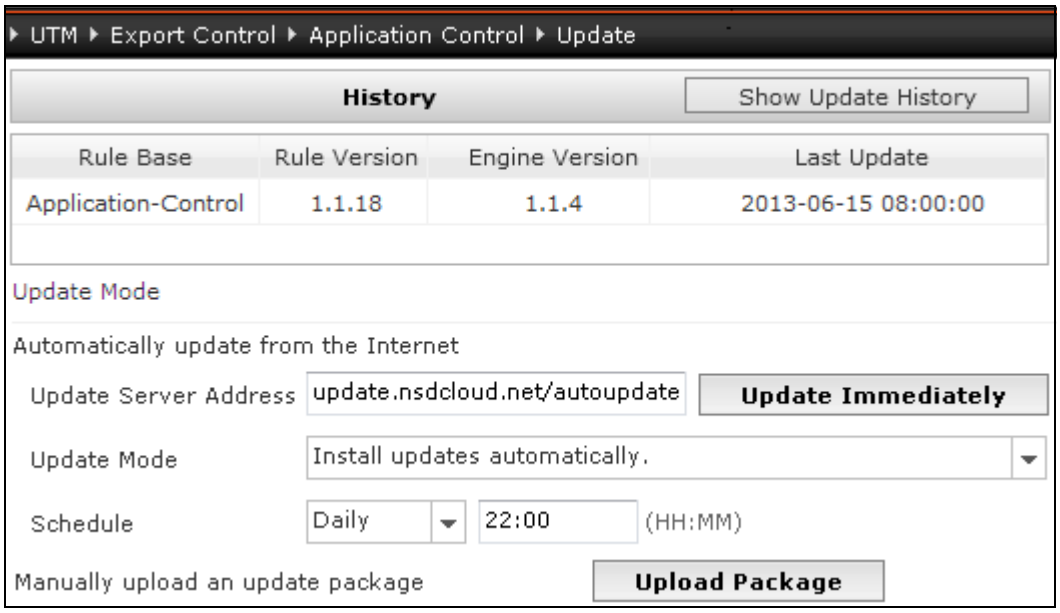
Application control configurations include:

- 10.2.1.2.1. Update application list
- 10.2.1.2.2. Create custom applications
- 10.2.1.2.3. Create application control profiles
- 10.2.1.2.4. Create application control policies

10.2.1.2.1. Update application list

For details see 10.5.2.2.4. (Application List) Update.

1. Choose **UTM > Export Control > Application Control > Update**.

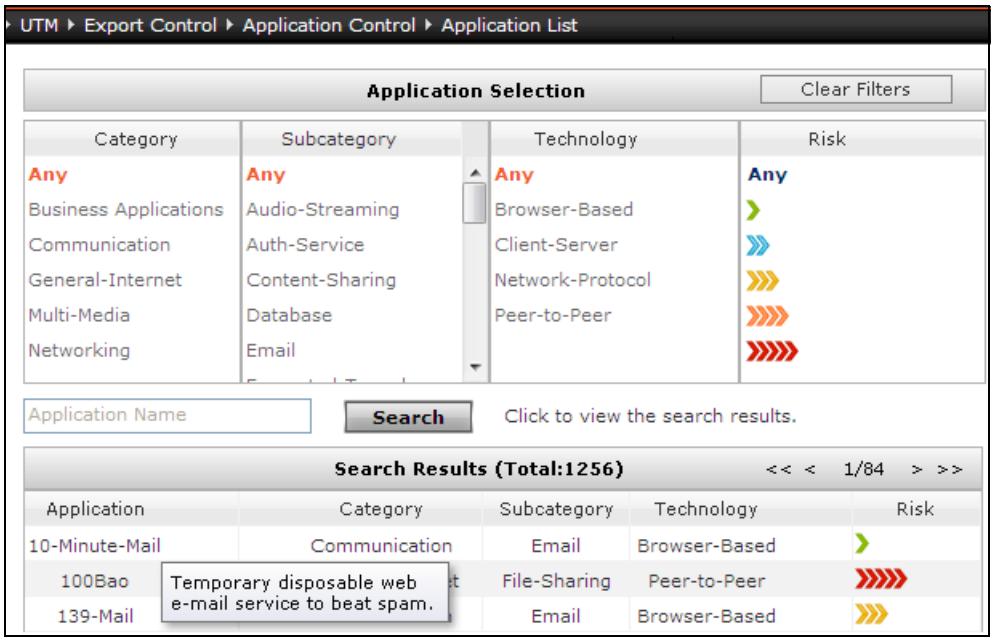


2. Update manually or from the Internet (if required).

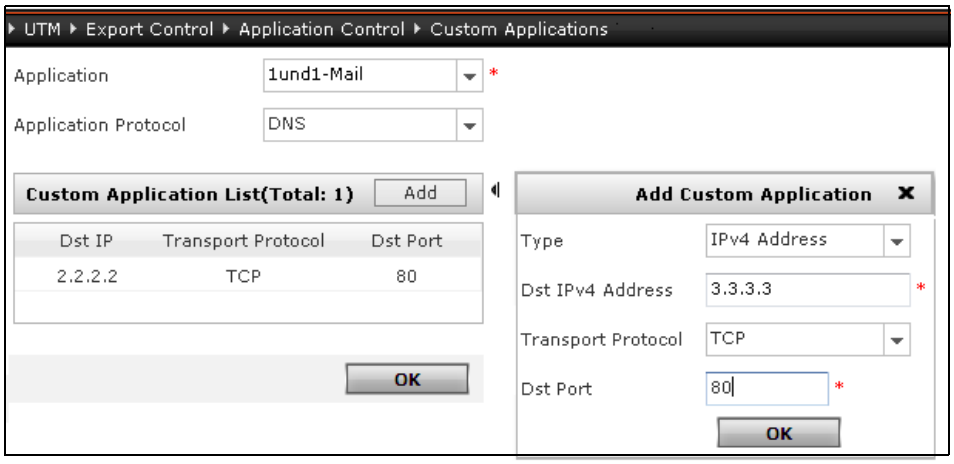
10.2.1.2.2. Create custom applications

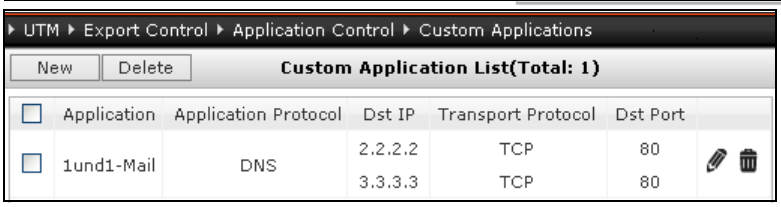
For details see 10.5.2.2.3. Application List and 10.5.2.2.2. Custom Applications.

1. Search for applications by category/technology/risk and/or name. Put your mouse cursor on an application name, the description of the application will be shown.



2. Customize any required applications. Customization basically restricts the IP address, protocol and port. The Application drop-down list supports automatic completion. For example, when you enter “G”, the drop-down list will list all applications whose names start with “G” and you can select the application you want.

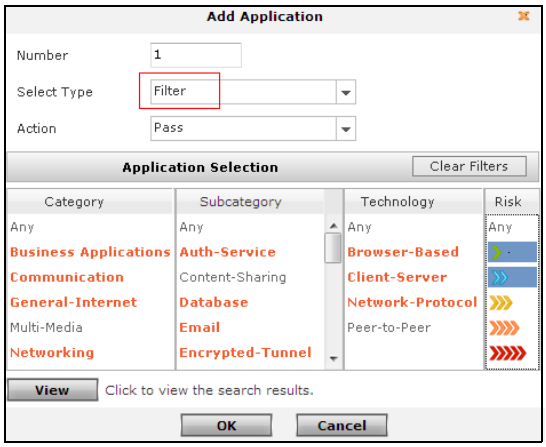


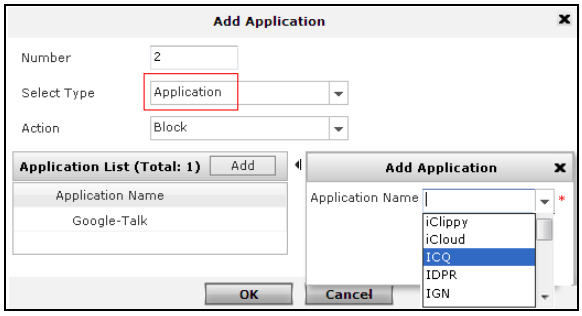


10.2.1.2.3. Create application control profiles

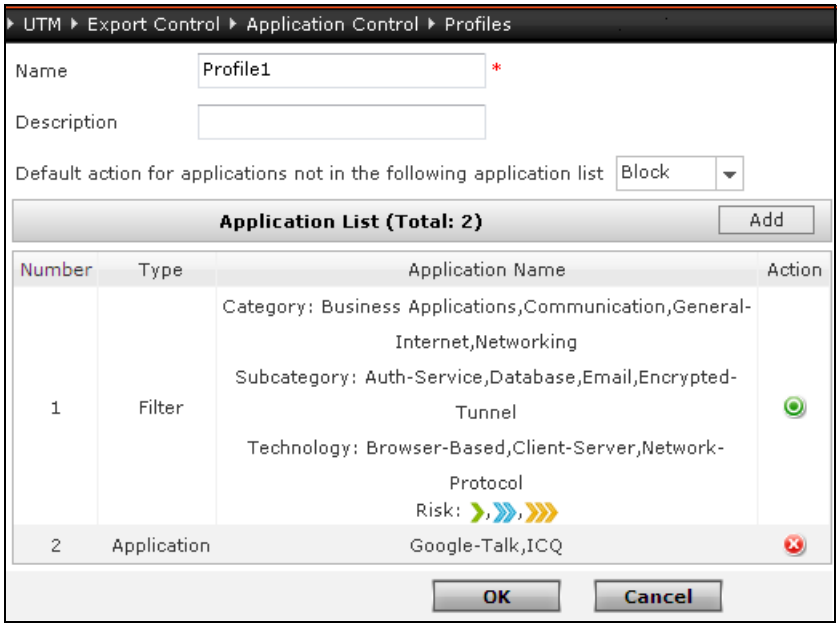
For details see 10.5.2.2.1. Application Control Profiles.

1. Choose **UTM > Export Control > Application Control > Profiles**.
2. Create application control profiles:
   a. Click **New** and add applications by filter or application name. The Application drop-down list supports automatic completion.

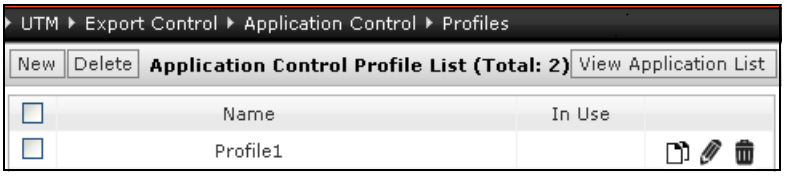




   b. Click **OK** to add the applications to the new profile.



   c. Click **OK** and view the new profile.You can click  to clone profiles.

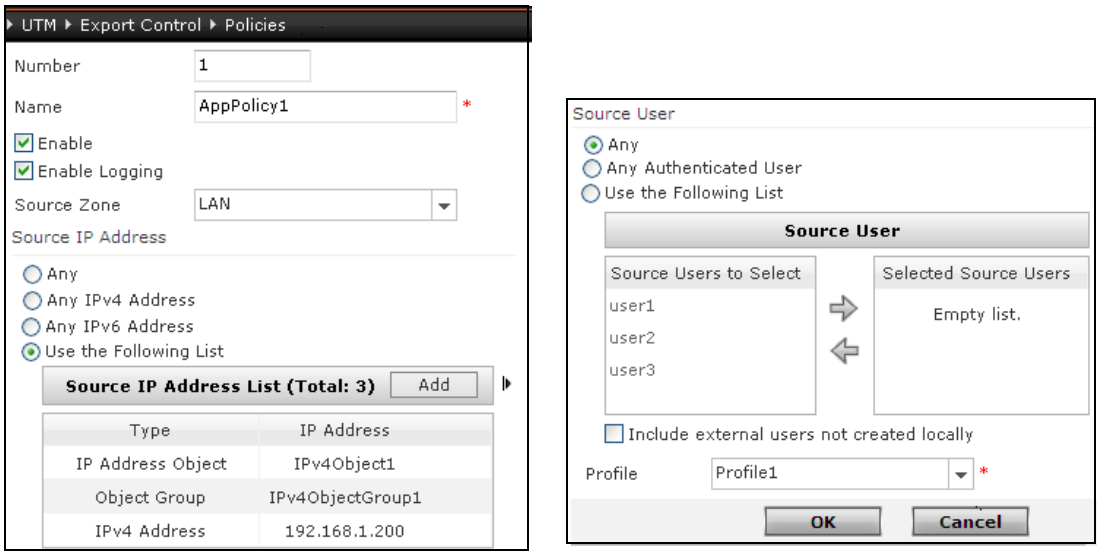


10.2.1.2.4. Create application control policies

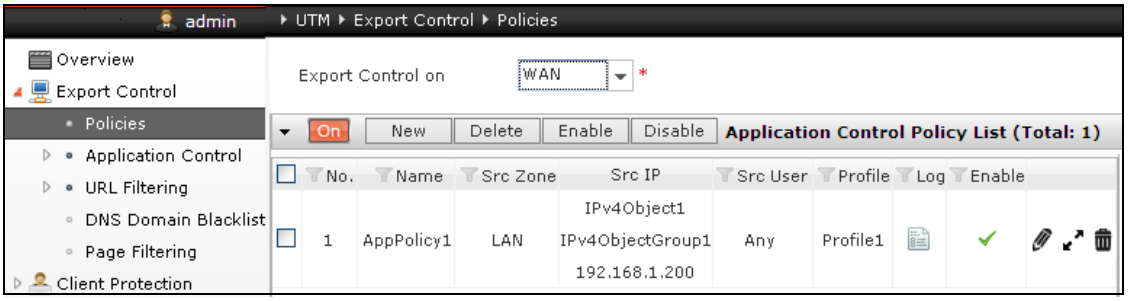
For details see 10.5.2.1.1. Application Control Policies.

1. Choose **UTM > Export Control > Policies**.
2. Select an outgoing zone and turn Application Control **ON**.

3. Click **Application Control** to expand the area, click **New**, and create an application control policy.



4. Click **OK**.



10.2.1.3. Configure (HTTP request) URL filtering

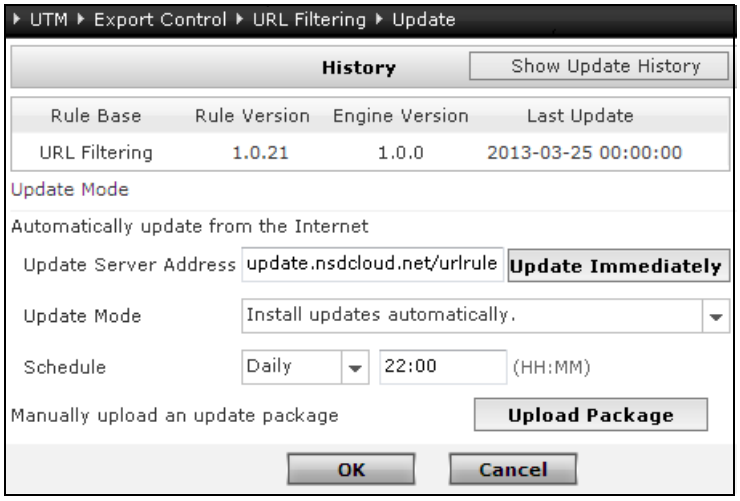
URL filtering configurations include:

- 10.2.1.3.1. Update URL filtering rule base
- 10.2.1.3.2. Configure URL filtering general settings
- 10.2.1.3.3. Create URL filtering profiles: Black/white lists
- 10.2.1.3.4. Create URL filtering profiles
- 10.2.1.3.5. Create URL filtering policies

10.2.1.3.1. Update URL filtering rule base

For details see 10.5.2.3.4. (URL Category) Update.

1. Choose **UTM > Export Control > URL Filtering > Update**.

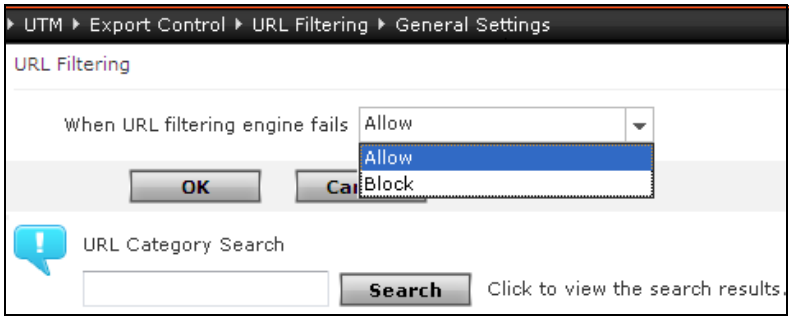


2. Update manually or from the Internet (if required).

10.2.1.3.2. Configure URL filtering general settings

For details see 10.5.2.3.1. (URL Filtering) General Settings.

1. Choose **UTM > Export Control > URL Filtering > General Settings**. Set the action for failure of URL filtering engine.

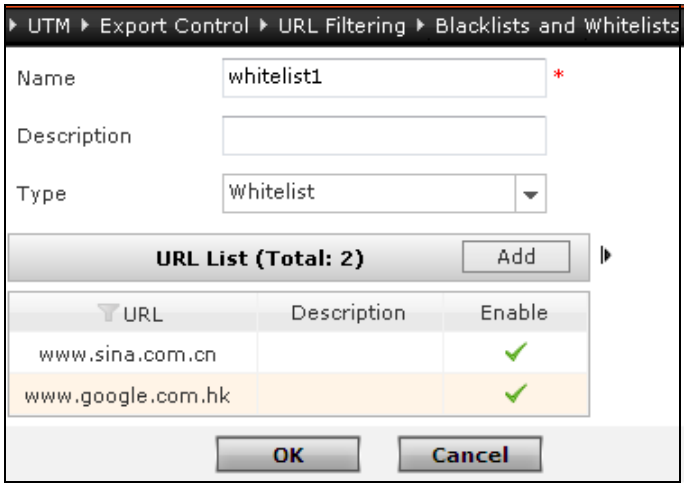


2. Click **OK**.
3. Search for URL category (if required).

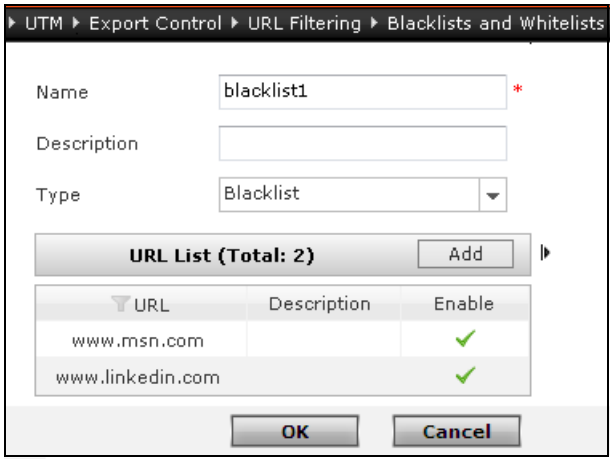
10.2.1.3.3. Create URL filtering profiles: Black/white lists

For details see 10.5.2.3.3. URL Blacklists & Whitelists.

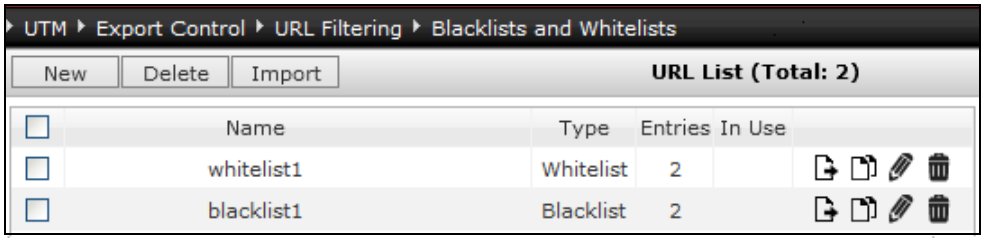
1. Choose **UTM > Export Control > URL Filtering > Blacklists and Whitelists**.
2. Click **New** and create a URL whitelist.



3. Click **OK**.
4. Click **New** and create a URL blacklist.



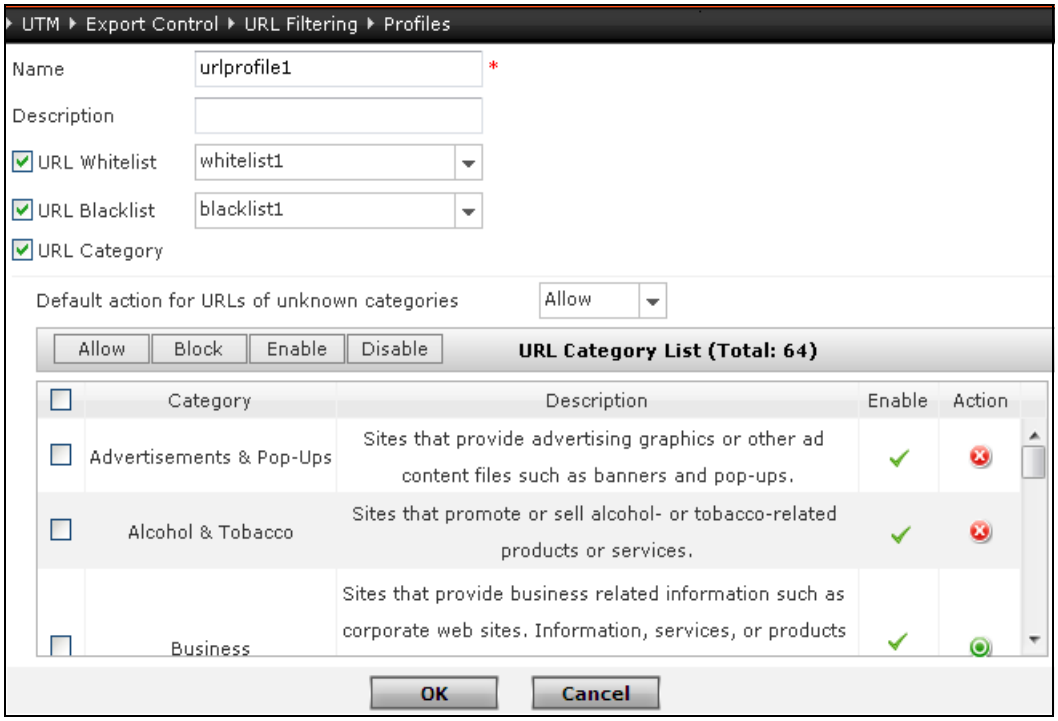
5. Click **OK** to view the created blacklists and whitelist. You can click  to clone URL lists.



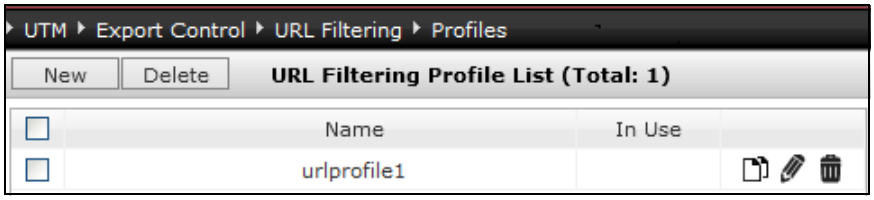
10.2.1.3.4. Create URL filtering profiles

For details see 10.5.2.3.2. (URL Filtering) Profiles.

1. Choose **UTM > Export Control > URL Filtering > Profiles**.
2. Click **New** and create a URL filtering profile.



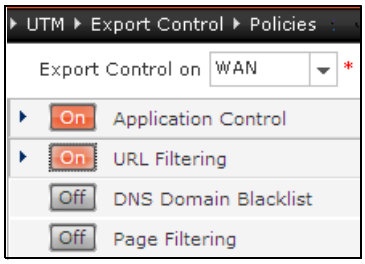
3. Click **OK** to view the created URL filtering profiles. You can click  to clone profiles.



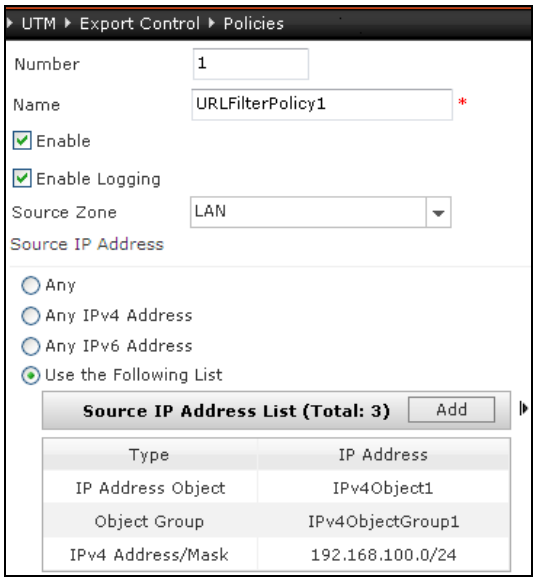
10.2.1.3.5. Create URL filtering policies

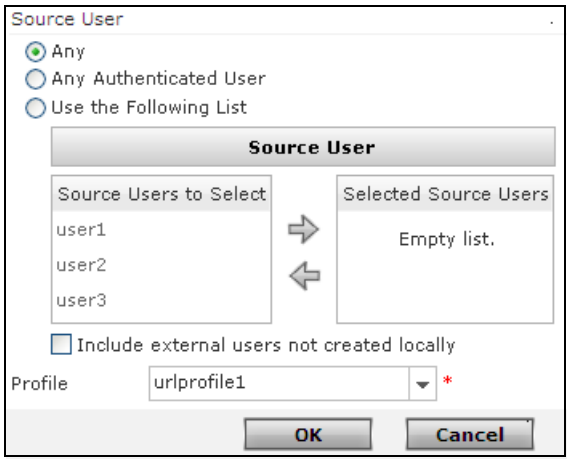
For details see 10.5.2.1.2. URL Filtering Policies.

1. Choose **UTM > Export Control > Policies**.
2. Select an outgoing zone and turn **ON** URL filtering.



3. Click **URL Filtering** to expand the area. Click **New** and create a URL filtering policy.



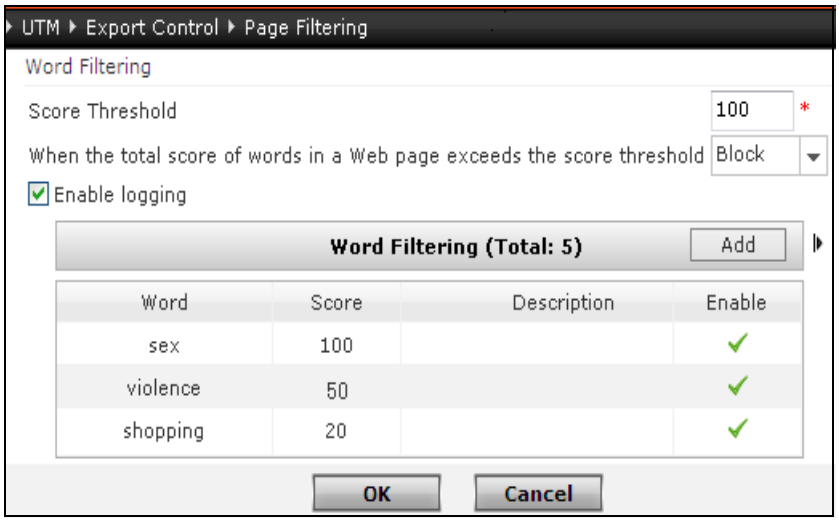


4. Click **OK**.

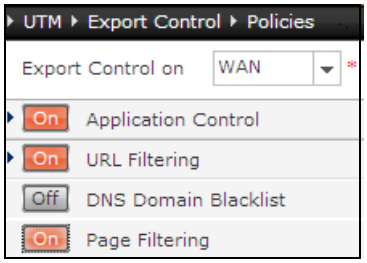
10.2.1.4. Configure (HTTP response) page filtering

For details see 10.5.2.5. Page Filtering.

1. Choose **UTM > Export Control > Page Filtering**.
2. Configure the page filtering settings to block HTTP response web pages comprising specified key words.



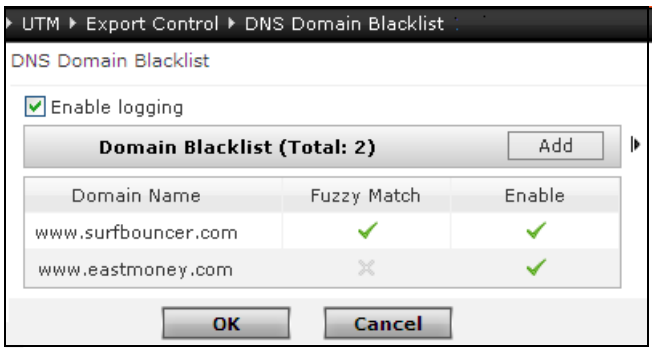
3. Click **OK**.
4. Choose **UTM > Export Control > Policies**.
5. Select an outgoing zone and turn **ON** page filtering.



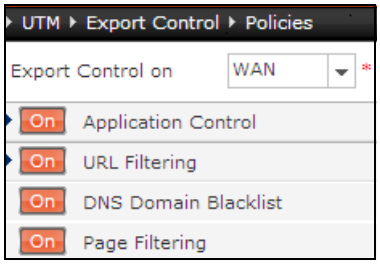
10.2.1.5. Configure DNS domain blacklist

For details see 10.5.2.4. DNS Domain Blacklist.

1. Choose **UTM > Export Control > DNS Domain Blacklist**.
2. Configure the DNS domain blacklist.



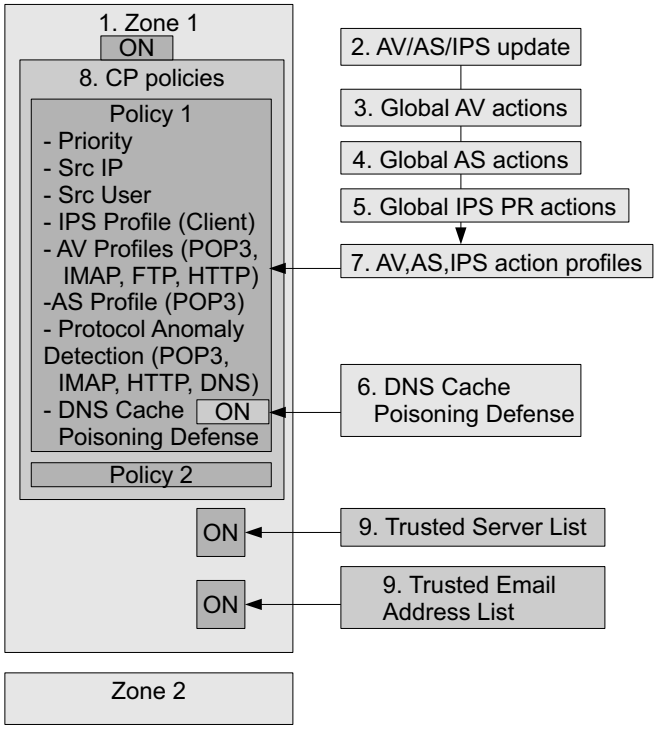
3. Click **OK**.
4. Choose **UTM > Export Control > Policies**.
5. Select an outgoing zone and turn **ON** DNS domain blacklist.



10.2.2. Client protection

Client protection configuration steps are shown below.

Figure 40 Client Protection Configuration Steps



Basic setup:

- 10.2.2.1. Create zones, access policies, default route, NAT rules

General settings (AV/AS/IPS update):

- 10.2.2.2. Update AV, AS, IPS rules

Global actions:

- 10.2.2.3. Configure global AV actions (trusted list, action when virus detected, heuristic, scan limits)
- 10.2.2.4. Configure global AS actions (allow/block list, spam word list, scan)
- 10.2.2.5. Configure IPS client SMTP, POP3, IMAP, DNS protocol restriction
- 10.2.2.6. Configure DNS CPD global actions

Action profiles:

- 10.2.2.7. Create AV, AS, IPS action profiles

Destination zone action / policies:

- 10.2.2.8. Create client protection policies
- 10.2.2.9. Create trusted server / email list

10.2.2.1. Create zones, access policies, default route, NAT rules

1. Choose **Network > Zones** and create required client protection zones. See 4.12 Zones.
2. Choose **Firewall > Access Policies** and create access policies. See 8.2.2 Create Access Policy.
3. Choose **Network > Routing > Default Route** and modify the default route. See 6.2.1 L3 Unicast.
4. If FGX works in Routing Mode, choose **Network > NAT > SNAT** and add an SNAT rule. See 5.2.1. Create SNAT Rule.

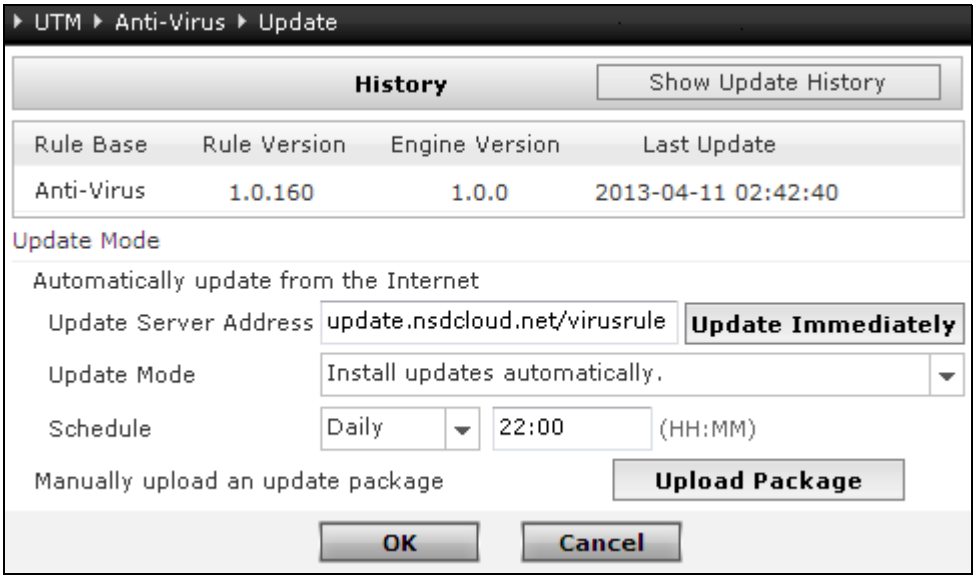
10.2.2.2. Update AV, AS, IPS rules

- 10.2.2.2.1. Update anti-virus rules
- 10.2.2.2.2. Update anti-spam rules
- 10.2.2.2.3. Update attack signature rules

10.2.2.2.1. Update anti-virus rules

Update the anti-virus rule database. For details see 10.5.5.6. (Anti-Virus Rule) Update.

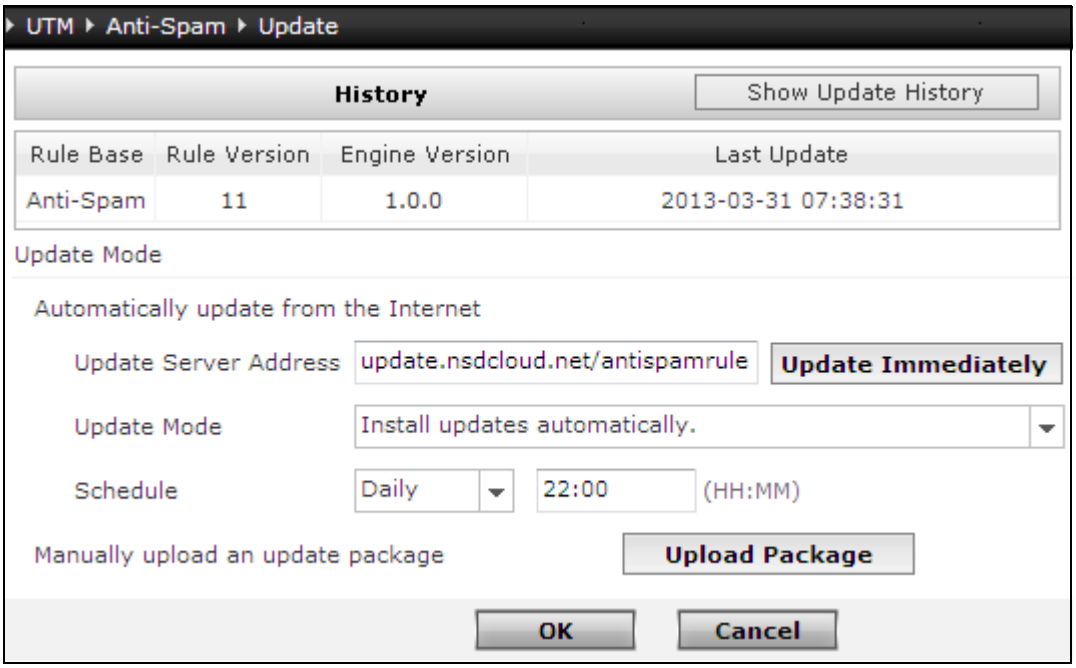
1. Choose **UTM > Anti-Virus > Update**.
2. Update manually or from the Internet (if required).



10.2.2.2.2. Update anti-spam rules

Update the anti-spam rule database. For details see 10.5.6.6. (Anti-Spam Rule) Update.

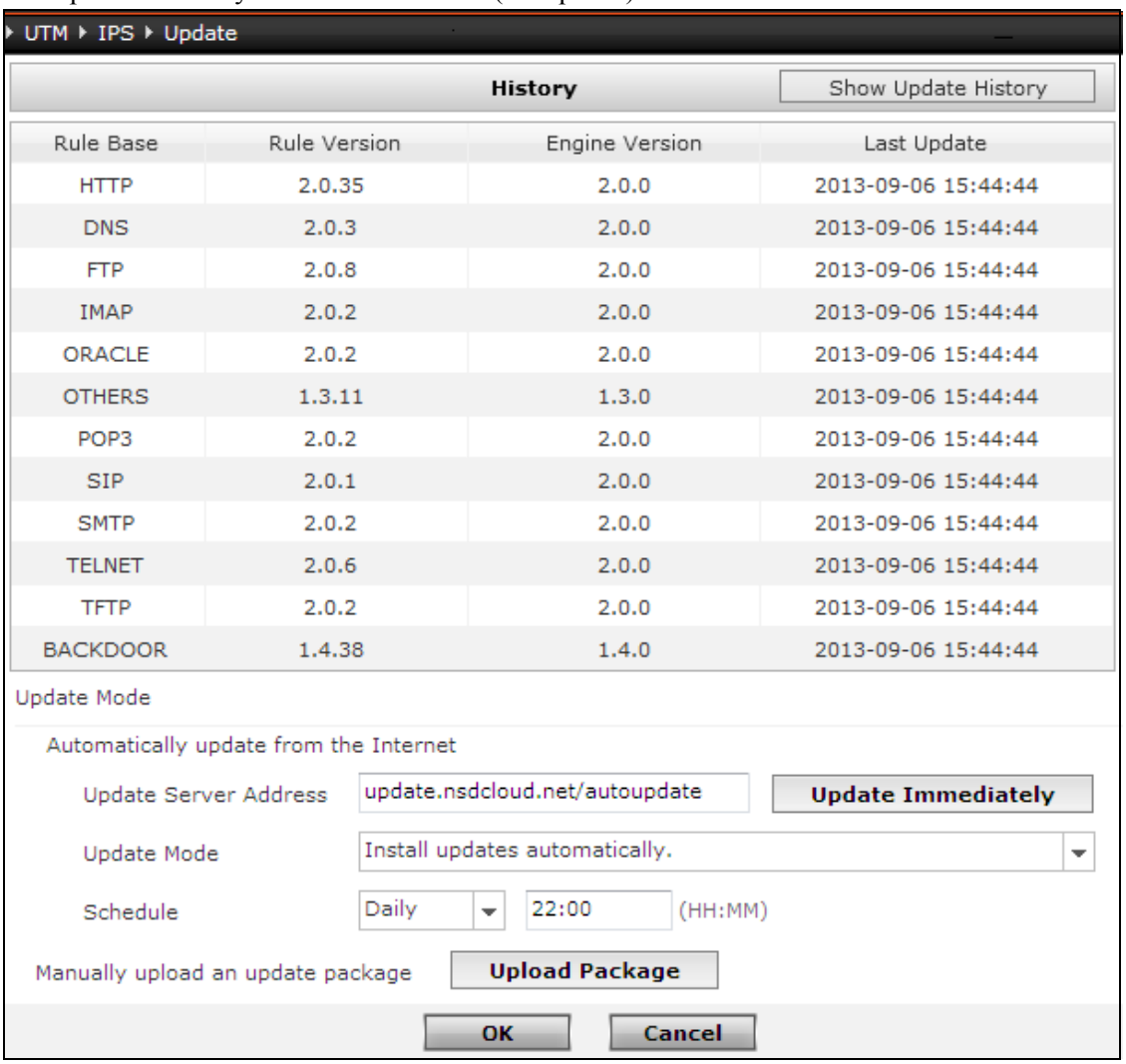
1. Choose **UTM > Anti-Spam > Update**.
2. Update manually or from the Internet (if required).



10.2.2.2.3. Update attack signature rules

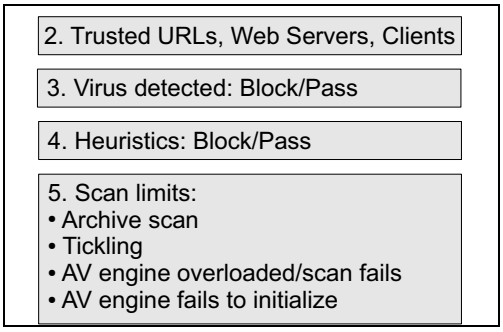
Update the attack signature rule database. For details see 10.5.7.3. (Attack Signature Rule) Update.

1. Choose **UTM > IPS > Update**.
2. Update manually or from the Internet (if required).



10.2.2.3. Configure global AV actions (trusted list, action when virus detected, heuristic, scan limits)

The following diagram provides an overview of anti-virus configuration.

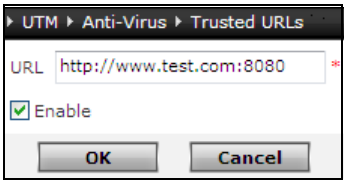


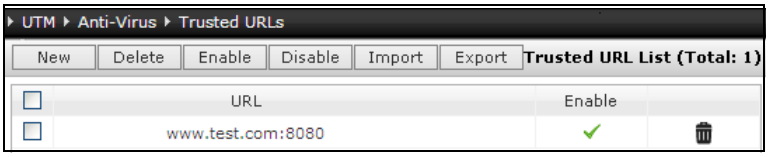
- 10.2.2.3.1. Create AV trusted URLs, web servers, clients
- 10.2.2.3.2. Set AV engine general settings

10.2.2.3.1. Create AV trusted URLs, web servers, clients

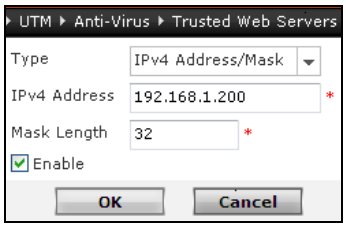
For details see 10.5.5.2. Trusted URLs, 10.5.5.3. Trusted Web Servers, and 10.5.5.4. Trusted Clients.

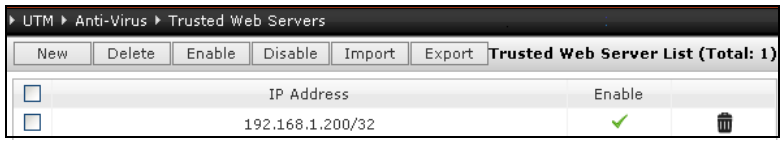
1. Select **UTM > Anti-virus > Trusted URLs**.



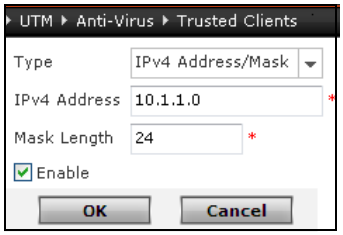


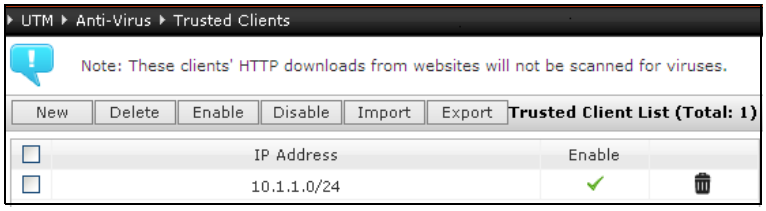
2. Select **UTM > Anti-Virus > Trusted Web Servers**.





3. Select **UTM > Anti-Virus > Trusted Clients**.

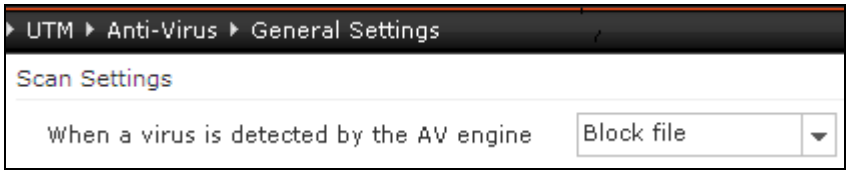




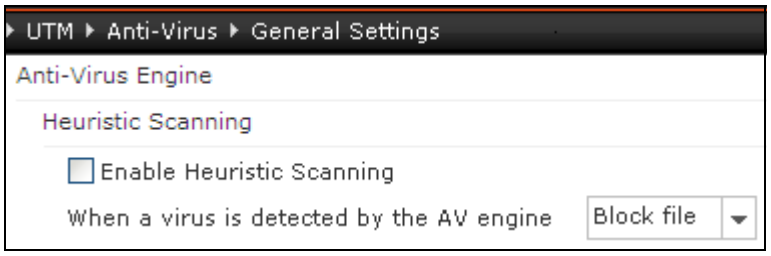
10.2.2.3.2. Set AV engine general settings

For details see 10.5.6.1. (Anti-Spam) General Settings.

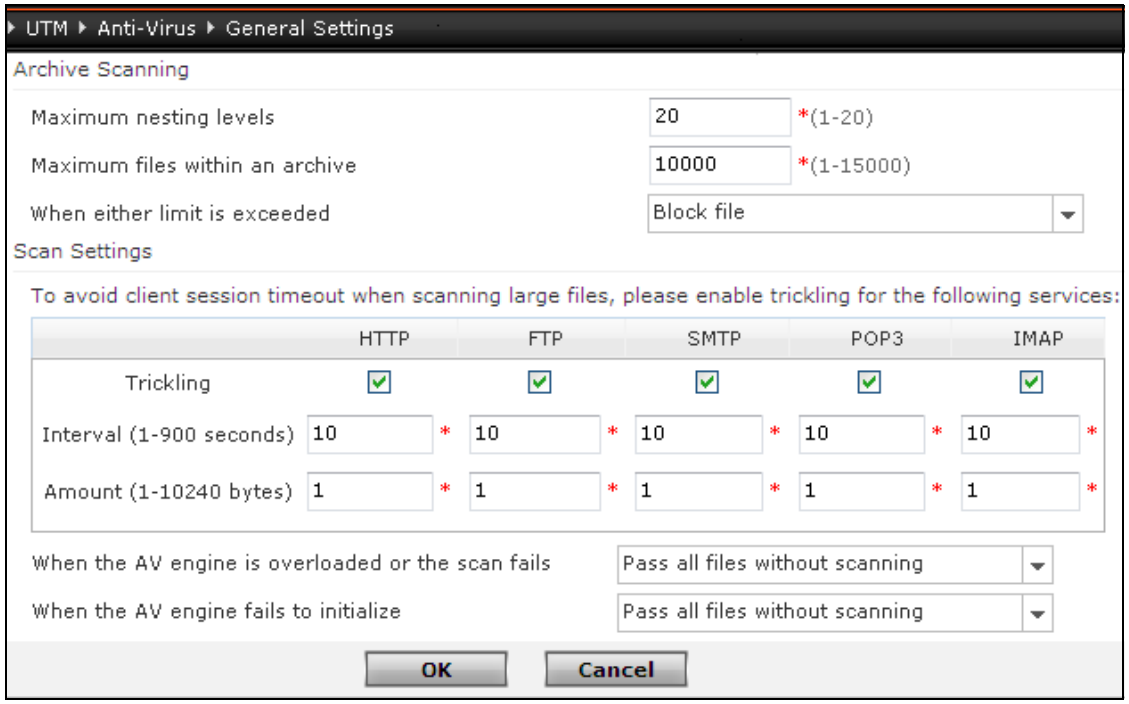
1. Select **UTM > Anti-virus > General Settings**.
2. Set action for situations when virus is found.



3. Set heuristics scan.

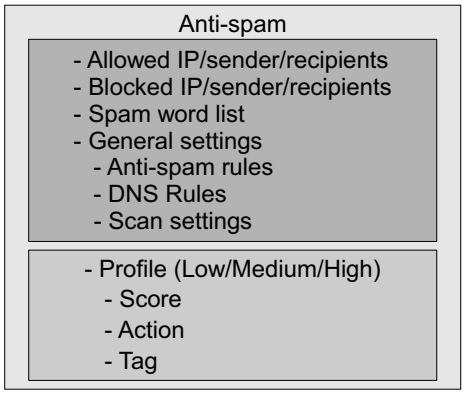


4. Set archive scan, trickling, and actions when AV engine is overloaded or fails.



10.2.2.4. Configure global AS actions (allow/block list, spam word list, scan)

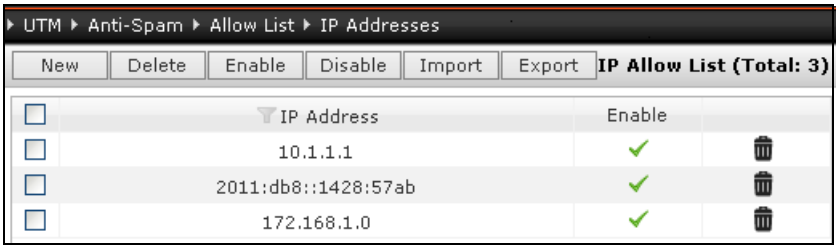
The following diagram provides an overview of anti-spam configuration.



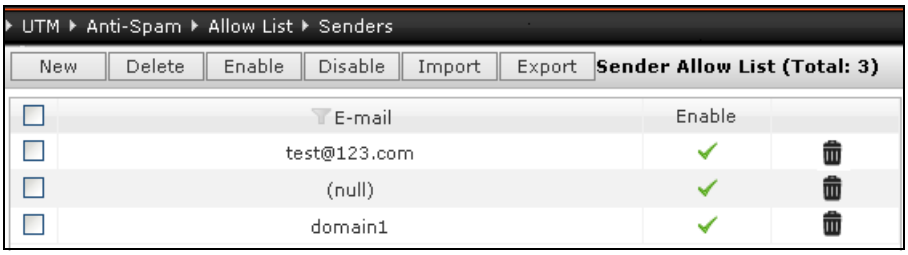
- 10.2.2.4.1. Create IP/sender/recipient allow/block lists
- 10.2.2.4.2. Configure custom spam word list
- 10.2.2.4.3. Set anti-spam rules (general settings)
- 10.2.2.4.4. Set scan timeout/failure actions

10.2.2.4.1. Create IP/sender/recipient allow/block lists

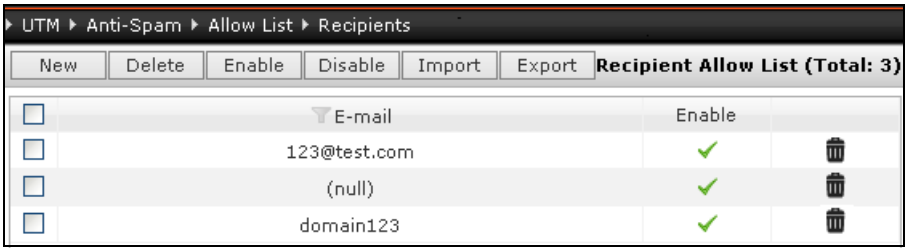
1. Select **UTM > Allow List > IP Addresses** and add allowed IP addresses.



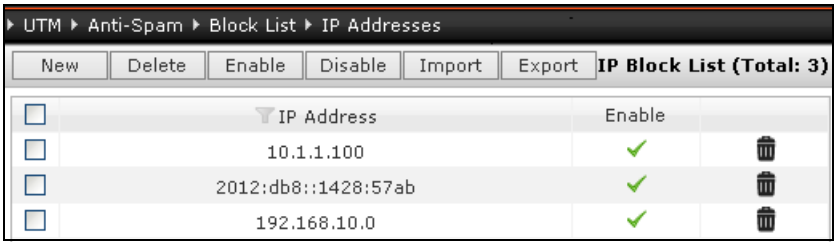
2. Select **UTM > Allow List > Senders** and add allowed senders.



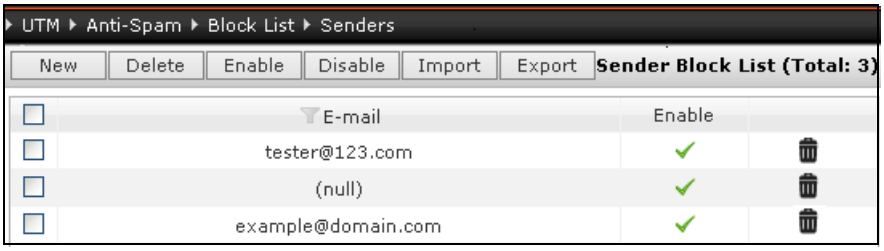
3. Select **UTM > Allow List > Recipients** and add allowed recipients.



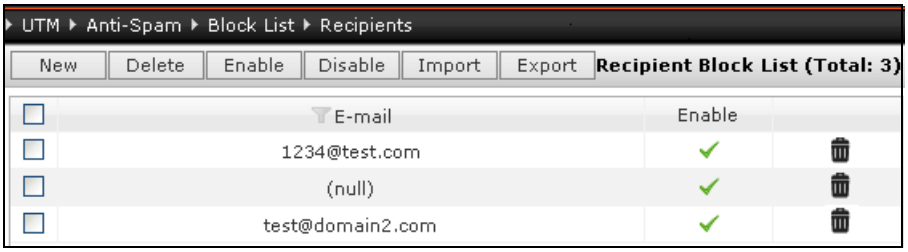
4. Select **UTM > Block List > IP Addresses** and add blocked IP addresses.



5. Select **UTM > Block List > Senders** and add blocked senders.

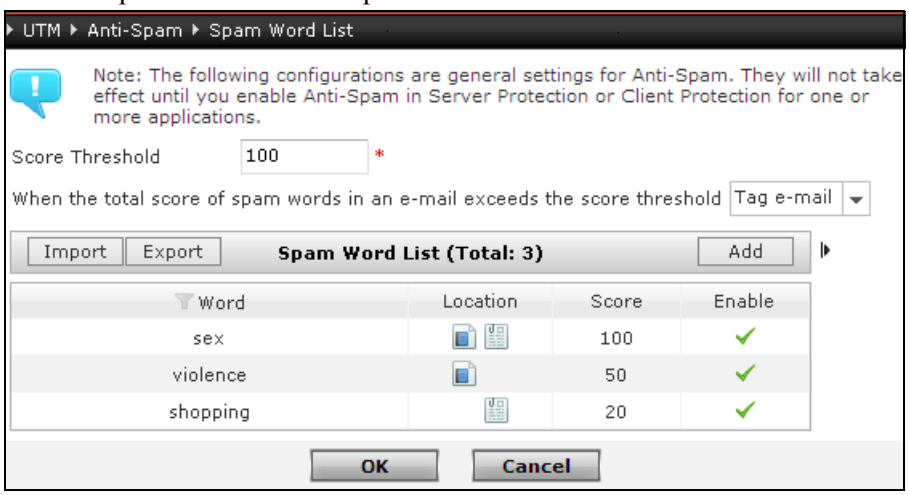


6. Select **UTM > Block List > Recipients** and add blocked recipients.



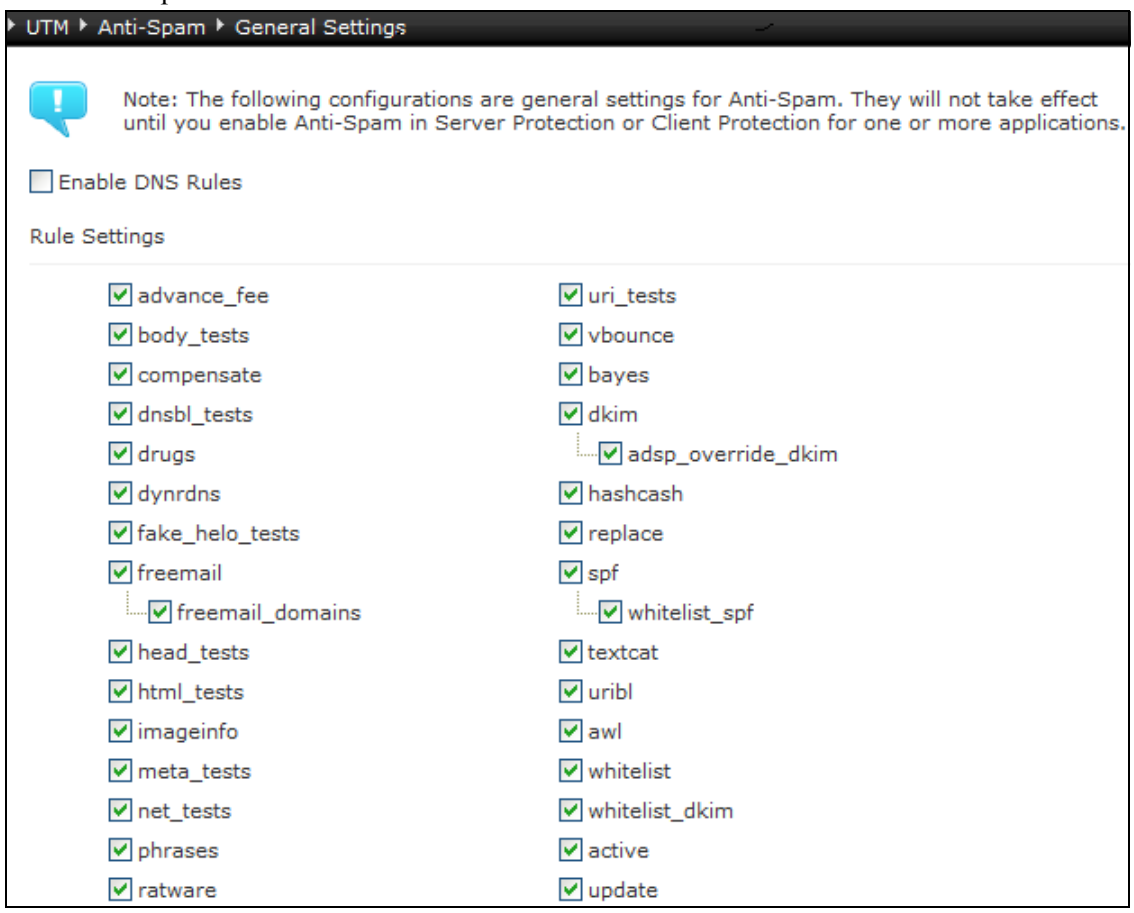
10.2.2.4.2. Configure custom spam word list

1. Select **UTM > Anti-Spam > Spam Word List**.
2. Add spam words into the spam word list.



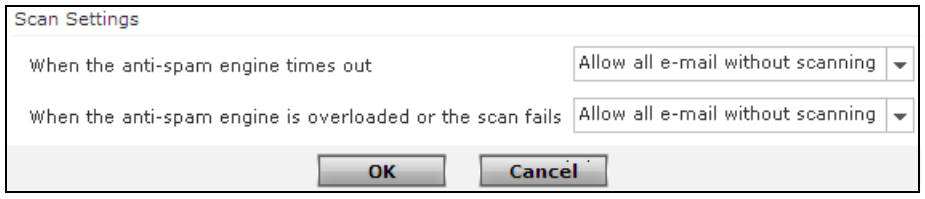
10.2.2.4.3. Set anti-spam rules (general settings)

1. Select **UTM > Anti-Spam > General Settings**.
2. Set anti-spam rules.



10.2.2.4.4. Set scan timeout/failure actions

3. Set actions for situations when scan times out or fails.



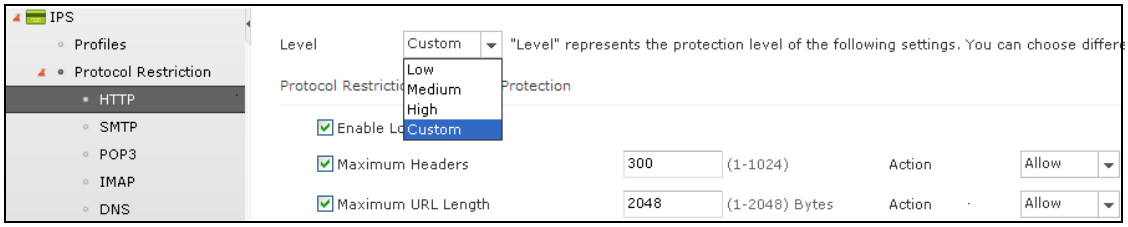
4. Click **OK**.

10.2.2.5. Configure IPS client SMTP, POP3, IMAP, DNS protocol restriction

The following diagram shows basic IPS protocol restriction components.

Protocol restriction
- Type (HTTP, SMTP, POP3, IMAP, DNS)
- Level (Low, Medium, High, Custom)
  ONLY the selected level is activated.
- Server PR settings (HTTP, SMTP, POP3, IMAP, DNS)
- Client PR settings (SMTP, POP3, IMAP, DNS)

1. Choose the protocol restriction type (SMTP, POP3, IMAP and DNS for client IPS profiles), for example, **UTM > IPS > Protocol Restriction > SMTP**.
2. Select the level (for example High).
3. Set the parameters for client protection.



4. Click **OK**.

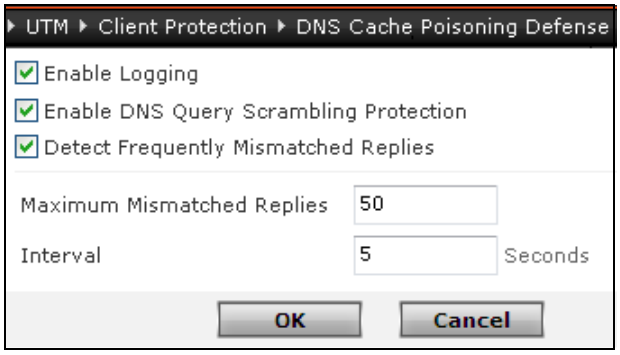
Note: The level you last selected is the enabled level.

5. Enable protocol restriction (for example, SMTP) in client IPS profiles.

10.2.2.6. Configure DNS CPD global actions

Set DNS cache poisoning defense (CPD). For details see 10.5.3.4. DNS Cache Poisoning Defense.

1. Choose **UTM > Client Protection > DNS Cache Poisoning Defense**.



2. Click **OK**.

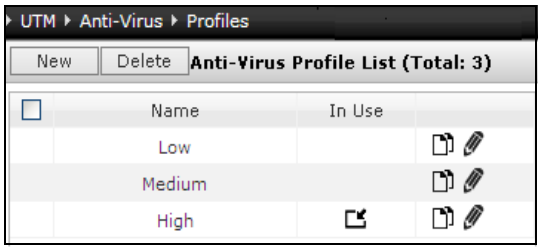
10.2.2.7. Create AV, AS, IPS action profiles

- 10.2.2.7.1. View default anti-virus profiles
- 10.2.2.7.2. Customize and specify anti-virus profiles
- 10.2.2.7.3. View default anti-spam profiles
- 10.2.2.7.4. Customize and specify anti-spam profiles
- 10.2.2.7.5. View default IPS profiles (overview)
- 10.2.2.7.6. Create custom IPS profiles
- 10.2.2.7.7. Enable / configure protocol restriction

10.2.2.7.1. View default anti-virus profiles

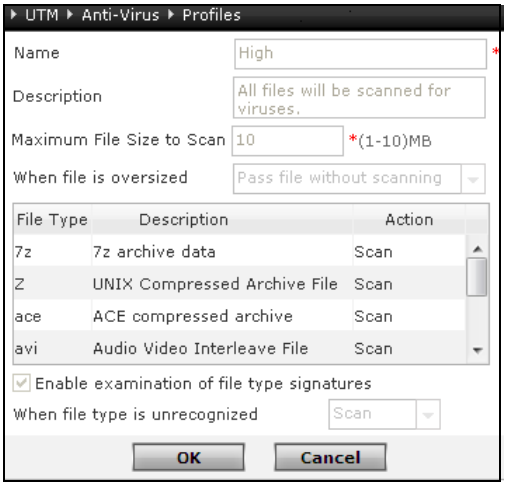
For details see Table 205.

1. Select **UTM > Anti-Virus > Profiles**.
2. View default profiles.



Note: There are 3 default AV profiles (Low, Medium and High) and a maximum of 29 custom AV profiles.

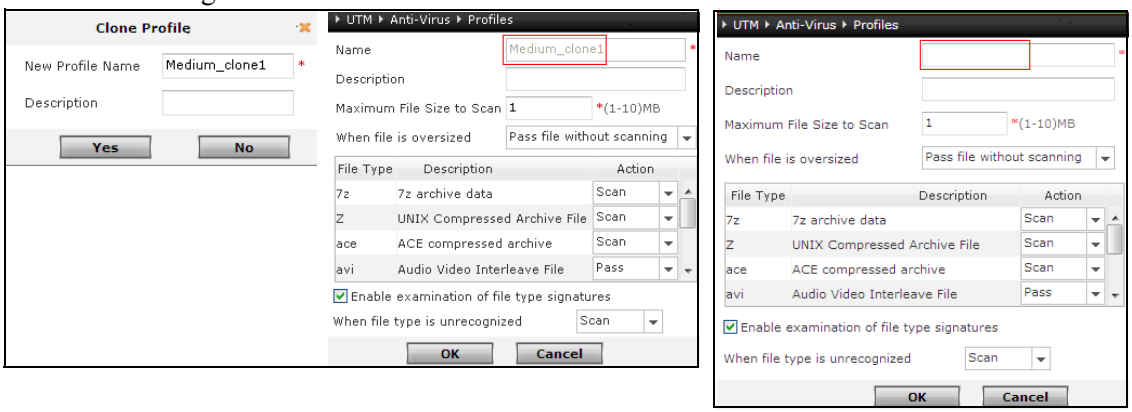
3. Click a default anti-virus profile to view the settings.



10.2.2.7.2. Customize and specify anti-virus profiles

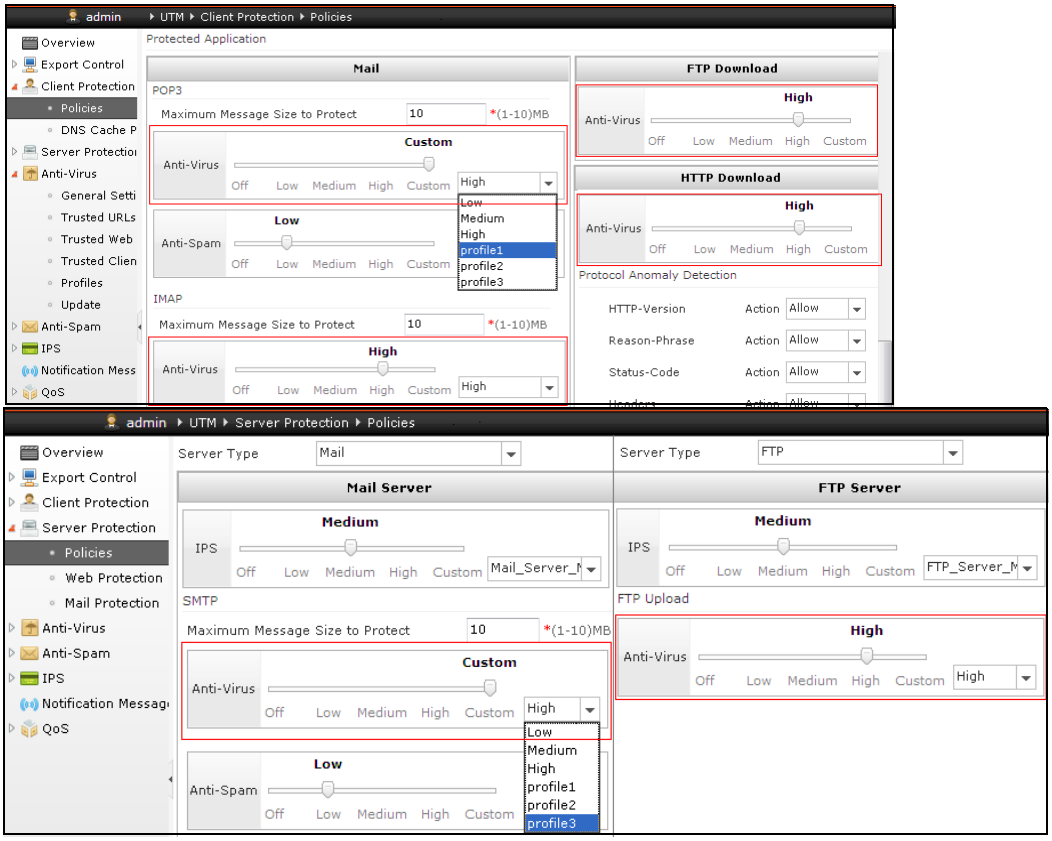
For details see 10.5.5.5. (Anti-Virus) Profiles.

1. Click or click **New**, and modify the settings. If you click **New** to create profile, the default settings are the same as Medium.



Note: The profile names are used as the unique identifier to select the profile in client and server protection policies.

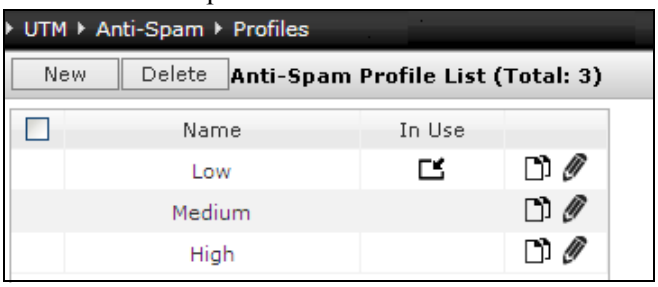
2. Specify anti-virus profiles in client/server protection policies.



10.2.2.7.3. View default anti-spam profiles

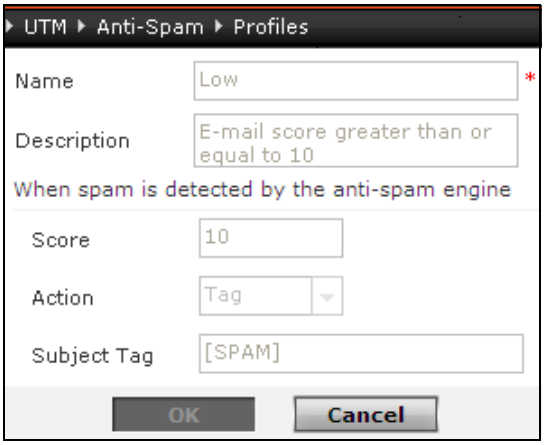
For details see 10.5.6.5. (Anti-Spam) Profiles.

1. Select **UTM > Anti-Spam > Profiles**.
2. View default profiles.



Note: There are 3 default AS profiles (Low, Medium and High) and a maximum of 29 custom AS profiles.

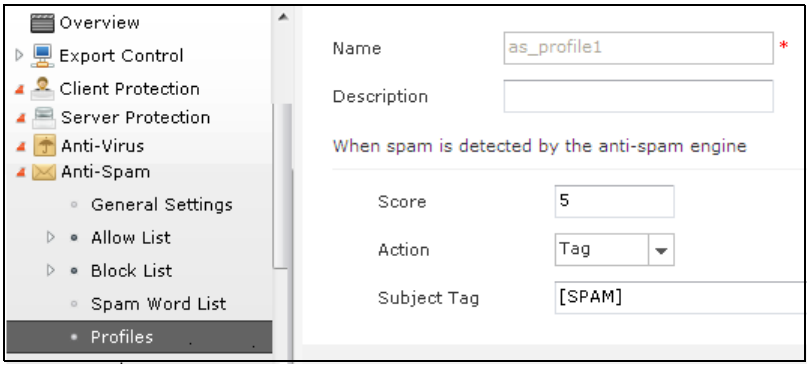
3. Click a default anti-spam profile to view the settings.



10.2.2.7.4. Customize and specify anti-spam profiles

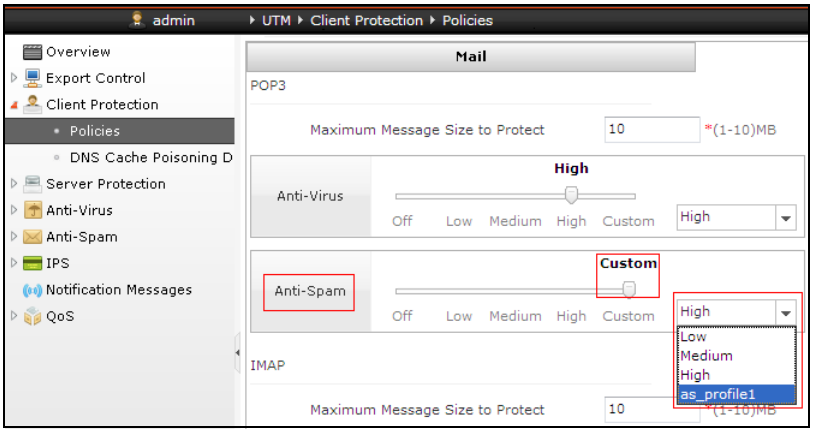
- Profile (Low/Medium/High)
  - Score
  - Action
  - Tag

4. Click or click **New** to create a profile, and set the score and action for the spam. If you click **New** to create a profile, the default settings are the same as Medium.



The profile names are used as the unique identifier to select the profile in client and server protection policies.

5. Specify anti-spam profiles in client/server protection policies.



10.2.2.7.5. View default IPS profiles (overview)

1. Select **UTM > IPS > Profiles**.
2. View the default IPS profiles.

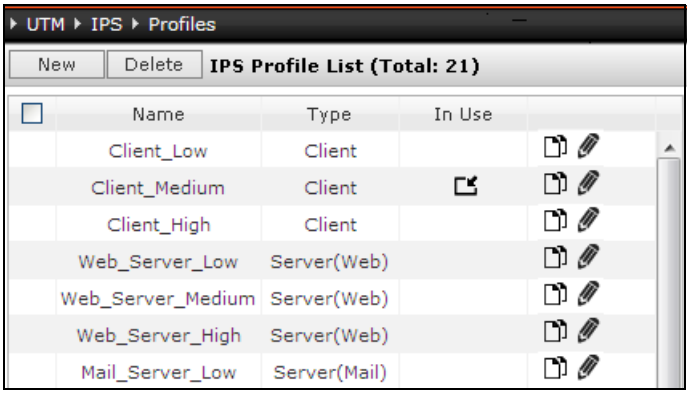


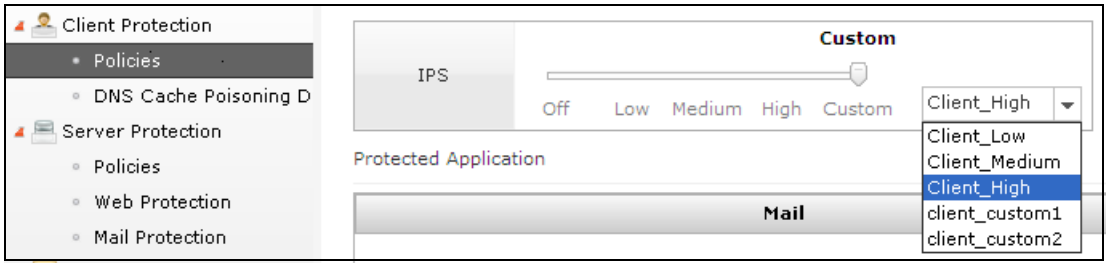
Table 169 Default IPS profiles

Client / server	Server type	Low priority name	Medium priority name	High priority name
Client		Client_Low	Client_Medium	Client_High
Server	Web	Server_Web_Low	Server_Web_Medium	Server_Web_High
Server	Mail	Server_Mail_Low	Server_Mail_Medium	Server_Mail_High
Server	FTP	Server_FTP_Low	Server_FTP_Medium	Server_FTP_High
Server	Telnet	Server_Telnet_Low	Server_Telnet_Medium	Server_Telnet_High
Server	DNS	Server_DNS_Low	Server_DNS_Medium	Server_DNS_High
Server	Other	Server_Other_Low	Server_Other_Medium	Server_Other_High

3. Click a default profile name to view the settings.

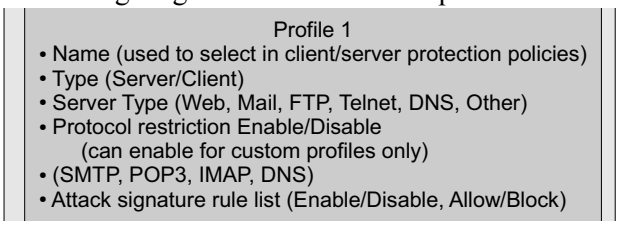
Put your mouse cursor on a parameter in the rule list, a ▼ icon will appear and you can click it to set the parameters you want to display.

4. The following shows how the profile is selected in client and server protection.

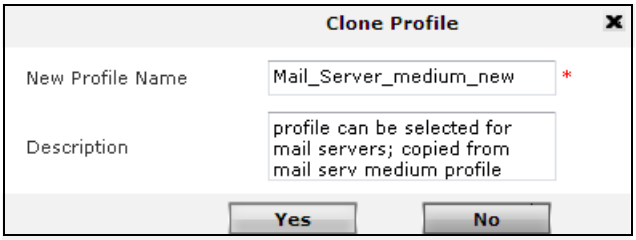


10.2.2.7.6. Create custom IPS profiles

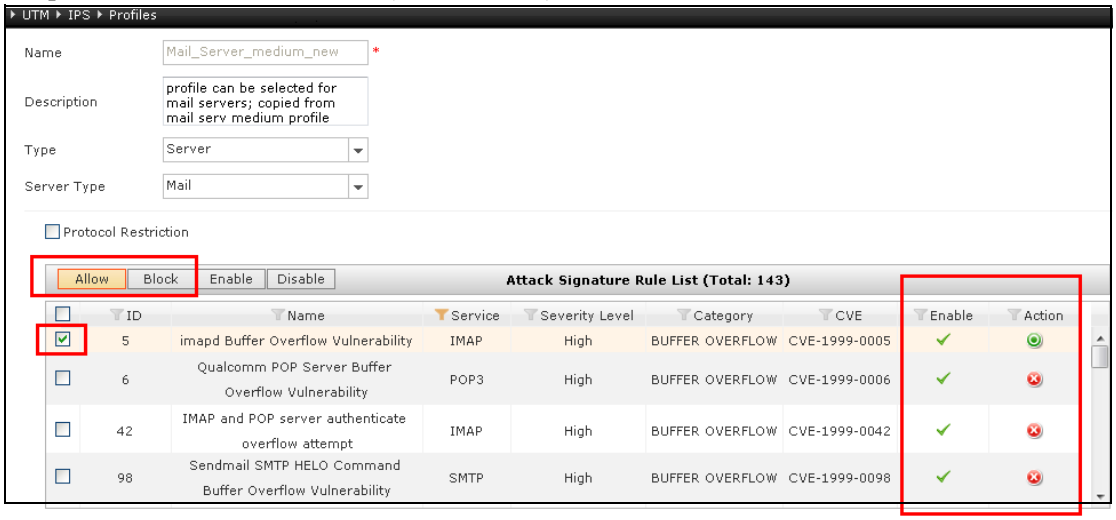
The following diagram shows basic IPS protocol restriction components.



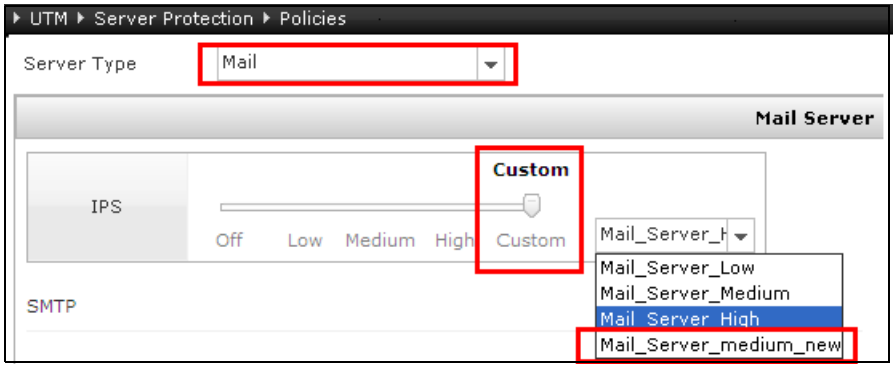
5. Click **Clone** to copy a profile or click **New** to create a new one.



6. In the **Attack Signature Rule List**, enable the attack signature rules that the profile performs and set the actions (Allow/Block).

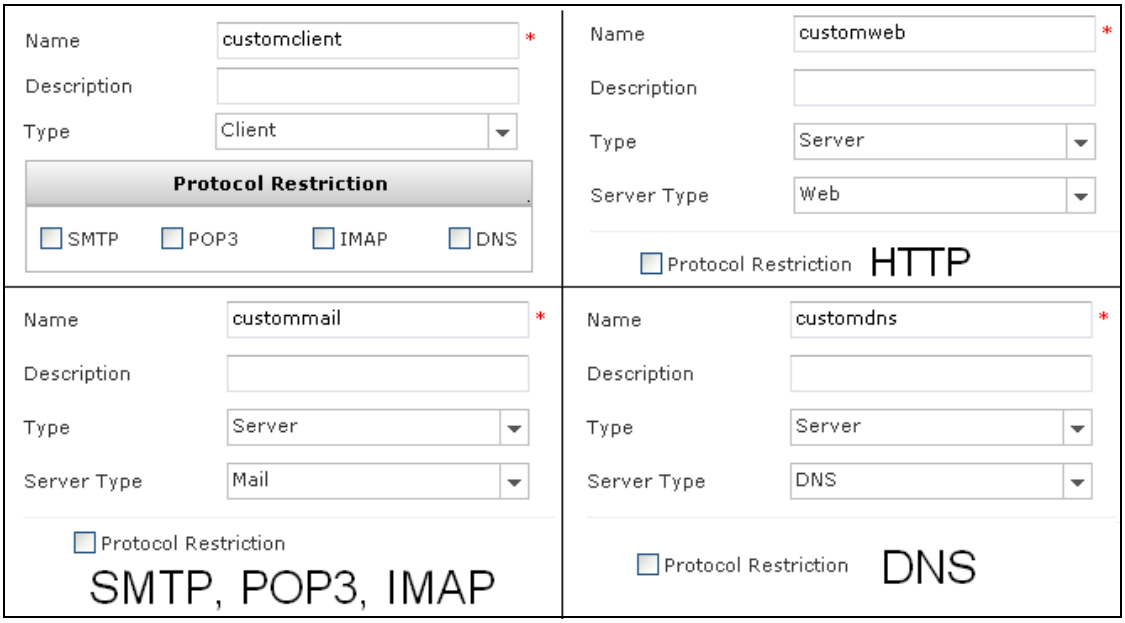


7. Profile names are used as the unique identifier to select the profile in client and server protection policies.



10.2.2.7.7. Enable / configure protocol restriction

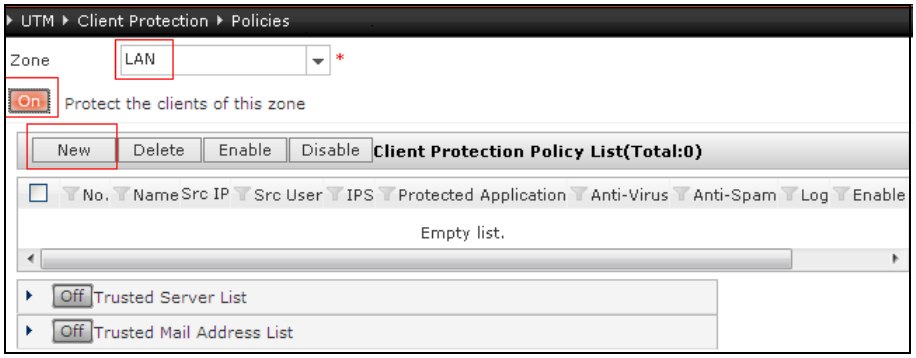
8. For certain types you can enable protocol restriction (note that you can only enable this for a custom profile).



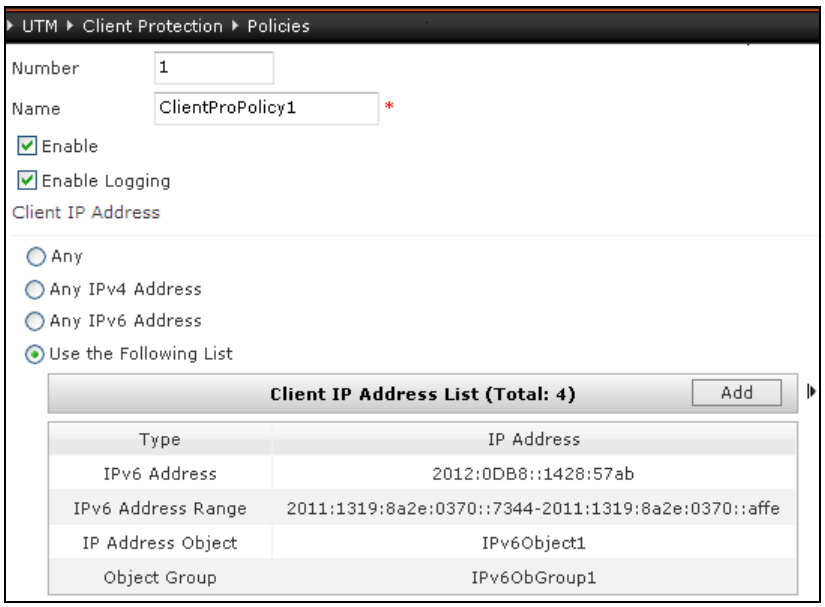
10.2.2.8. Create client protection policies

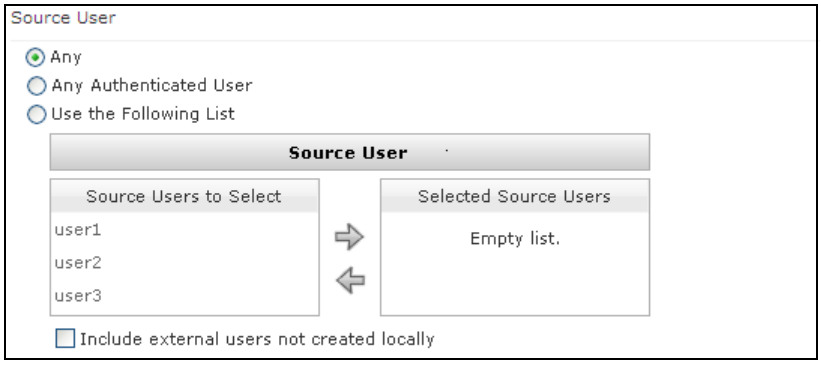
Create client protection policies. For details see 10.5.3. Client Protection.

1. Choose **UTM > Client Protection > Policies**.
2. Select an incoming zone for client protection and turn client protection policies **ON**.

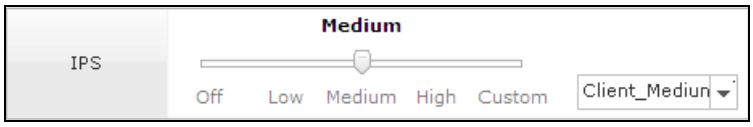


3. Click **New** in the **Client Protection Policy List** and create a client protection policy:
   a. Enter the basic information and set the client IP address.

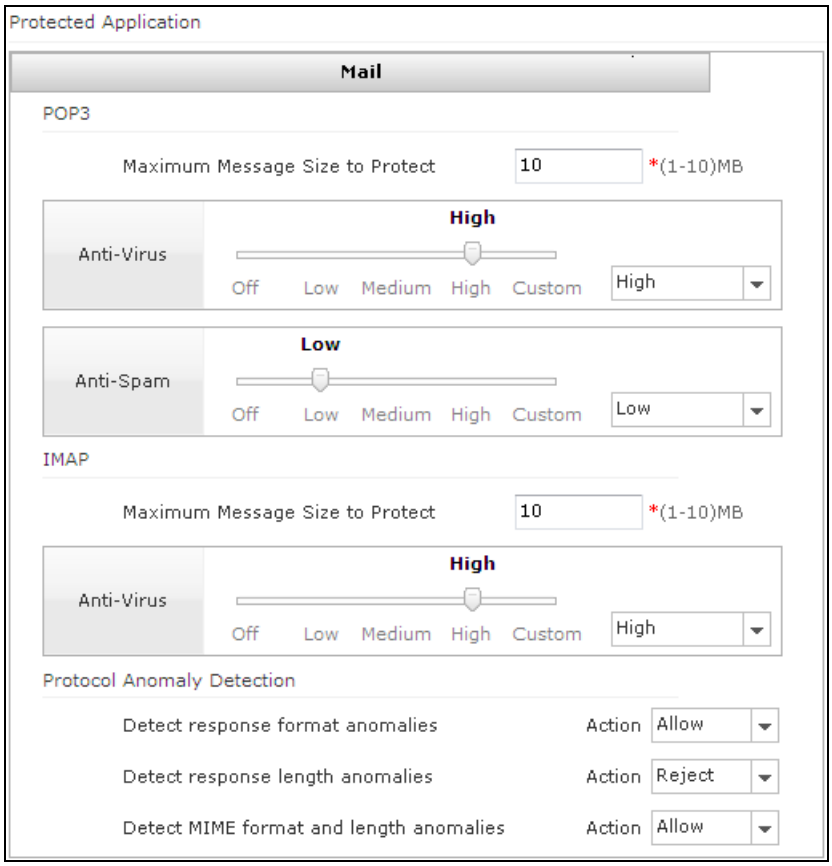




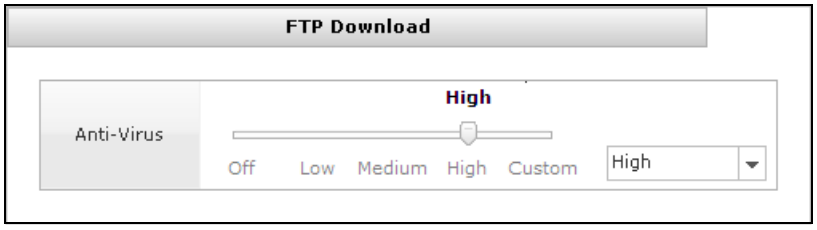
b. Set the IPS inspection level and select an IPS profile.



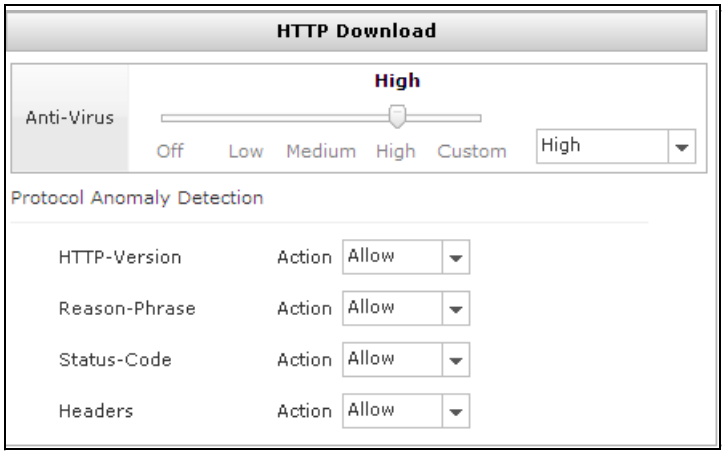
c. Enable/disable the mail protection.



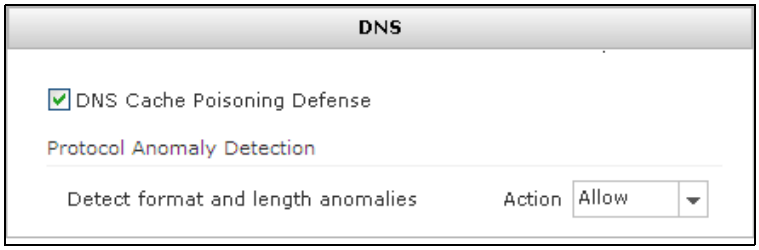
d. Set the anti-virus scanning level and select an anti-virus profile for **FTP Download**.



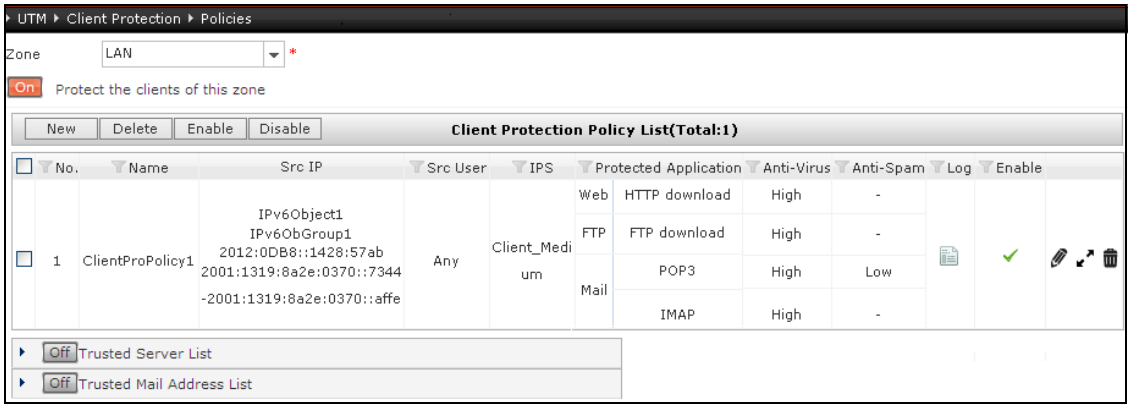
e. Set the anti-virus scanning level, select an anti-virus profile, and set protocol anomaly detection for **HTTP Download**.



f. Enable DNS Cache Poisoning Defense for DNS client traffic.



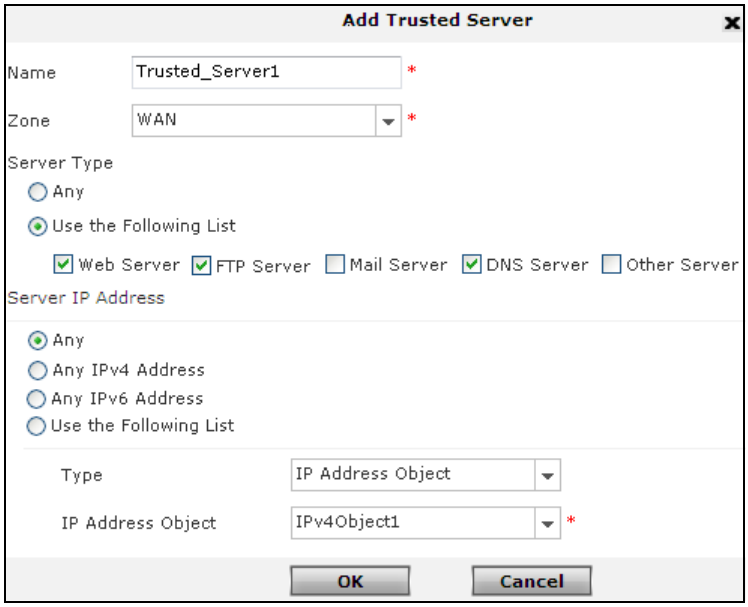
4. Click **OK**.

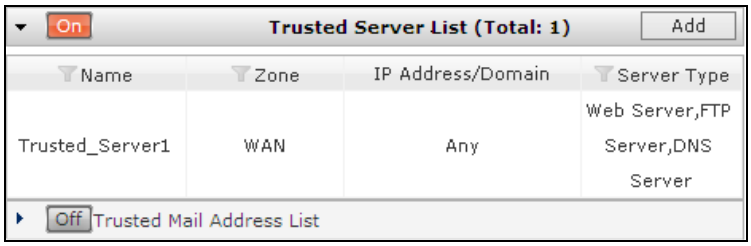


10.2.2.9. Create trusted server / email list

Create trusted server list. For details see 10.5.3.2. (Client Protection) Trusted Server List.

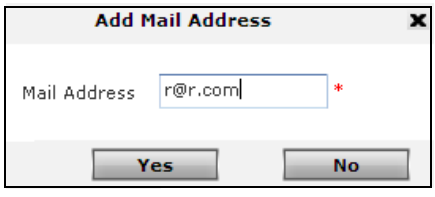
1. Choose **UTM > Client Protection > Policies > Trusted Server List**.
2. Turn **ON** trusted server list and click blank area following Trusted Server List to expand the list.
3. Configure the trusted server list. Locate your mouse cursor at an entry, a ✖ icon will appear and you can click it to delete the entry. Double click a trusted server entry to edit it.

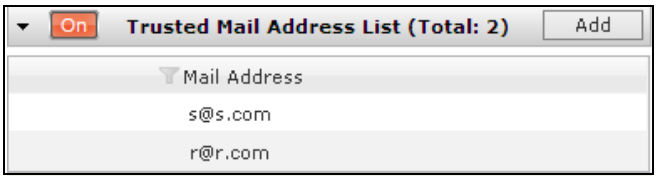




Create trusted mail address list. For details see 10.5.3.3. (Client Protection) Trusted Mail Address List.

4. Choose **UTM > Client Protection > Policies > Trusted Mail Address List**.
5. Turn **ON** trusted mail address list.
6. Configure the trusted mail address list.You can delete/edit entries as to trusted server entries.

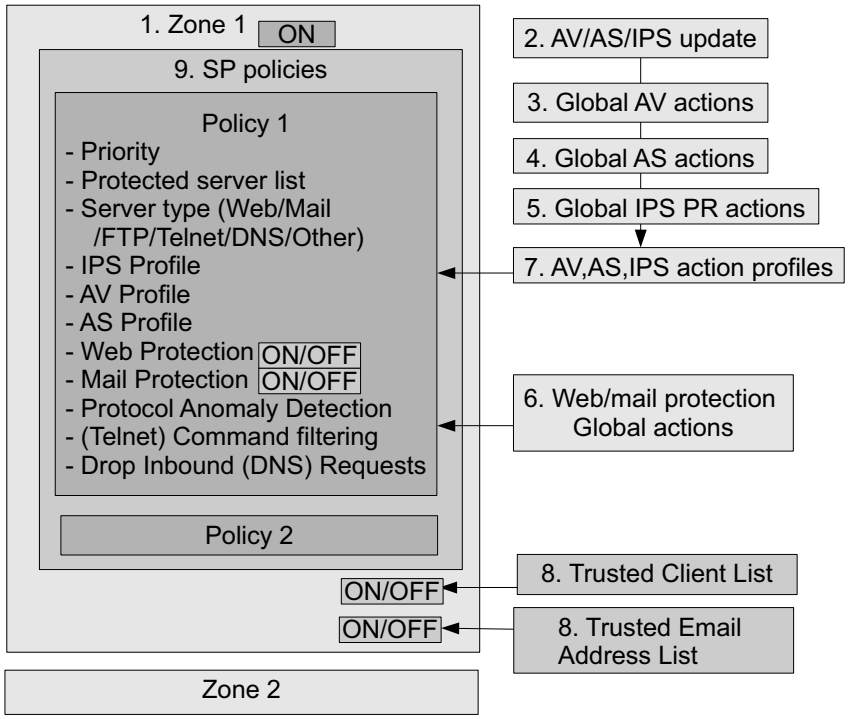




10.2.3. Server protection

Server protection configuration steps are shown below.

Figure 41 Server Protection Configuration Steps



Basic setup:

- 10.2.3.1. Create zones, access policies, default route, NAT rules

General settings (AV/AS/IPS rule update):

- 10.2.3.2. Update AV, AS, IPS rules

Global actions:

- 10.2.3.3. Configure global AV actions (trusted list, action when virus detected, heuristic, scan limits)
- 10.2.3.4. Configure global AS actions (allow/block list, spam word list, scan failures)
- 10.2.3.5. Configure IPS server HTTP, SMTP, POP3, IMAP, DNS protocol restriction
- 10.2.3.6. Configure web/mail protection global actions

Action profiles:

- 10.2.3.7. Create AV, AS, IPS action profiles

Destination zone action / policies:

- 10.2.3.8. Create server protection policies
- 10.2.3.9. Create trusted client / mail address list

10.2.3.1. Create zones, access policies, default route, NAT rules

Same as for client protection 10.2.2.1. Create zones, access policies, default route, NAT rules.

10.2.3.2. Update AV, AS, IPS rules

Same as for client protection 10.2.2.2. Update AV, AS, IPS rules.

10.2.3.3. Configure global AV actions (trusted list, action when virus detected, heuristic, scan limits)

Same as for client protection 10.2.2.3. Configure global AV actions (trusted list, action when virus detected, heuristic, scan limits).

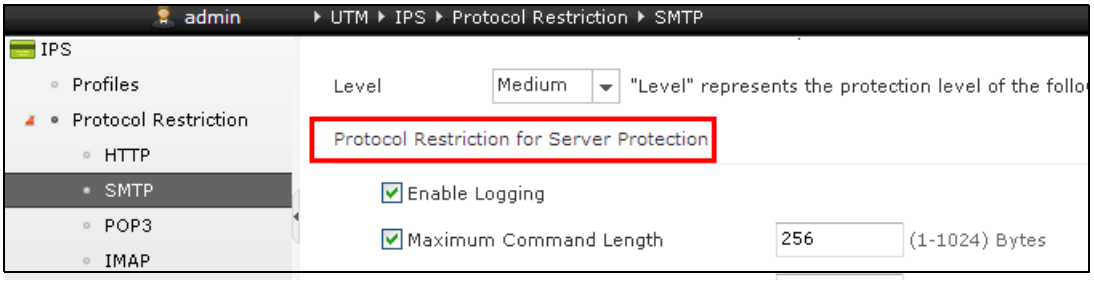
10.2.3.4. Configure global AS actions (allow/block list, spam word list, scan failures)

Same as for client protection 10.2.2.4. Configure global AS actions (allow/block list, spam word list, scan).

10.2.3.5. Configure IPS server HTTP, SMTP, POP3, IMAP, DNS protocol restriction

For client protection settings, see 10.2.2.5. Configure IPS client SMTP, POP3, IMAP, DNS protocol restriction.

1. Choose the protocol restriction type (HTTP, SMTP, POP3, IMAP and DNS for server IPS profiles), for example, **UTM > IPS > Protocol Restriction > SMTP**.
2. Select the level (for example High).
3. Set the parameters for server protection.



4. Click **OK**.

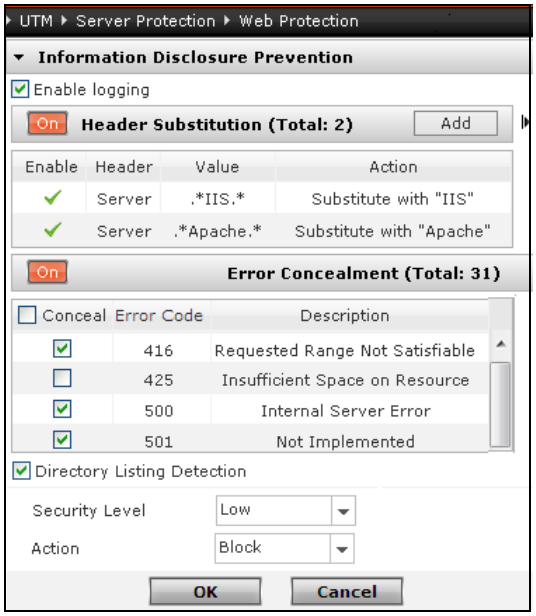
Note: The level you last selected is the enabled level.

5. Choose a server IPS profile and enable protocol restriction in the specified IPS profile.

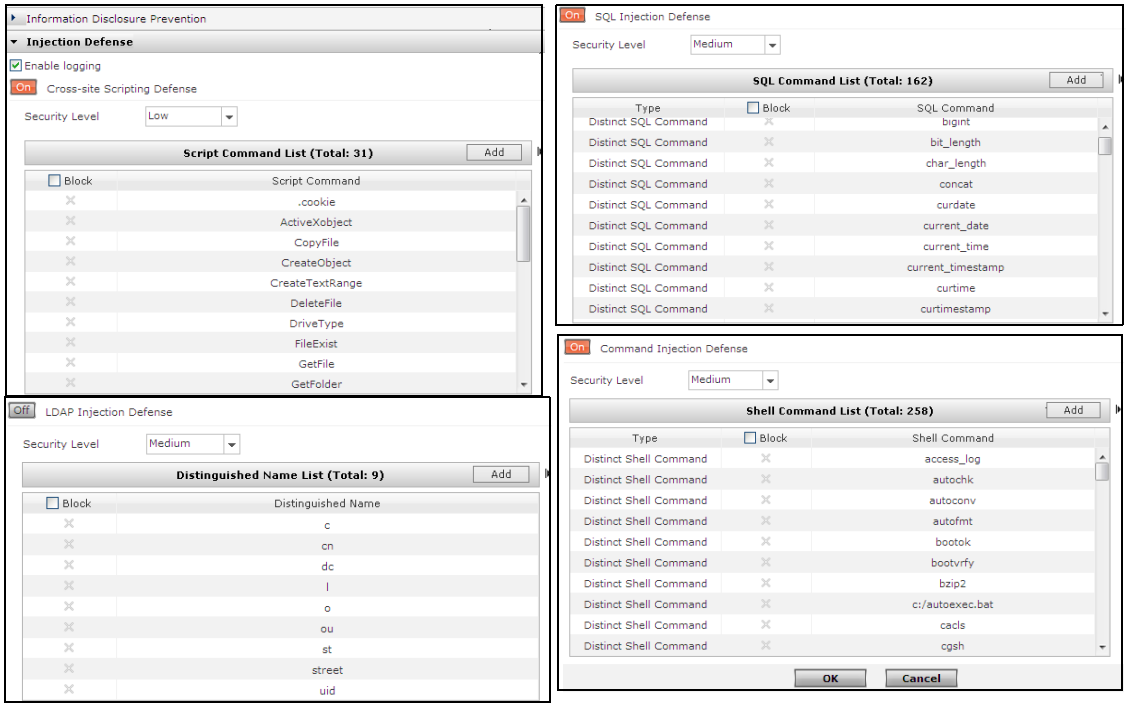
10.2.3.6. Configure web/mail protection global actions

Set Web protection. For details see 10.5.4.4. Web Protection.

1. Choose **UTM > Server Protection > Web Protection**.
2. Enable functions of **Information Disclosure Prevention** and the logging function.



3. Click **Injection Defense** and configure related settings.



4. Click **OK**.

Set mail protection. For details see 10.5.4.5. Mail Protection.

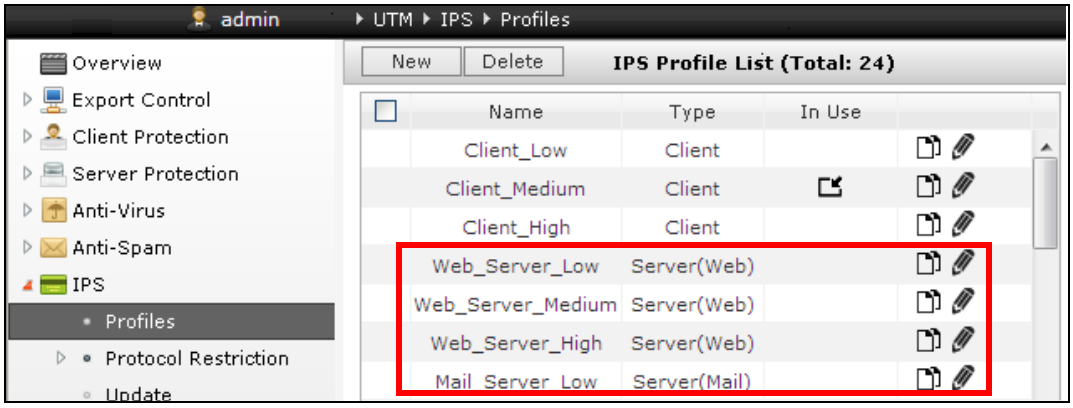
5. Choose **UTM > Server Protection > Mail Protection**.
6. Enable or disable functions of **Mail Protection** and the logging function.

7. Click **OK**.

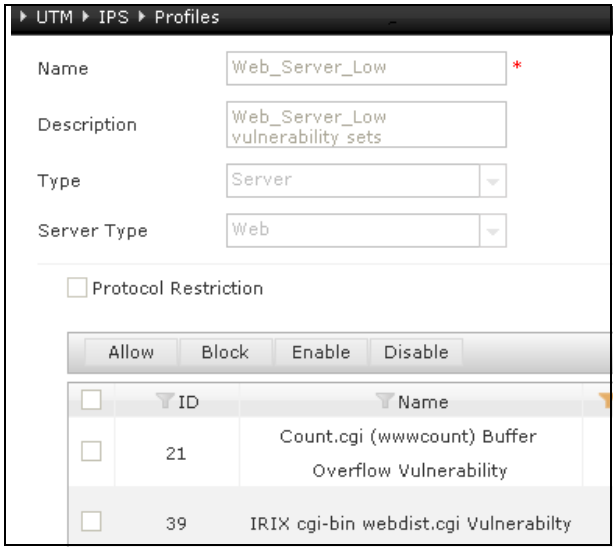
10.2.3.7. Create AV, AS, IPS action profiles

For details about profiles, see the client protection description 10.2.2.7. Create AV, AS, IPS action profiles.

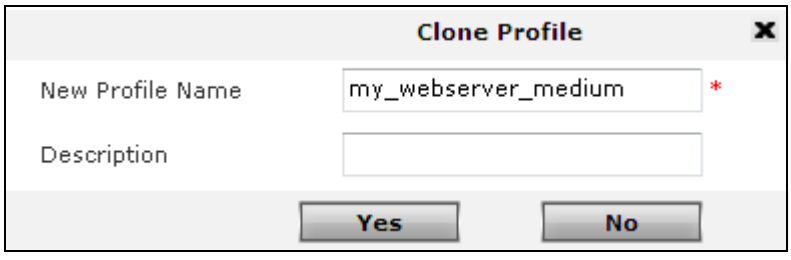
1. The server profiles are listed below.



2. Click ✎ to view the default server profiles.



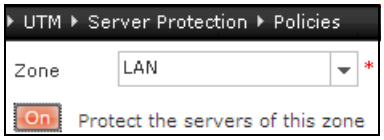
3. Click ❐ to create a copy of a default profile that you can edit.



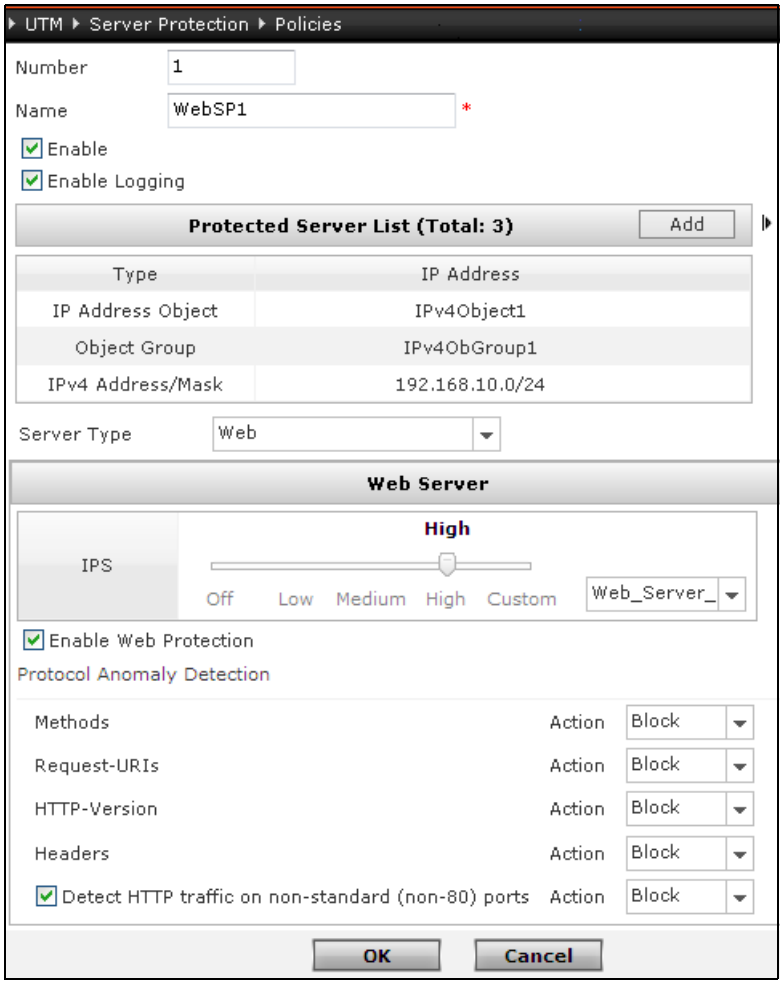
10.2.3.8. Create server protection policies

For details see 10.5.4. Server protection.

1. Choose **UTM > Server Protection > Policies**.
2. Choose an incoming zone and turn ON server protection.

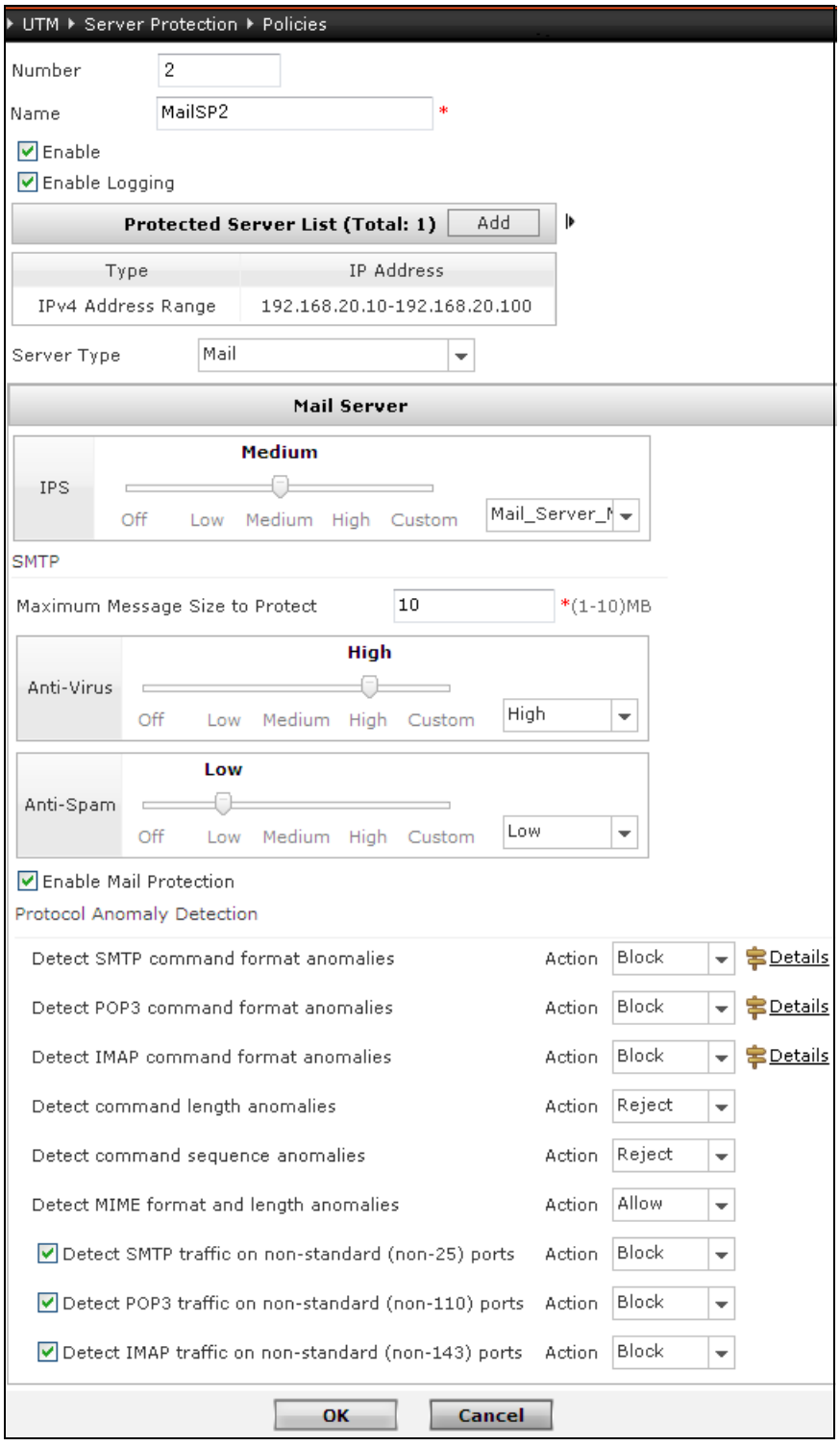


3. Click **New** to create a Web server protection policy and enable web protection in the policy.



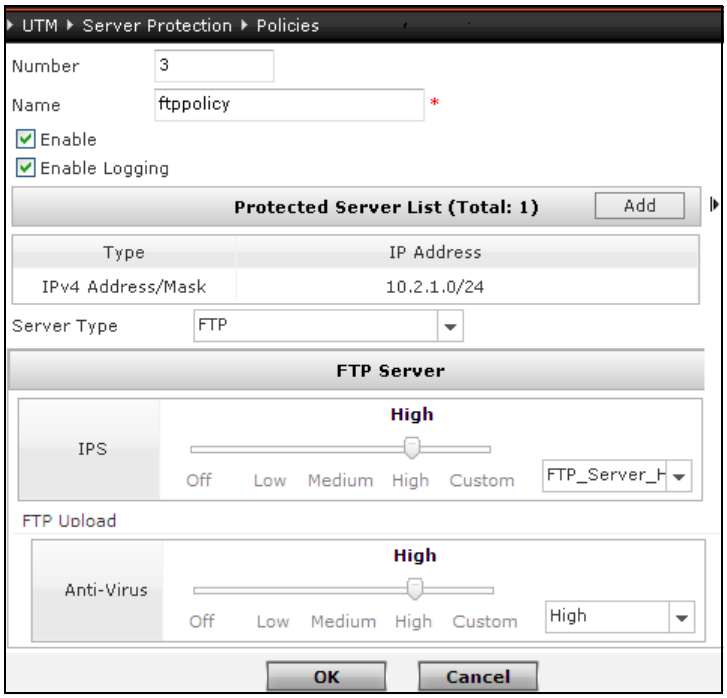
4. Click **OK**.

5. Click **New** to create a mail server protection policy and enable mail protection in the policy.



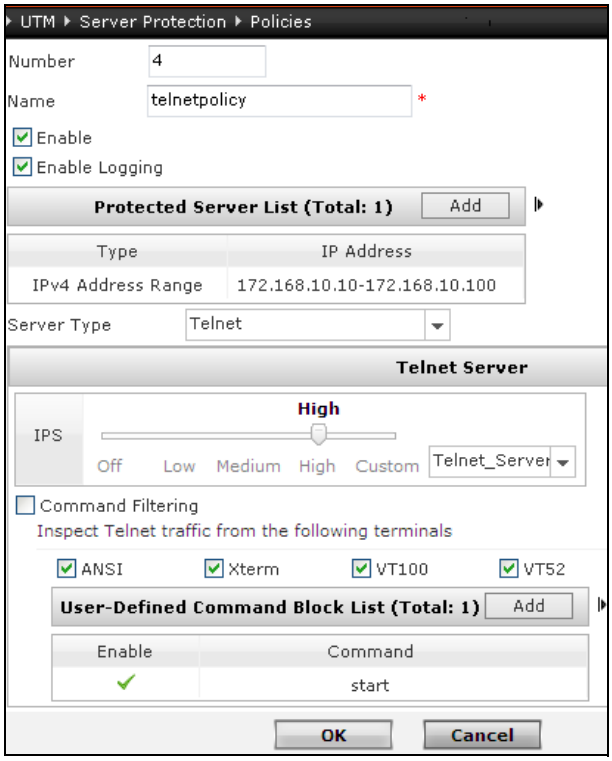
6. Click **OK**.

7. Create an FTP server protection policy.



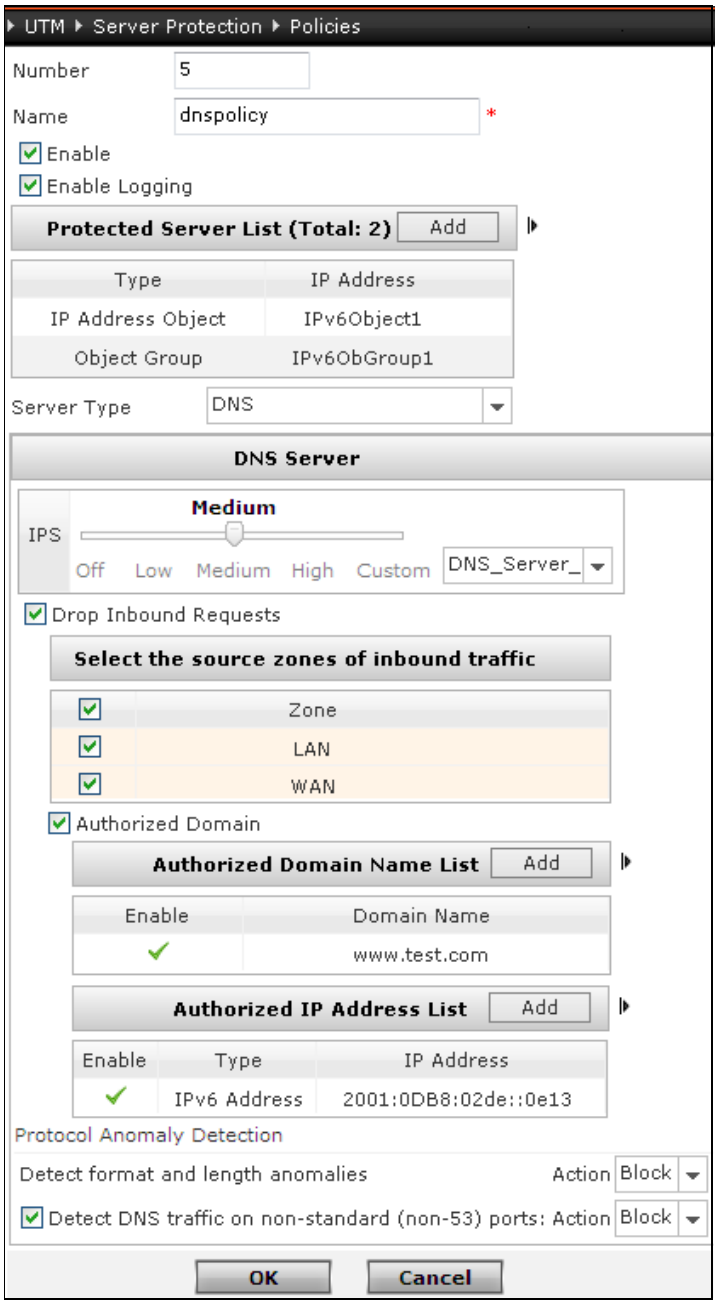
8. Click **OK**.

9. Create a telnet server protection policy.



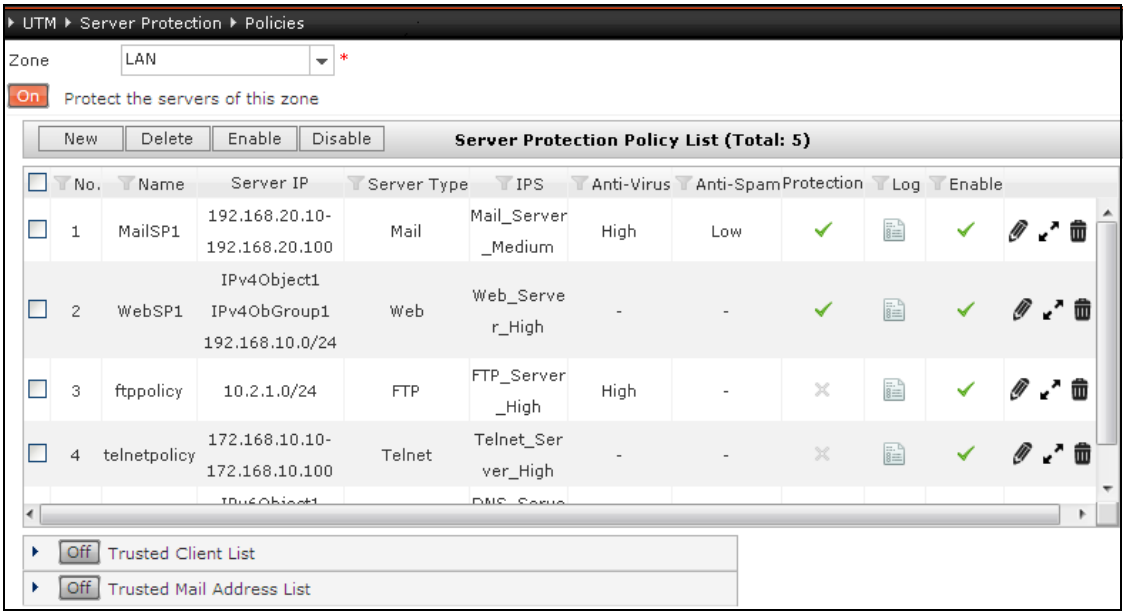
10. Click **OK**.

11. Create a DNS server protection policy.



12. Click **OK**.

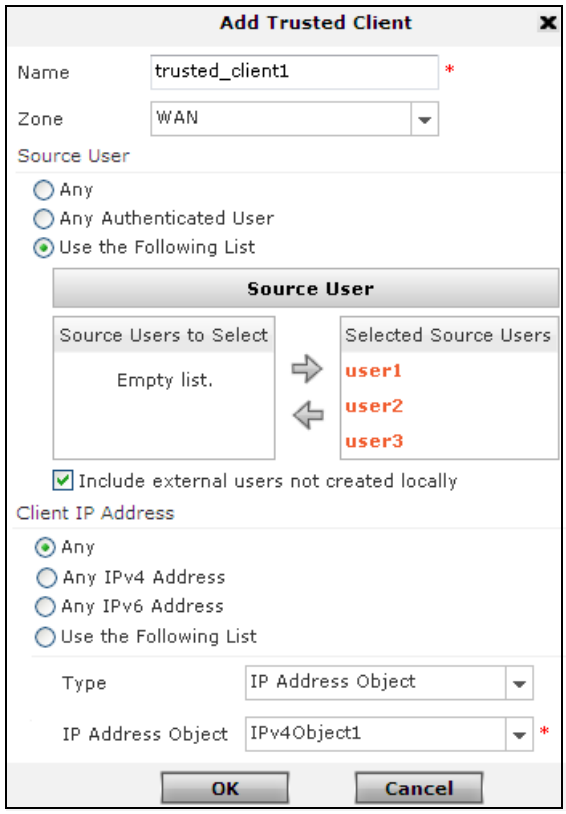
13. View created policies.

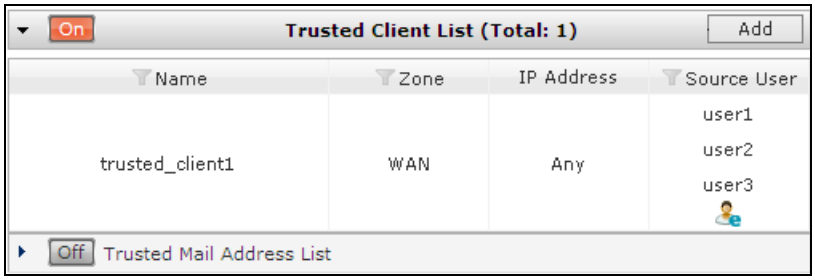


10.2.3.9. Create trusted client / mail address list

Create trusted client list. For parameter details see 10.5.4.2. (Server Protection) Trusted Client List.

1. Choose **UTM > Server Protection > Policies**.
2. Turn ON trusted client list and configure the trusted client list.





Create trusted mail address list. Configurations are the same as for client protection (see 10.2.3.9. Create trusted client / mail address list). For parameter details see 10.5.4.3. (Server Protection) Trusted Mail Address List.

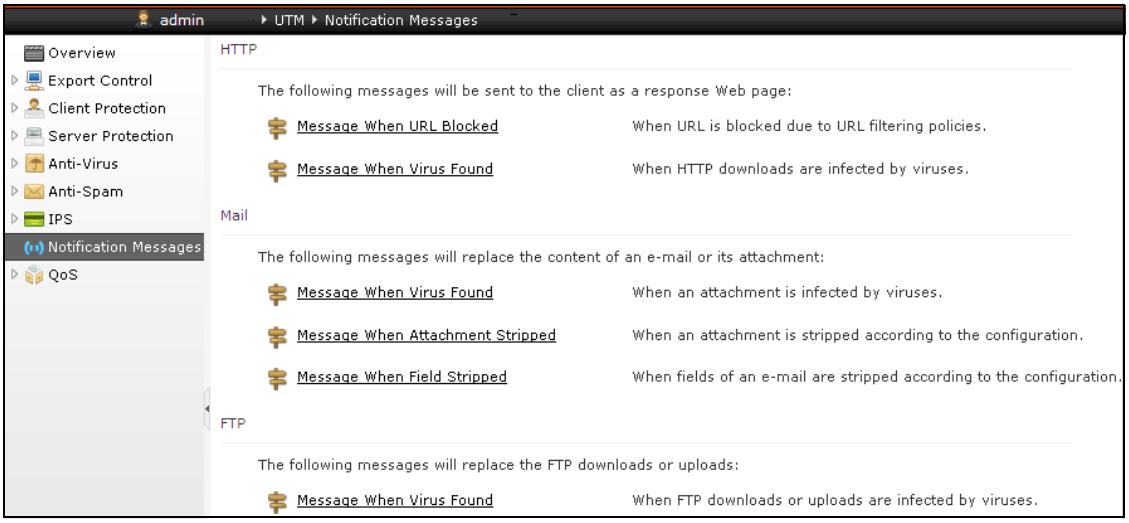
10.2.4. Notification messages

Notification messages are classified into two types:

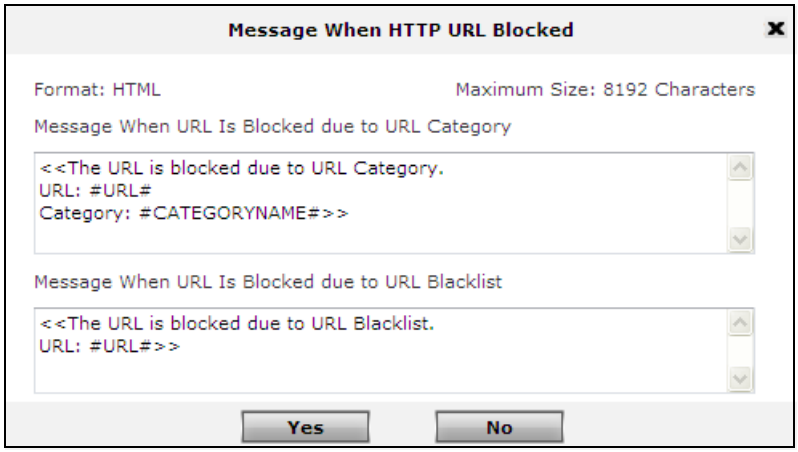
- System Notification Messages—cannot be modified.
- User-Defined Notification Messages—can be configured through the WebUI.

For details see 10.5.8. Notification Messages.

1. Select **UTM > Notification Messages**.



2. Click a link to edit the notification message.

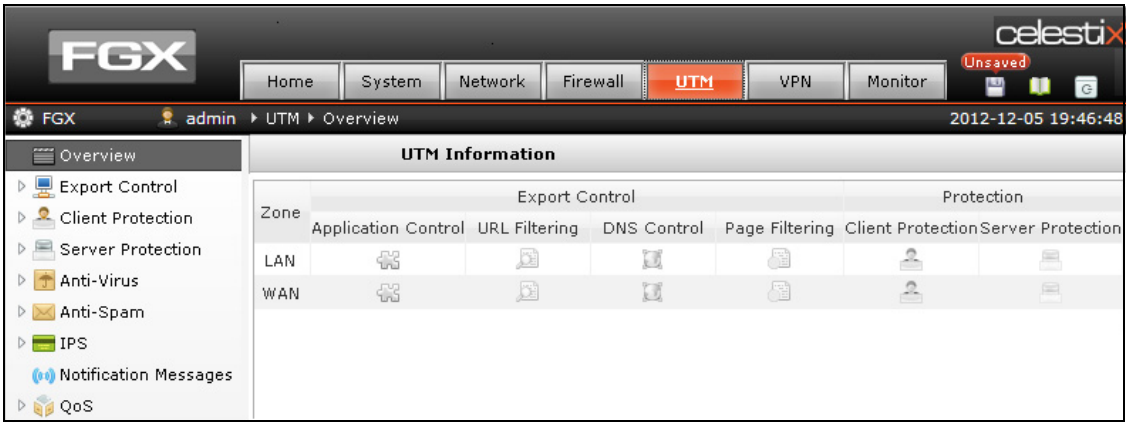


3. Click **Yes**.

10.2.5. Overview page

Overview page shows the UTM information of all zones. UTM policies are applied to zones.

1. Select **UTM > Overview** and view the UTM information on all zones.



2. Click the icons to go to the corresponding pages and configure related settings.

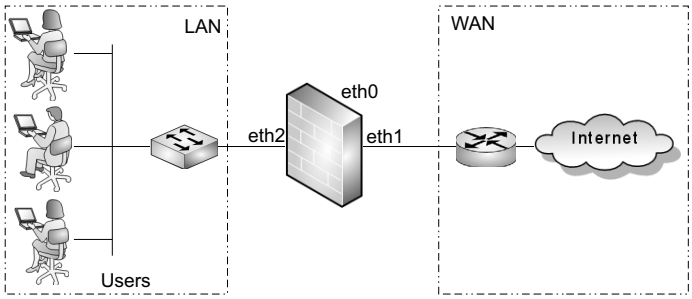
10.3. Scenarios

Typical scenarios of UTM include export control, client protection, and server protection.

Scenario 1: Export Control

As shown below, zone LAN includes interface eth2 and zone WAN includes eth1. The enterprise wants to control user traffic to the Internet. Then you can configure application control, URL filtering, DNS domain blacklist, and page filtering on FGX.

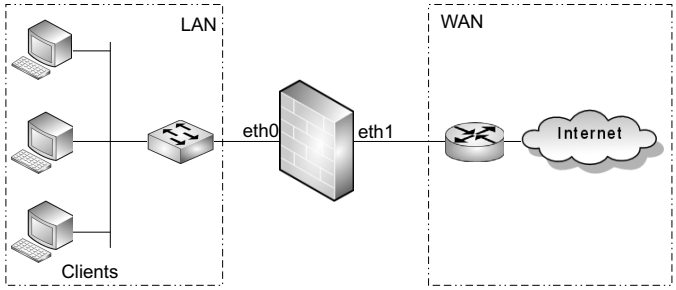
Figure 42 Typical Application of UTM Export Control



Scenario 2: Client Protection

As shown below, there are two zones on FGX: LAN and WAN. LAN includes interface eth0 and WAN includes interface eth1. The enterprise wants to protect the clients within LAN. Then you can configure client protection on zone LAN.

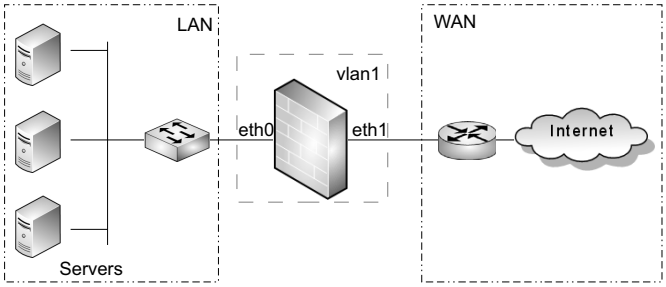
Figure 43 Typical Application of UTM Client Protection



Scenario 3: Server Protection

As shown below, there are two zones on FGX: LAN and WAN. LAN includes interface eth0 and WAN includes interface eth1. The enterprise wants to protect the servers within LAN. Then you can configure server protection on LAN.

Figure 44 Typical Application of UTM Server Protection



10.4. UTM Examples

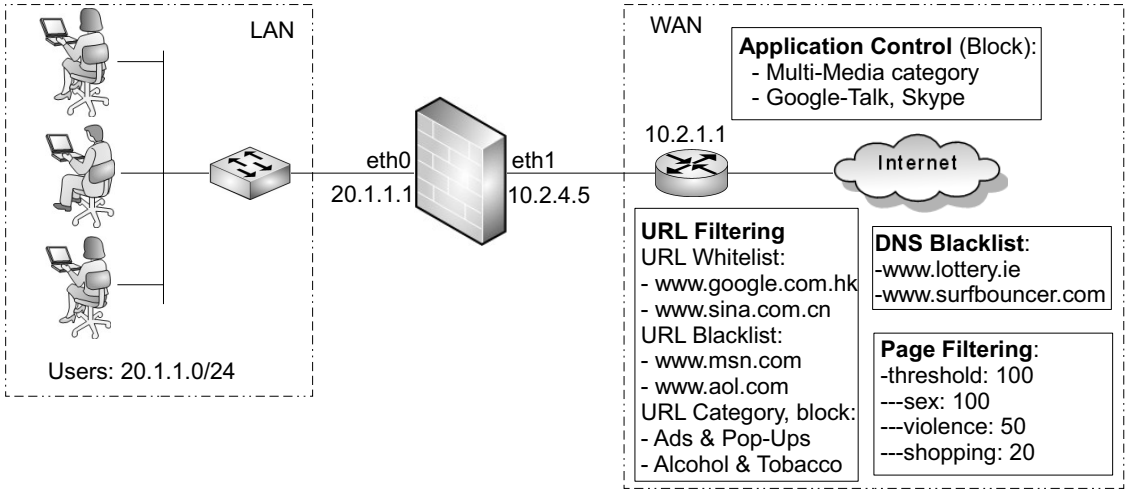
This section mainly gives three examples to show how to apply UTM in three typical scenarios:

- Example 1: Typical Application of UTM Export Control
- Example 2: Typical Application of UTM Client Protection
- Example 3: Typical Application of UTM Server Protection

Example 1: Typical Application of UTM Export Control

In this example, users in zone LAN access the Internet through FGX. To control user access to the Internet, the network administrator needs to configure export control as shown in the following diagram:

Figure 45 Typical Application of UTM Export Control



Before you configure UTM, the following need to be configured (if you skip initialization for the first login):

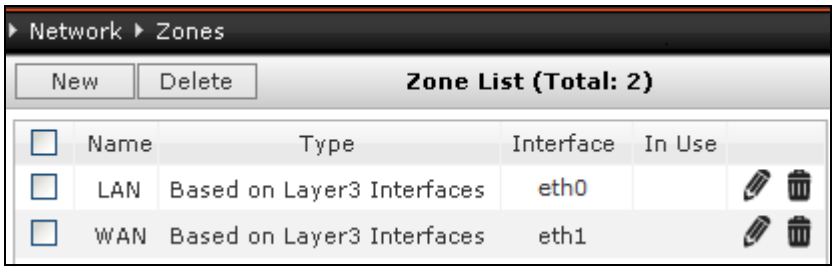
1. Create interfaces, zones, default route, access policies, and NAT rules

The UTM configuration steps are:

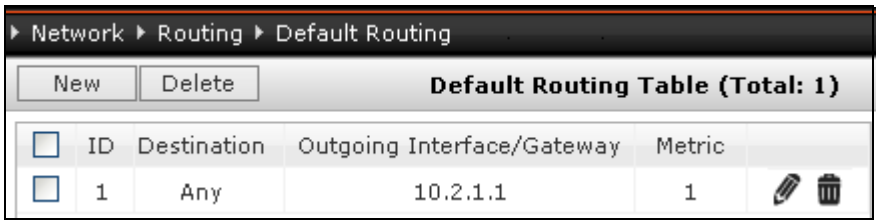
2. Configure Application Control
3. Configure URL Filtering
4. Configure DNS Domain Blacklist
5. Configure Page Filtering

1. Create interfaces, zones, default route, access policies, and NAT rules

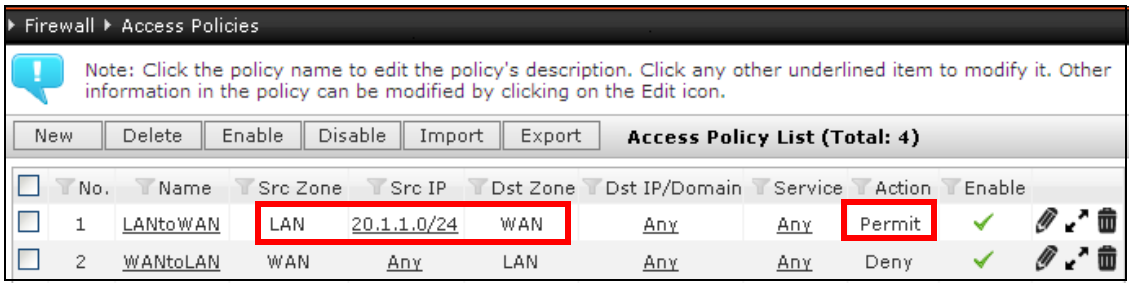
1. Choose **Network > Interfaces**, set eth1 and eth0 to Layer 3 interfaces, and set their IP addresses to 10.2.4.5/21 and 20.1.1.1/24.
2. Choose **Network > Zones**, create two Layer 3 zones LAN and WAN, and assign eth0 to LAN and eth1 to WAN.



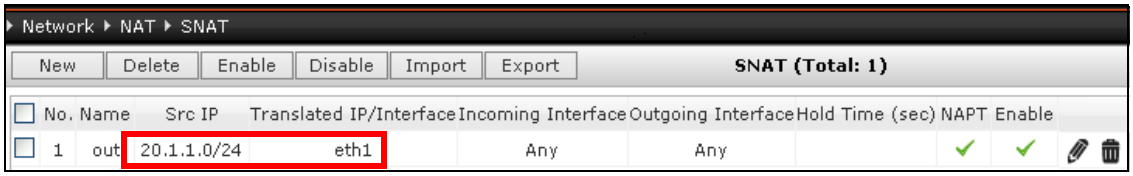
3. Choose **Network > Routing > Default Route**, and modify the gateway of the default route to 10.2.1.1.



4. Choose **Firewall > Access Policies**, and create access policies as follows to allow clients to access the Internet:



5. Choose **Network > NAT > SNAT**, and add a SNAT policy. Then FGX will translate the client IP addresses to the IP address of eth1 to protect internal clients from Internet attacks:

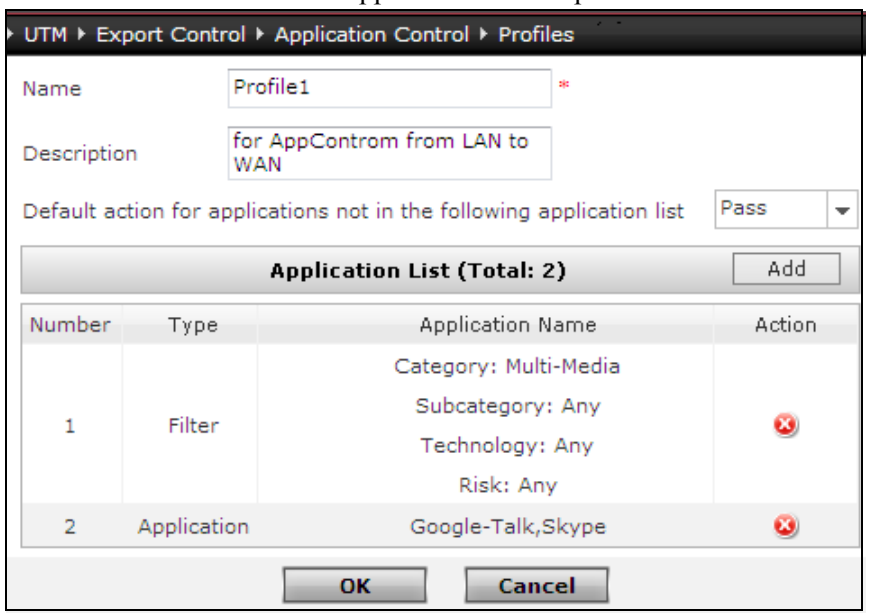


2. Configure Application Control

Application control configuration involves creating an application control profile and policy.

2.1 Create an Application Control Profile

1. Choose **UTM > Export Control > Application Control > Profiles**.
2. Click **New** and create an application control profile named Profile1.

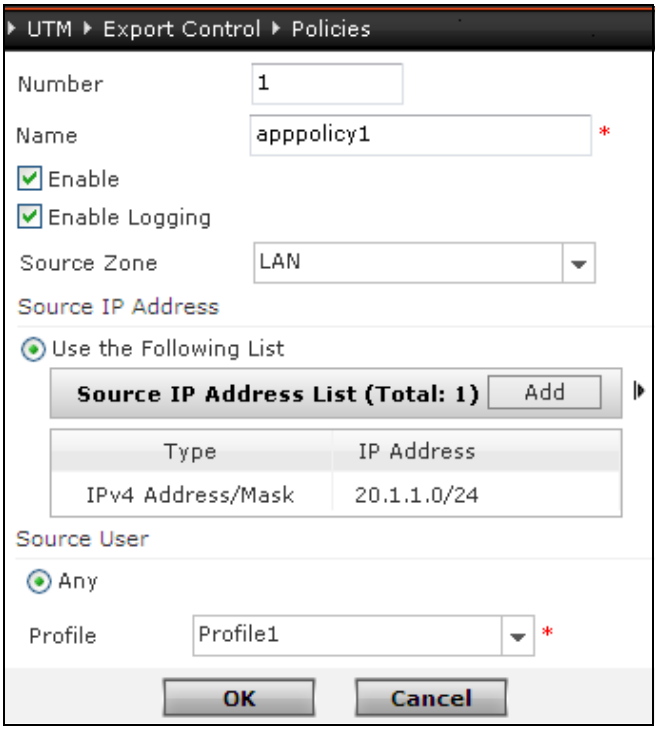


Note: When adding an application to the profile, you can enter the first one or two letters of the application name and use the drop-down list to automatically complete the application name.

3. Click **OK**.

2.2 Create an Application Control Policy

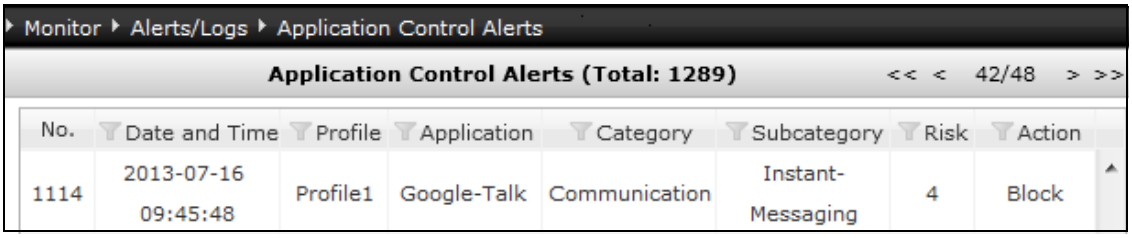
1. Choose **UTM > Export Control > Policies**.
2. Choose WAN from the zone ("**Export Control on**") drop-down list and enable (turn "**ON**") the application control function.
3. Expand **Application Control** area. Click **New** to create an application control policy named apppolicy1 as shown below.



4. Click **OK**. Then the intranet users in subnet 20.1.1.0 cannot use Google-Talk or Skype or access multi-media applications over the Internet.

2.3 Monitor Application Control

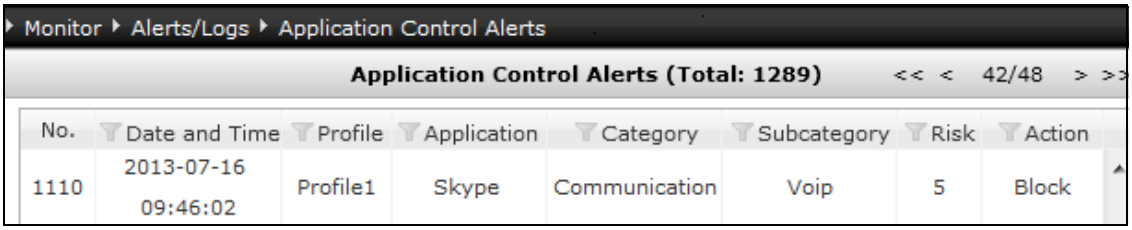
1. Start Google-Talk and Skype, and you will find that you cannot logon.
2. Choose **Monitor > Alerts/Logs > Application Control Alerts**, you can view system logs saying that Google-Talk, Skype or other multi-media applications have been blocked.
   - Google-Talk is blocked:


Monitor ▸ Alerts/Logs ▸ Application Control Alerts

Application Control Alerts (Total: 1289) << < 42/48 > >>

No.	Date and Time	Profile	Application	Category	Subcategory	Risk	Action
1114	2013-07-16 09:45:48	Profile1	Google-Talk	Communication	Instant-Messaging	4	Block

   - Skype is blocked:


Monitor ▸ Alerts/Logs ▸ Application Control Alerts

Application Control Alerts (Total: 1289) << < 42/48 > >>

No.	Date and Time	Profile	Application	Category	Subcategory	Risk	Action
1110	2013-07-16 09:46:02	Profile1	Skype	Communication	Voip	5	Block

   - Multi-media applications are blocked:


Monitor ▸ Alerts/Logs ▸ Application Control Alerts

Application Control Alerts (Total: 1289) << < 42/48 > >>

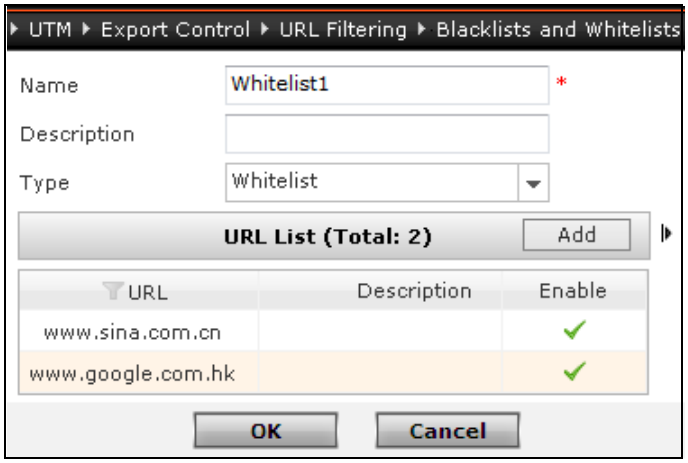
No.	Date and Time	Profile	Application	Category	Subcategory	Risk	Action
1120	2013-07-16 07:50:22	Profile1	PPStream	Multi-Media	Photo-Video	4	Block
1121	2013-07-16 07:49:45	Profile1	PPLive	Multi-Media	Photo-Video	4	Block

3. Configure URL Filtering

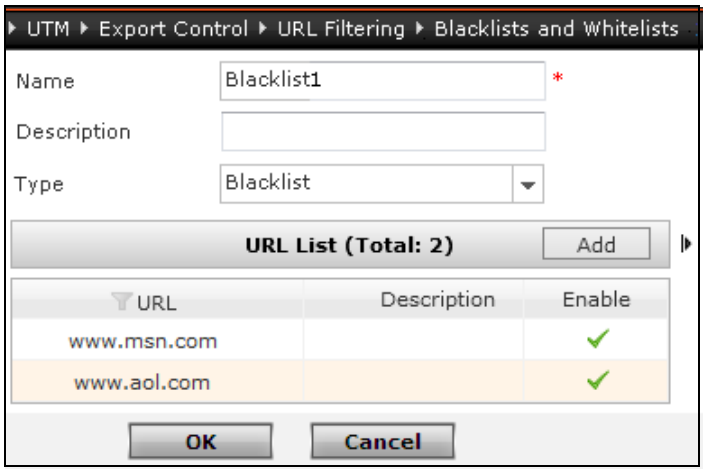
URL Filtering configuration involves creating: (1) URL blacklist and whitelist, (2) URL filtering profile, and (3) URL filtering policy.

3.1 Create URL Blacklist and Whitelist

1. Choose **UTM > Export Control > URL Filtering > Blacklists and Whitelists**.
2. Click **New** and create a URL whitelist named Whitelist1.



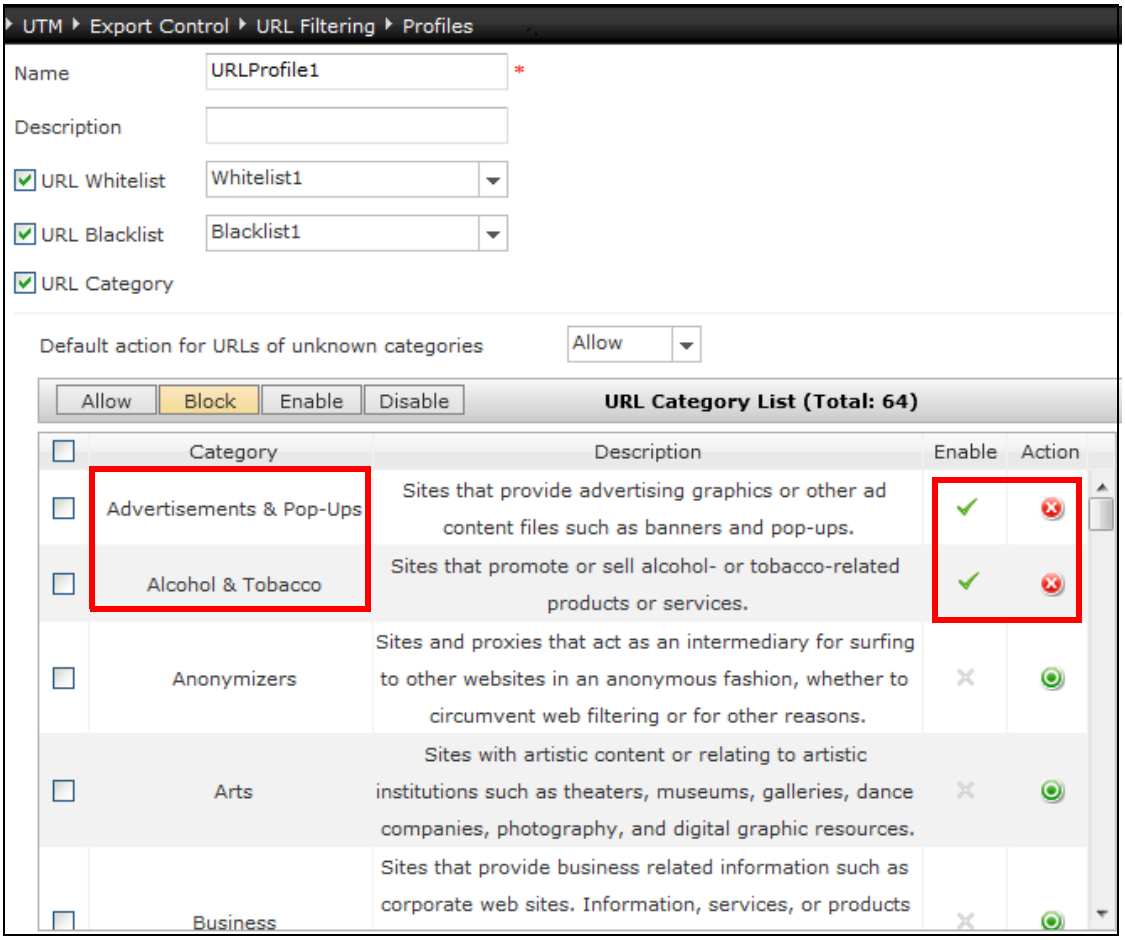
3. Click **OK**.
4. Click **New** and create a URL blacklist named Blacklist1.



5. Click **OK**.

3.2 Create URL Filtering Profile

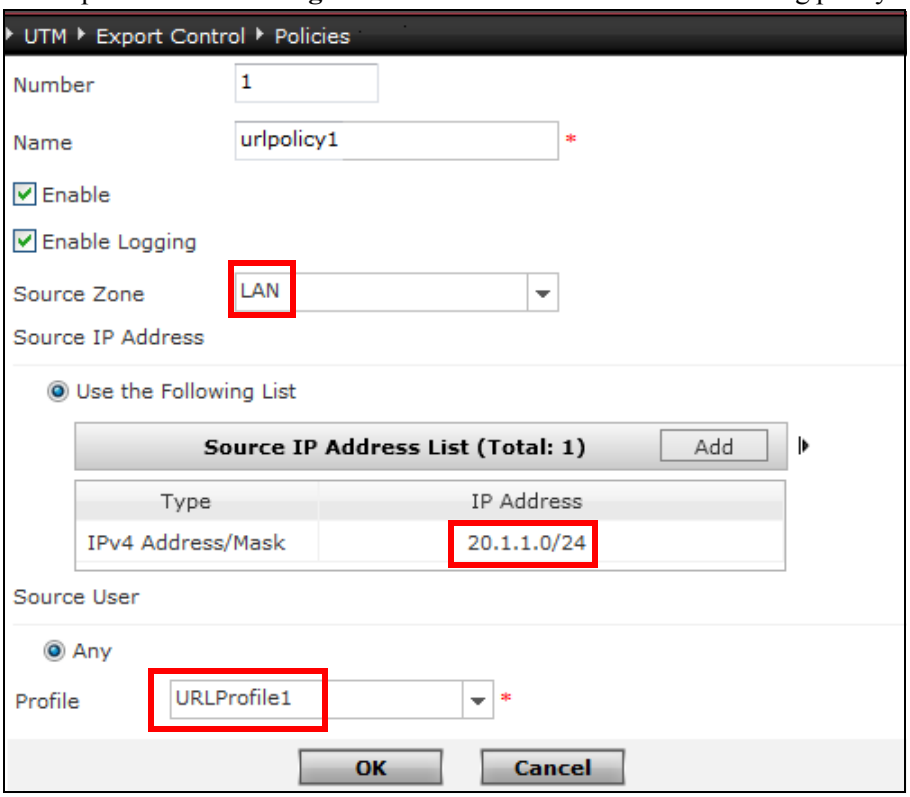
1. Choose **UTM > Export Control > URL Filtering > Profiles**.
2. Click **New** and create a URL profile named URLProfile1 (for Advertisements & Pop-ups and Alcohol &Tobacco check the check boxes and then click **Block**).



3. Click **OK**.

3.3 Create URL Filtering Policy

1. Choose **UTM > Export Control > Policies**.
2. Choose WAN from the zone (**Export Control on**) drop-down list and enable (turn **ON**) the URL filtering function.
3. Expand **URL Filtering** area. Click **New** to create a URL filtering policy named urlpolicy1.

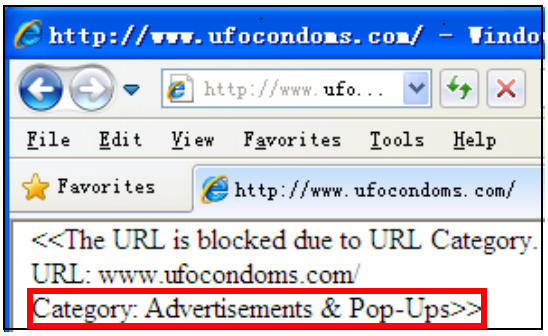


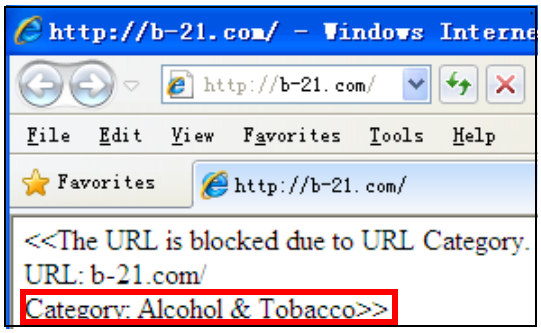
4. Click **OK**. Then the intranet users on subnet 20.1.1.0 can access the whitelisted URLs and URL categories successfully but cannot access the blacklisted URLs and URLs of the blocked URL categories (Advertisements & Pop-Ups, Alcohol & Tobacco).

3.4 Monitor URL Filtering

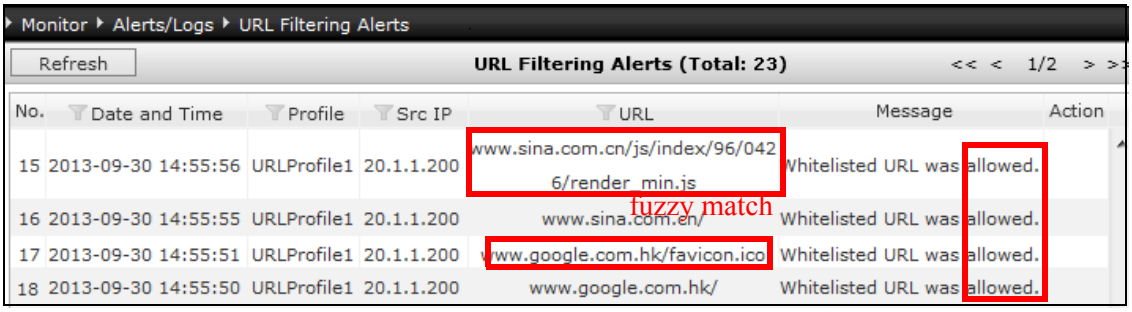
1. The intranet users can access the whitelisted URLs www.google.com.hk and www.sina.com.cn successfully.
2. When the intranet users access the blacklisted URLs, a notification message webpage will be sent back the client.

3. The URLs of Advertisements & Pop-ups and Alcohol & Tobacco categories will be blocked by URL category filtering.

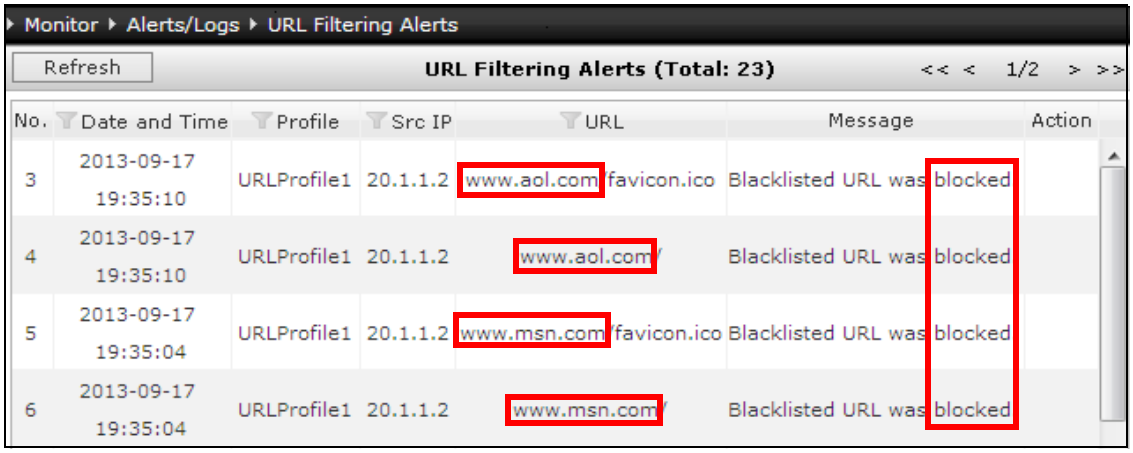




4. Choose **Monitor > Alerts/Logs > URL Filtering Alerts**, and you can view the logs about whitelisted and blacklisted URLs. URL filtering supports fuzzy match.
   - Whitelisted URLs:



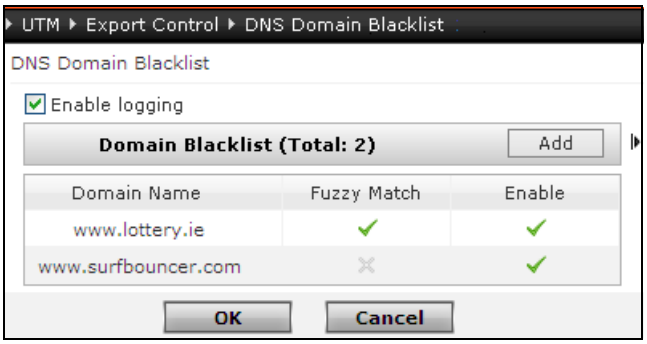
- Blacklisted URLs:



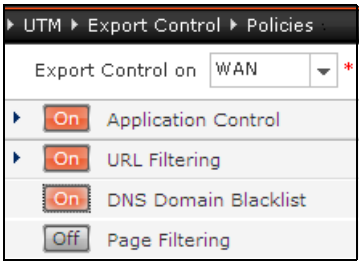
- URLs blocked by category filtering:

4. Configure DNS Domain Blacklist

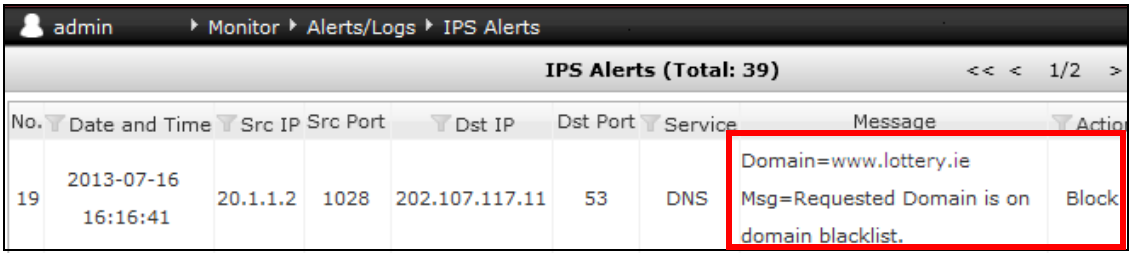
1. Choose **UTM > Export Control > DNS Domain Blacklist**.
2. Configure the DNS domain blacklist to block DNS requests for www.lottery.ie and www.surfbouncer.com.



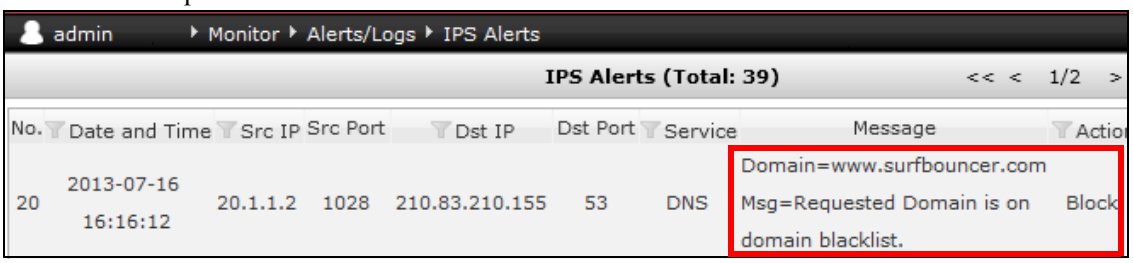
3. Click **OK**.
4. Choose **UTM > Export Control > Policies**.
5. Choose WAN from the zone (**Export Control on**) drop-down list and enable (turn **ON**) the DNS domain blacklist function. The intranet users cannot access www.lottery.ie or www.surfbouncer.com.



6. Choose **Monitor > Alerts/Logs > IPS Alerts**, and you can view the DNS logs.
   - DNS requests for www.lottery.ie are blocked:

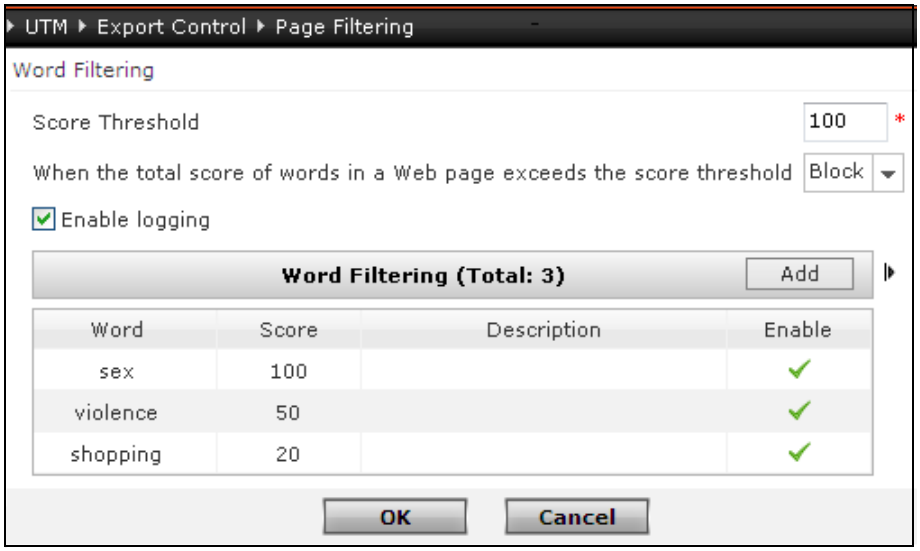


   - DNS requests for www.surfbouncer.com are blocked:

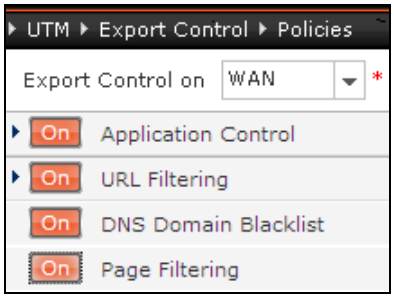


5. Configure Page Filtering

1. Choose **UTM > Export Control > Page Filtering**.
2. Configure the page filtering settings to block web pages containing the listed filtered words whose total score reaches 100%. For example, a page that contains 1 instance of "sex" will be blocked. A page that contains 1 instance of "violence" and 3 instances of "shopping" (1*50 + 3*20 = 110%) will also be blocked.



3. Click **OK**.
4. Choose **UTM > Export Control > Policies**.
5. Choose WAN from the zone (**Export Control on**) drop-down list and enable (turn **ON**) the page filtering function.



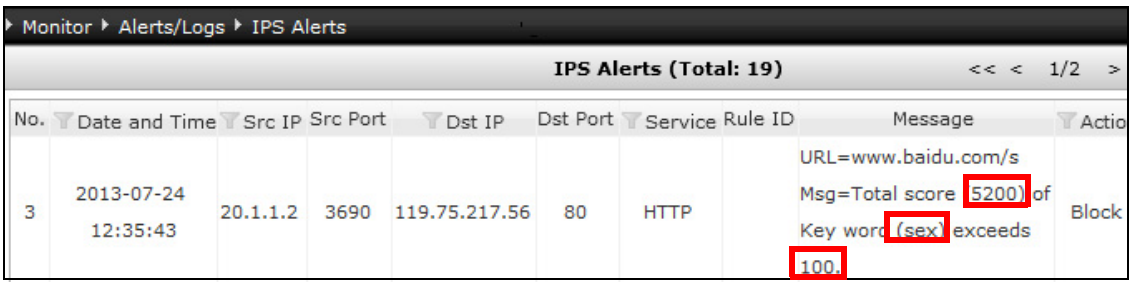
6. Click . When the Intranet users access webpages containing specified key words and the total score reaches the threshold, the webpages will be blocked.

7. Choose **Monitor > Alerts/Logs > IPS Alerts**, and you can view the response page filtering logs.

   - Webpages containing the key word “shopping” are blocked when the total score exceeds the limit:

   - Webpages containing the key word “violence” are blocked when the total score exceeds the limit:

   - Webpages containing the key word “sex” are blocked when the total score exceeds the limit:

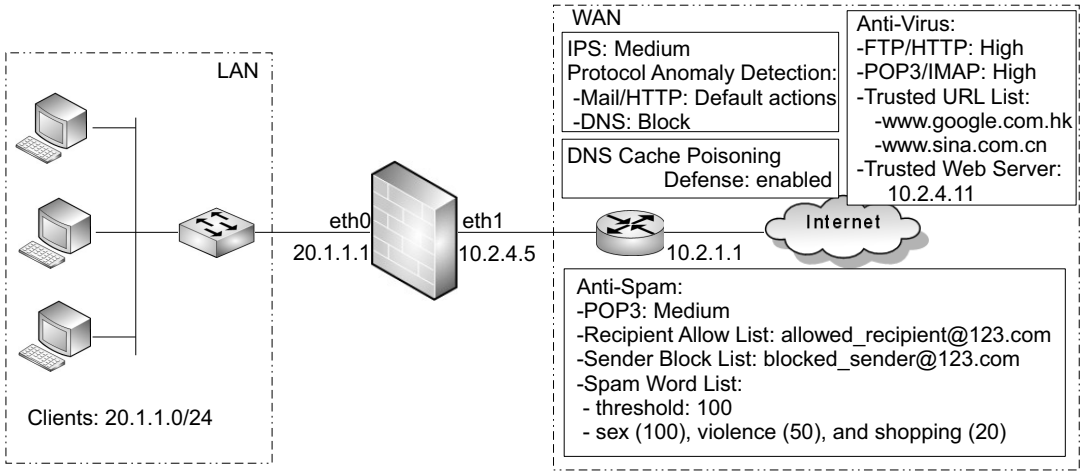


Note: Sometimes, a whitelisted URL’s response may be blocked by page filtering if the response page contains specified key words and the total score reaches the threshold. Check if your URL filtering and page filtering configurations conflict with each other.

Example 2: Typical Application of UTM Client Protection

In this example, clients in zone LAN communicate with the Internet through FGX. To protect clients from Internet threats, the network administrator needs to configure client protection as shown in the following diagram, including anti-virus, anti-spam, attack signature defense (IPS), and DNS cache poisoning defense.

Figure 46 Typical Application of UTM Client Protection



If you have chosen Routing Mode and the above topology when you initialized FGX (using the initialization wizard), then the configuration steps include:

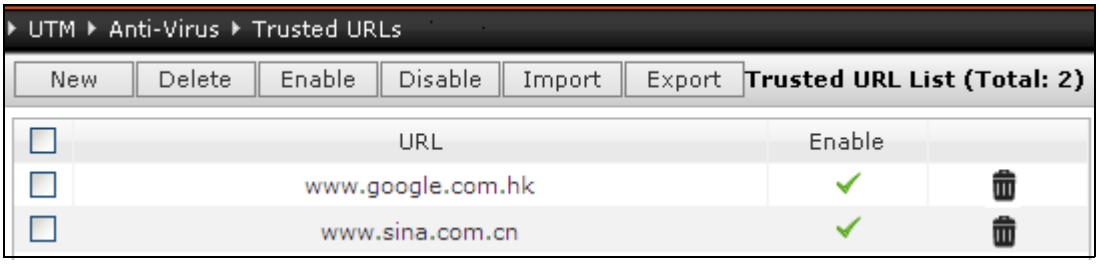
1. Modify Access Policies
2. Configure Anti-Virus
3. Configure Anti-Spam
4. Configure DNS Cache Poisoning Defense
5. Create Client Protection Policy
6. Monitor Client Protection

1. Modify Access Policies

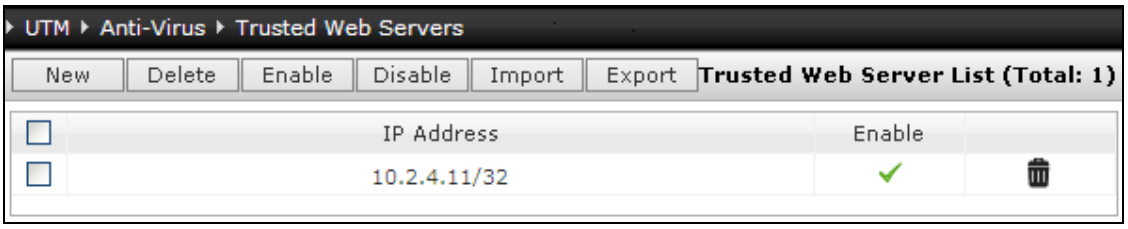
1. Choose **Firewall > Access Policies**.
2. Modify the access policies as follows to allow client traffic:

2. Configure Anti-Virus

1. Choose **UTM > Anti-Virus > Trusted URLs**, and add two trusted URLs www.google.com.hk and www.sina.com.cn.



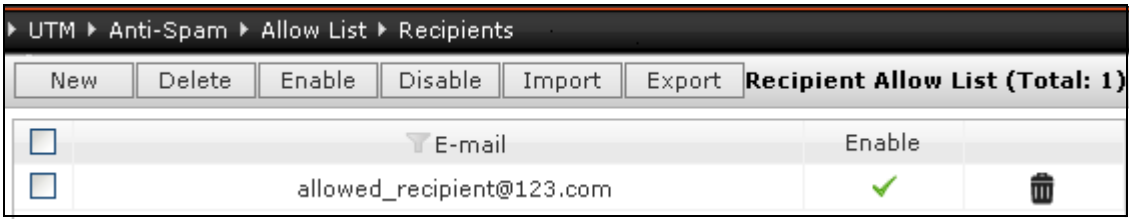
2. Choose **UTM > Anti-Virus > Trusted Servers**, and add trusted server 10.2.4.11.



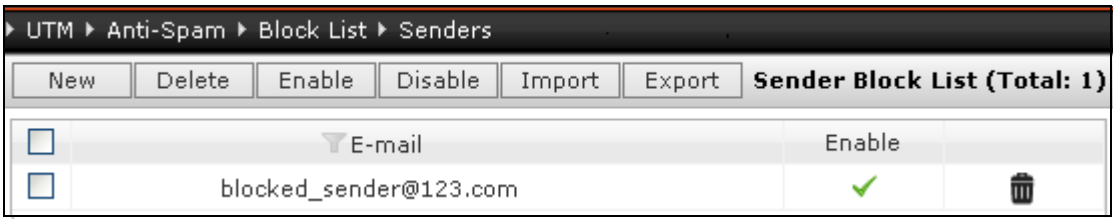
3. Configure Anti-Spam

To configure the allow and block lists:

1. Choose **UTM > Anti-Spam > Allow List > Recipients**, and add an allowed recipient e-mail address allowed_recipient@123.com.



2. Choose **UTM > Anti-Spam > Block List > Senders**, and add a blocked sender e-mail address blocked_sender@123.com.



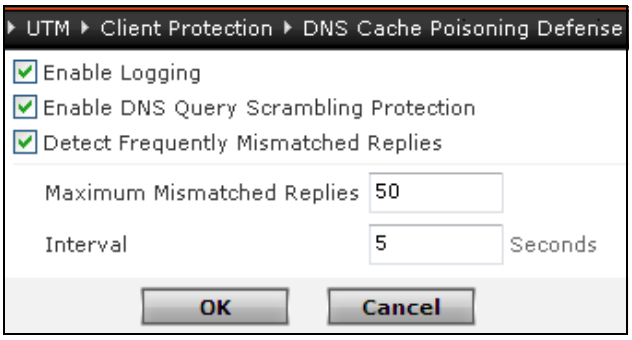
To configure the spam word list:

1. Choose **UTM > Anti-Spam > Spam Word List**.
2. Configure the score threshold and the spam word list to block e-mails containing the listed filtered words whose total score reaches 100%. For example, an e-mail that contains 1 instance of "sex" will be blocked. An e-mail that contains 1 instance of "violence" and 3 instances of "shopping" (1*50 + 3*20 = 110%) will be also blocked:

3. Click **OK**.

4. Configure DNS Cache Poisoning Defense

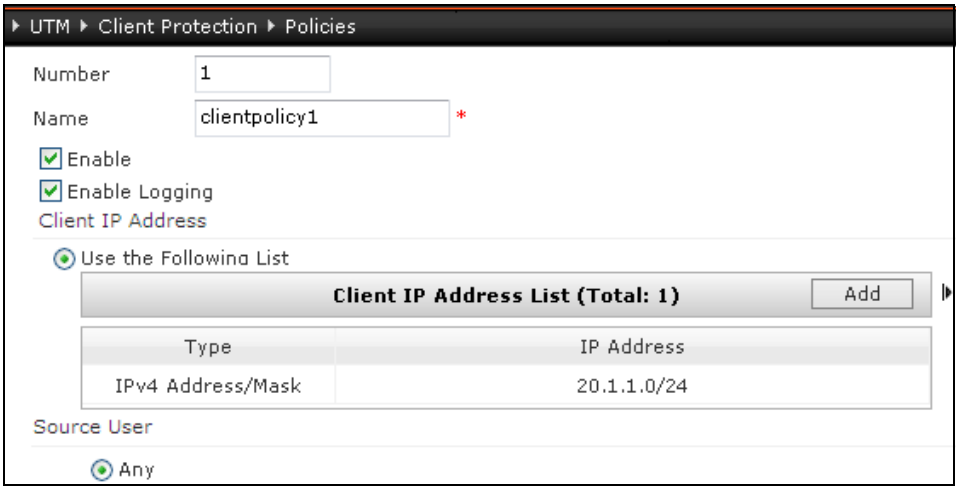
1. Choose **UTM > Client Protection > DNS Cache Poisoning Defense**.
2. Configure DNS cache poisoning defense settings as follows:



3. Click **OK**.

5. Create Client Protection Policy

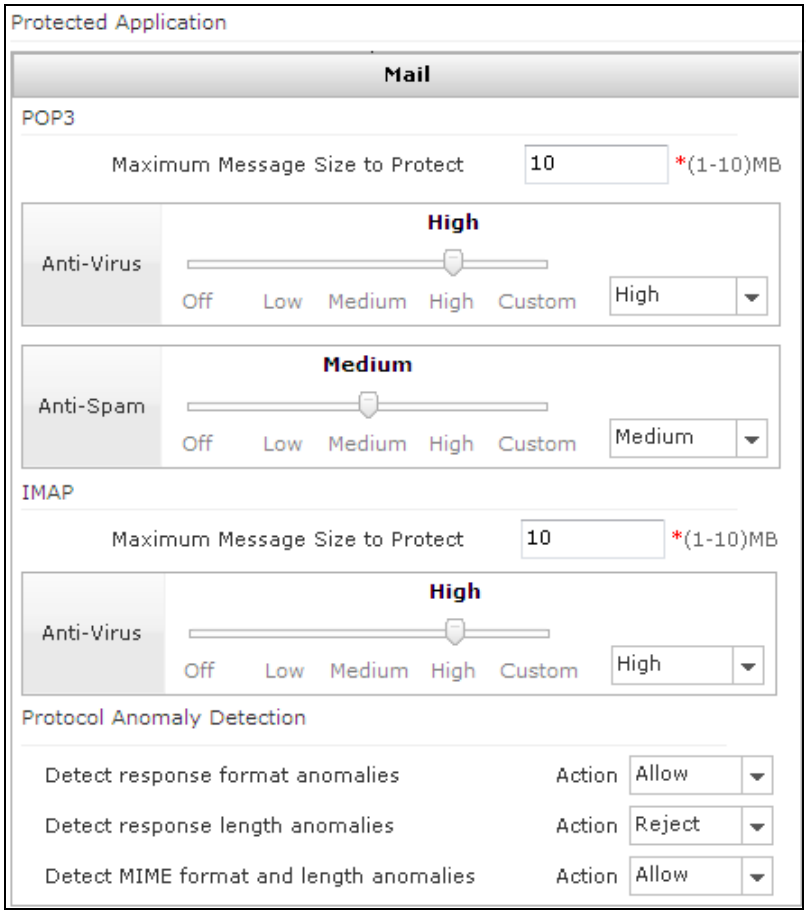
1. Choose **UTM > Client Protection > Policies**.
2. Choose **LAN** from the **Zone** drop-down list and click **New** in the upper left of the **Client Protection Policy List**.
3. Click **New**, and set the basic information and the client IP address as follows:



4. Set the IPS inspection level to Medium.

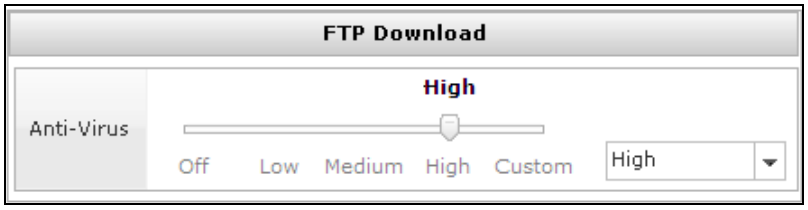
Note: Choose **UTM > IPS > Profiles** and click the default profile **Client_Medium** to view the settings. You can also create a custom IPS profile and use it here.

5. Set mail protection as follows:

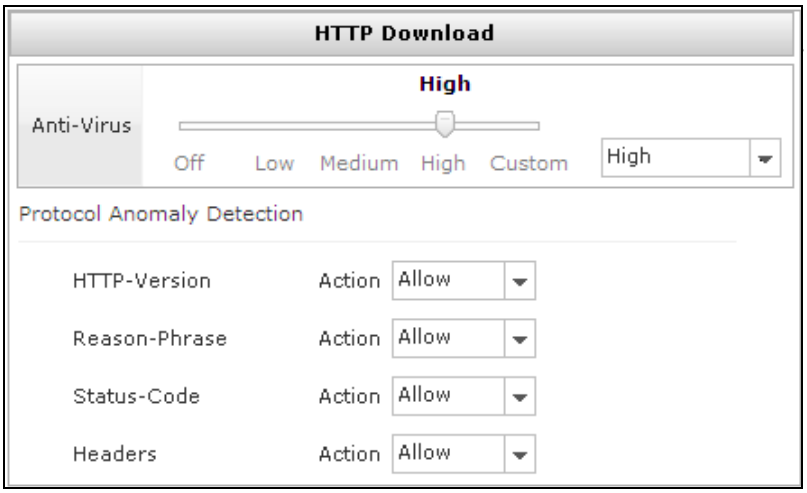


Note: Choose **UTM > Anti-Virus/Anti-Spam > Profiles** and click the default profile **Medium** to view the settings. You can also create a custom anti-virus or anti-spam profile and use it here.

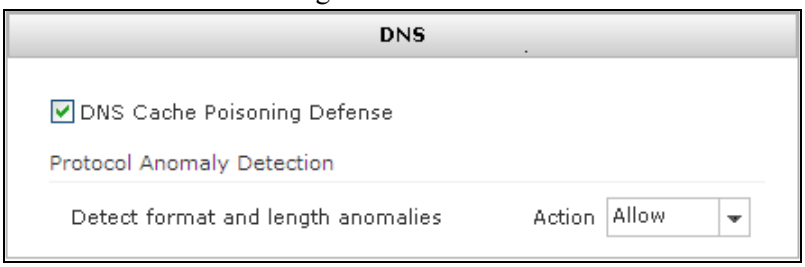
6. Set the anti-virus scanning level to **High** for **FTP Download**.



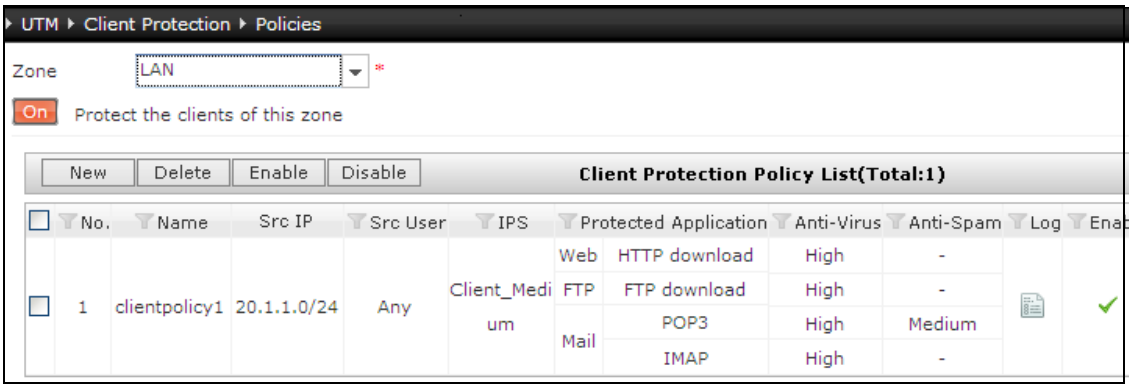
7. Set the anti-virus scanning level to **High** and use protocol anomaly detection default settings for **HTTP Download**.



8. Enable **DNS Cache Poisoning Defense** for DNS client traffic and use the protocol anomaly detection default settings.



9. Click **OK**.



10. Click .

6. Monitor Client Protection

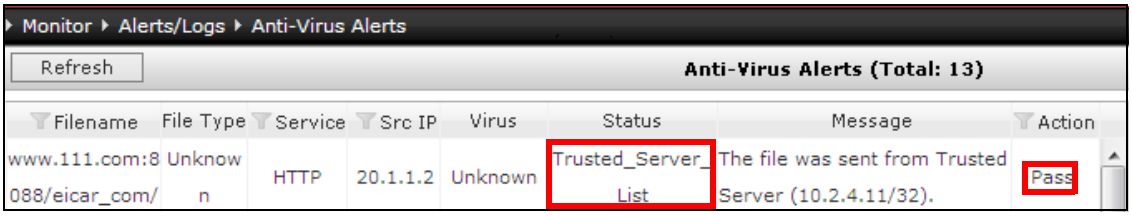
- 6.1 Monitor AV
- 6.2 Monitor AS
- 6.3 Monitor IPS
- 6.4 Monitor DNS Cache Poisoning Defense

6.1 Monitor AV

1. Choose **Monitor > Alerts/Logs > Anti-Virus Alerts**, and view the anti-virus logs.
2. When intranet users access the trusted URLs, FGX will generate logs as follows.
   - URLs matching www.google.com.hk are trusted:

   - URLs matching www.sina.com.cn are trusted:

3. When intranet users access the trusted web server, FGX will generate logs as follows:



4. When the AV engine detects virus in files, FGX will generate logs as follows.
   - When the AV engine is overloaded or the scan fails:

Monitor ▸ Alerts/Logs ▸ Anti-Virus Alerts

Anti-Virus Alerts (Total: 32) << < 1/2 >

Profile	Filename	File Type	Service	Src IP	Virus	Status	Message	Action
High	testtarfile.tar	tar	FTP	20.1.1.2	Unknown	AV_Failure	The AV engine was overloaded or the scan failed.	Pass

   - When the scanned file is oversized:

Monitor ▸ Alerts/Logs ▸ Anti-Virus Alerts

Anti-Virus Alerts (Total: 32) << < 1/2 > >>

Profile	Filename	File Type	Service	Src IP	Virus	Status	Message	Action
High	wireshark-setup-1.0.6.exe	exe	FTP	20.1.1.2	Unknown	File_Oversize	File is too large.	Pass

   - When the nesting levels of the scanned archive exceeds the limit:

Monitor ▸ Alerts/Logs ▸ Anti-Virus Alerts

Anti-Virus Alerts (Total: 32) << < 1/2 >

Profile	Filename	File Type	Service	Src IP	Virus	Status	Message	Action
High	21.7z	7z	POP3	20.1.1.2	Unknown	Archive_File	The nesting levels of the archive file exceed the limit (20).	Block

   - When FGX detects files sent from trusted URLs:

Monitor ▸ Alerts/Logs ▸ Anti-Virus Alerts

Anti-Virus Alerts (Total: 32) << < 1/2 >

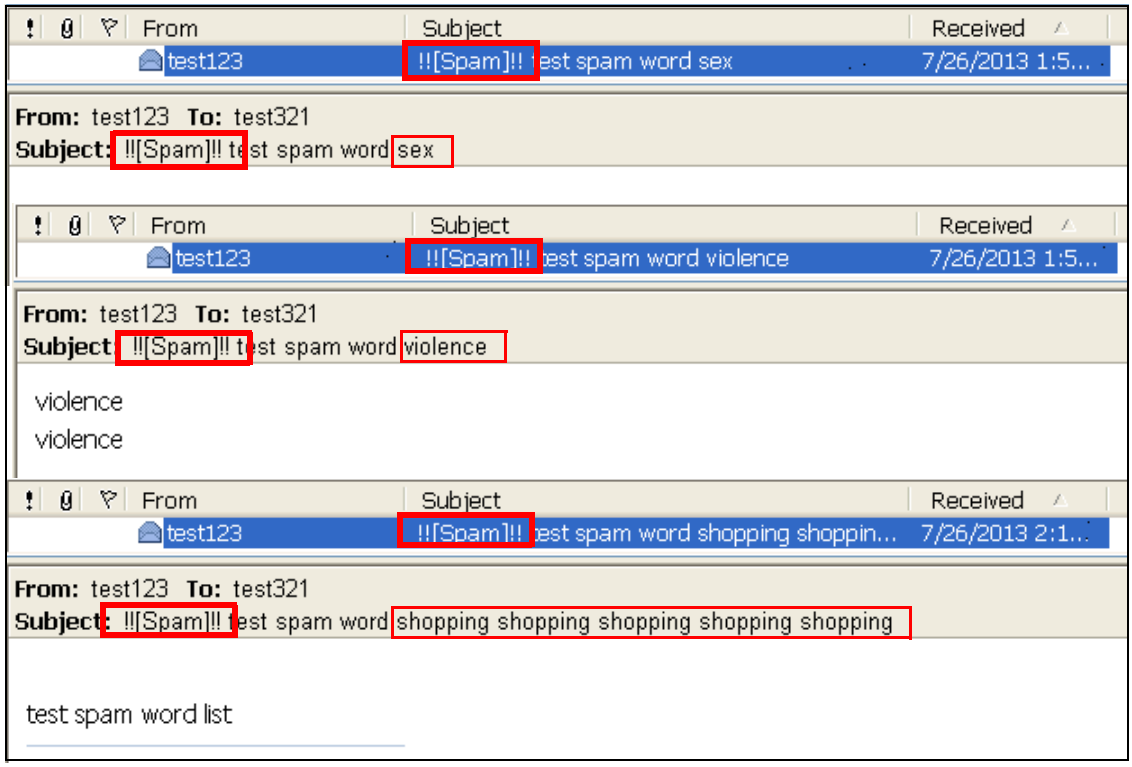
Filename	File Type	Service	Src IP	Virus	Status	Message	Action
scrollpic.js	Unknown	HTTP	20.1.1.2	Unknown	Trusted_URL_List	The file was sent from Trusted URL (www.sina.com.cn/js/index/96/scrollpic.js).	Pass
gen_204	Unknown	HTTP	20.1.1.2	Unknown	Trusted_URL_List	The file was sent from Trusted URL (www.google.com.hk/gen_204).	Pass

6.2 Monitor AS

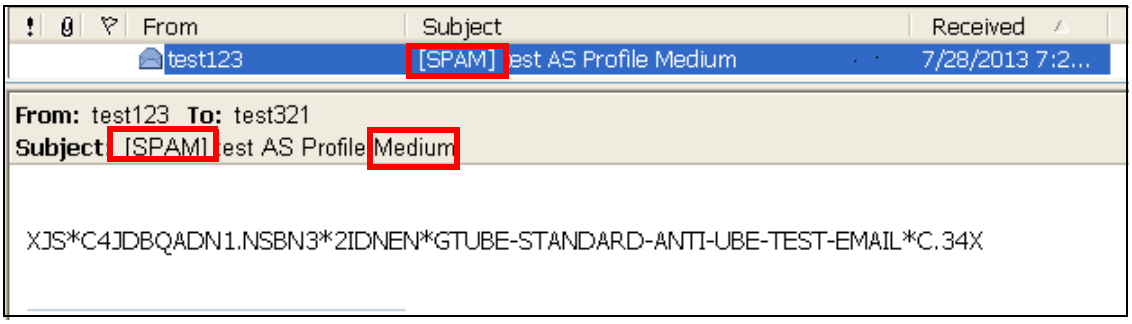
1. E-mails to the allowed recipient will be allowed by FGX and a log will be generated.
2. E-mails from the blocked sender will be blocked by FGX and the recipient will receive a notification message as follows:

3. E-mails to the blocked recipient will be blocked by FGX and the recipient will receive a notification message as follows:

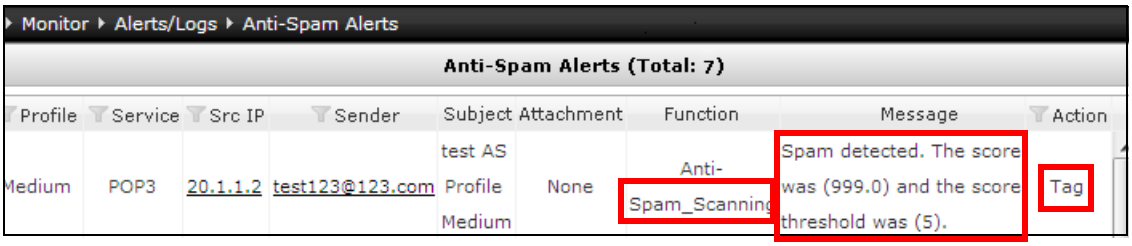
4. When e-mails contain specified spam words and the total score reaches the threshold, FGX will drop the original e-mail and send a notification message to the recipient as follows:



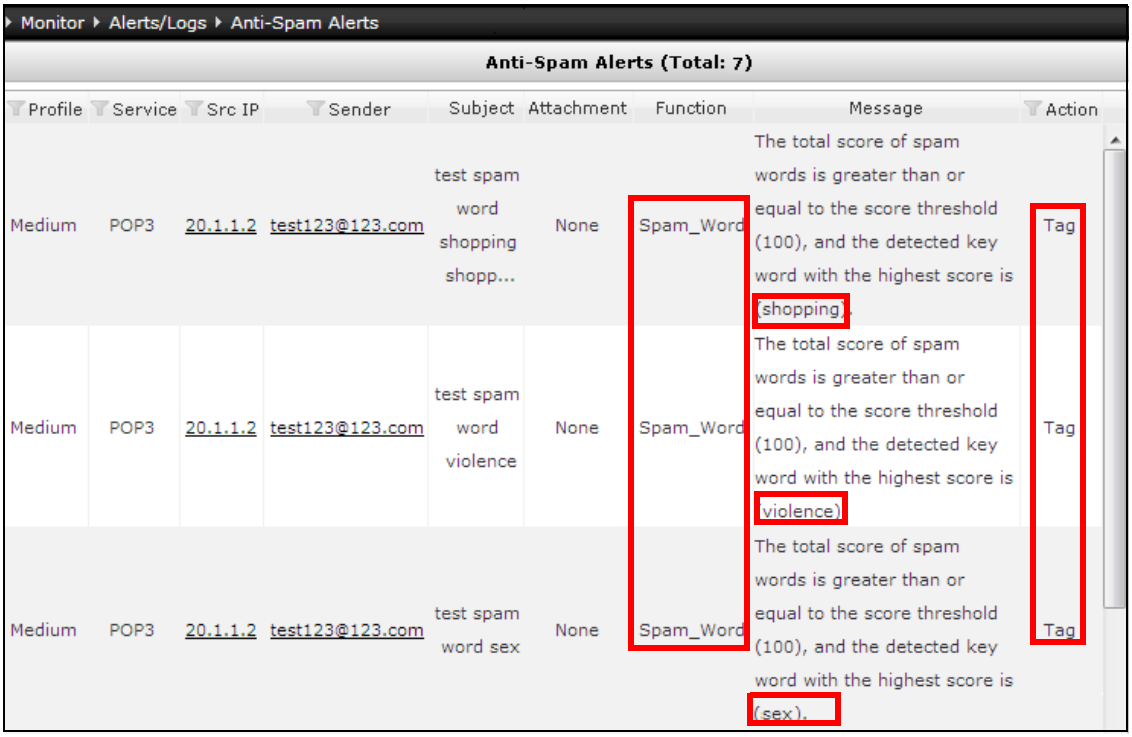
5. According to anti-spam rules in profile Medium specified in the client protection policy, FGX will drop the original e-mail and send a notification message to the recipient:



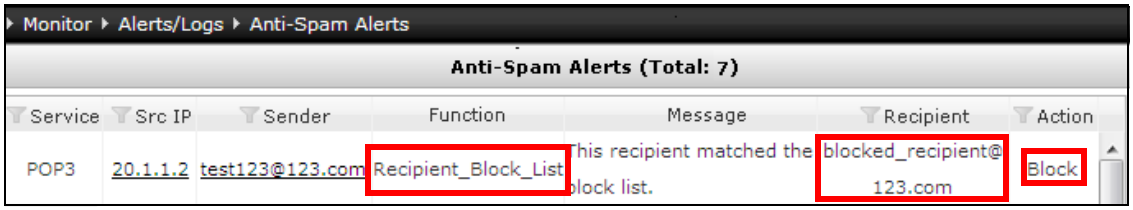
6. Choose **Monitor > Alerts/Logs > Anti-Spam Alerts**, and view the generated logs.
   - When the anti-spam engine detects spam:



   - When FGX detects spam by matching emails against the spam word list:



- Recipient block list:



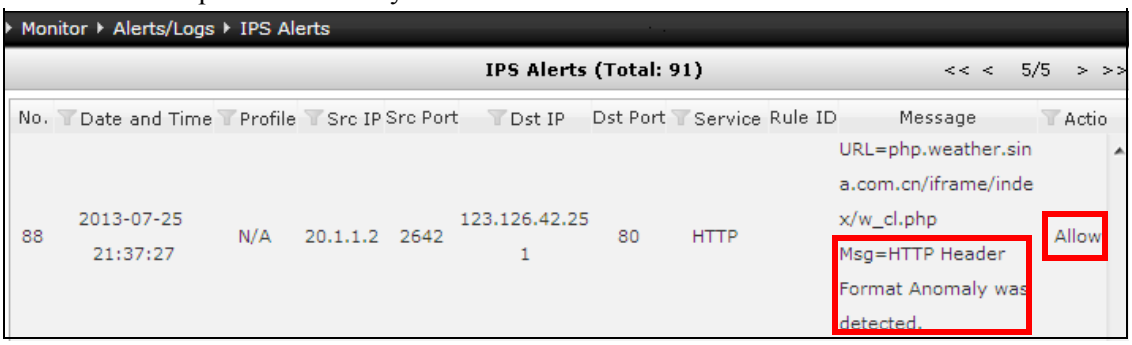
- Sender block list:

- Recipient allow list:

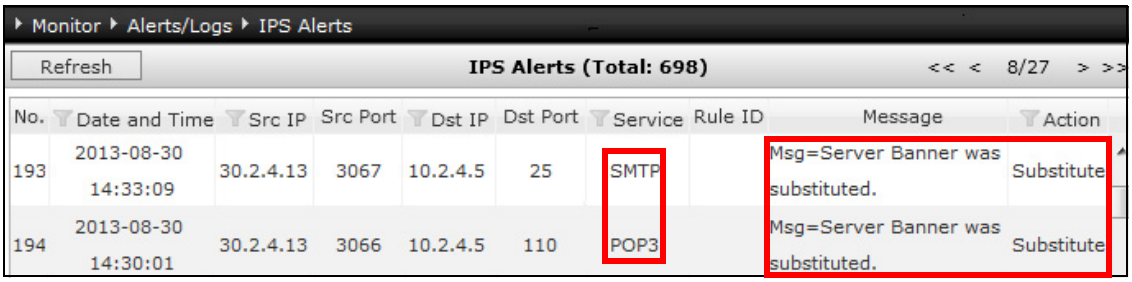
Note: You can click the hyperlinks on the monitoring page to edit the source IP or sender address settings if you find configuration mistakes.

6.3 Monitor IPS

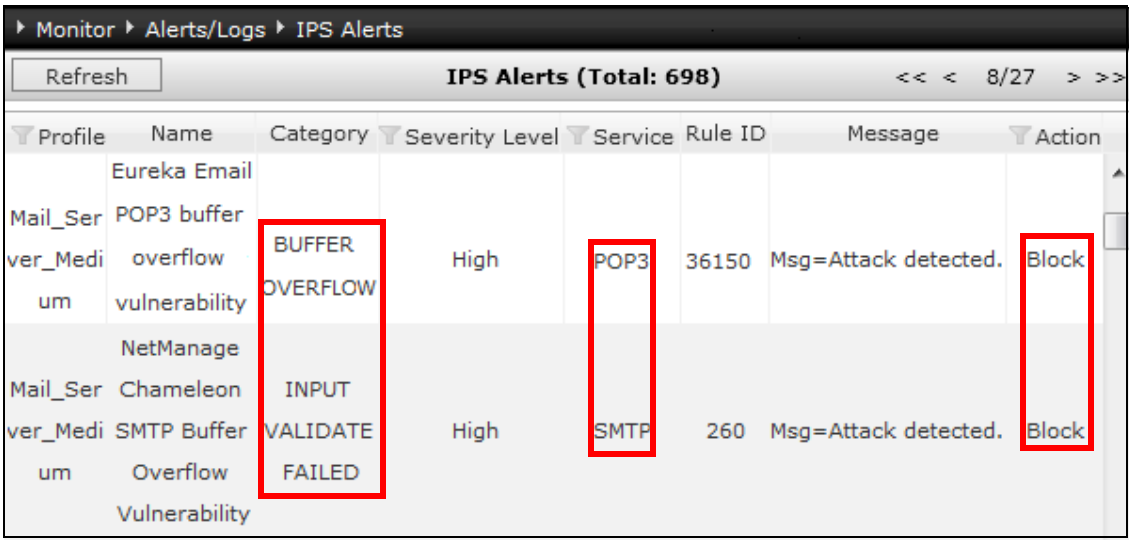
1. Choose **Monitor > Alerts/Logs > IPS Alerts**, and view the generated logs.
2. View HTTP protocol anomaly detection alerts:



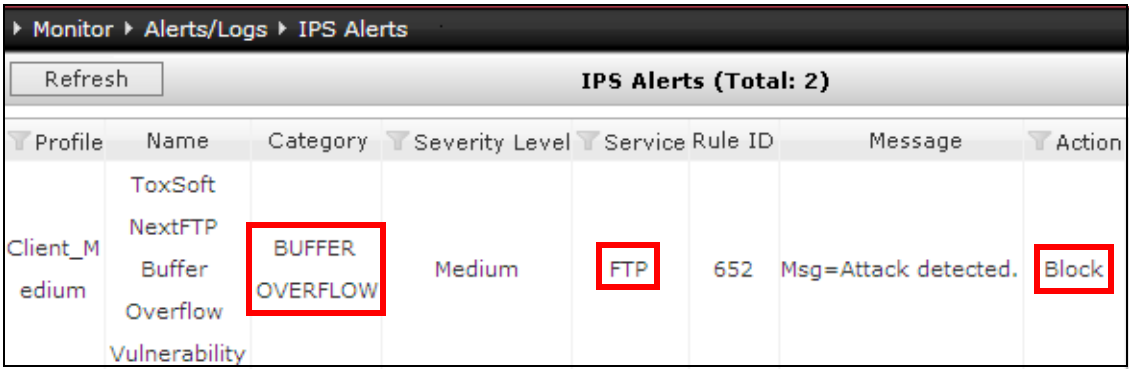
3. View mail (SMTP & POP3) server protection alerts and attack alerts.
   - View server banner information replacement alerts:



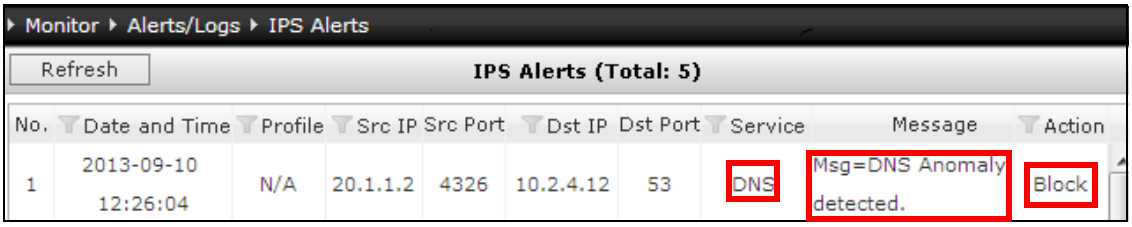
   - View POP3 and SMTP attack alerts:



4. View FTP attack alerts:

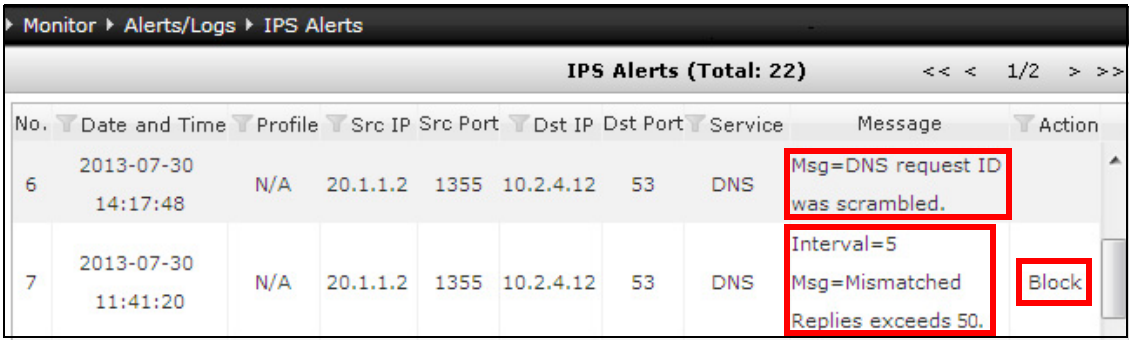


5. View DNS protocol anomaly detection alerts:



6.4 Monitor DNS Cache Poisoning Defense

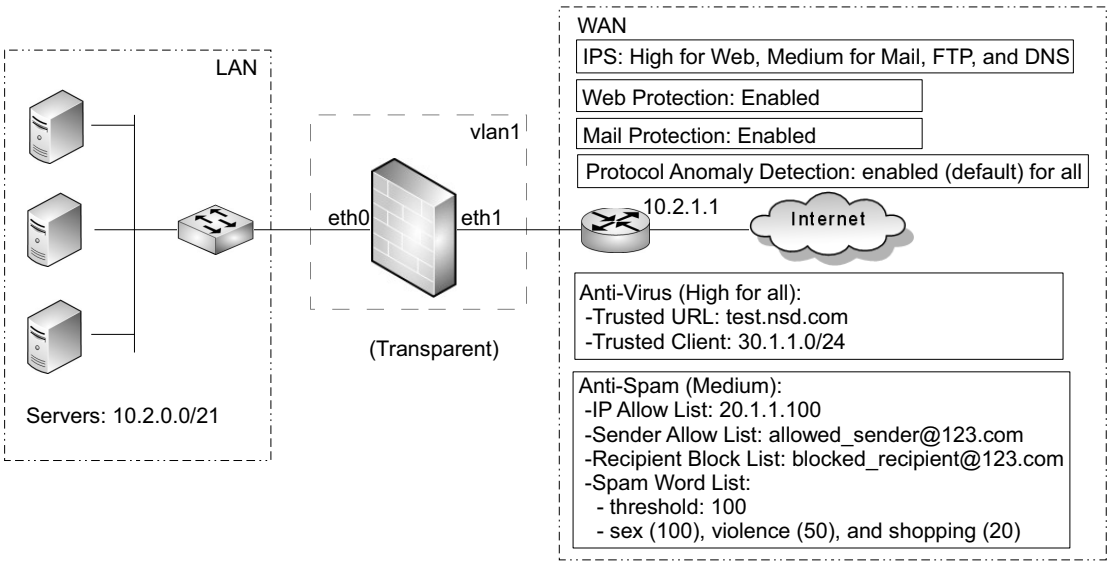
1. UTM will randomize the IDs of DNS requests sent by the protected client to defend against attacks using the request ID sequence.
2. If the number of mismatched replies detected within the specified interval reaches the threshold, the DNS requests will be dropped and a system log is generated.
3. Choose **Monitor > Alerts/Logs > IPS Alerts**, and view the generated DNS logs:



Example 3: Typical Application of UTM Server Protection

As shown below, a company deploys several servers in LAN providing service to the Internet. To protect servers from the Internet threats, the enterprise network administrator can configure web, mail, FTP, and DNS server protection policies on FGX.

Figure 47 Typical Application of UTM Server Protection

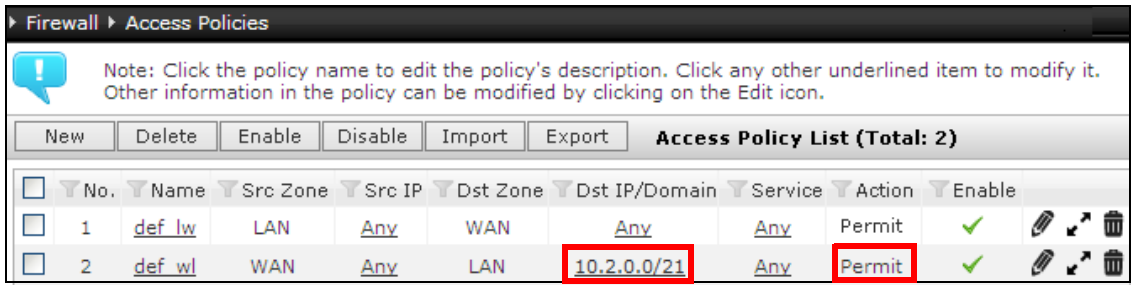


If you have chosen Transparent Mode and the above topology when you initialized FGX (using the initialization wizard), then the configuration steps include:

1. Modify Access Policies
2. Configure Anti-Virus
3. Configure Anti-Spam
4. Create Server Protection Policies
5. Configure Web Protection
6. Configure Mail Protection
7. Monitor Server Protection

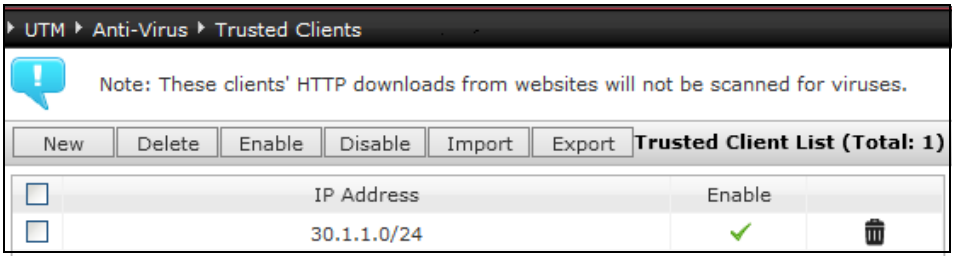
1. Modify Access Policies

1. Choose **Firewall > Access Policies**.
2. Modify the access policies as follows:



2. Configure Anti-Virus

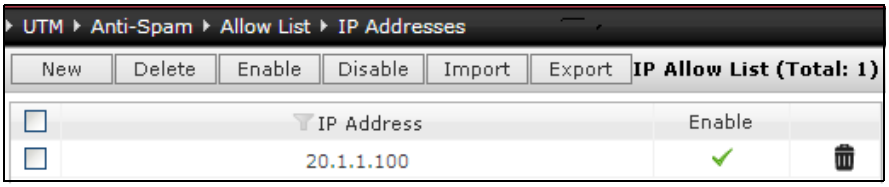
1. Choose **UTM > Anti-Virus > Trusted Clients**.
2. Add a trusted client 30.1.1.0/24.



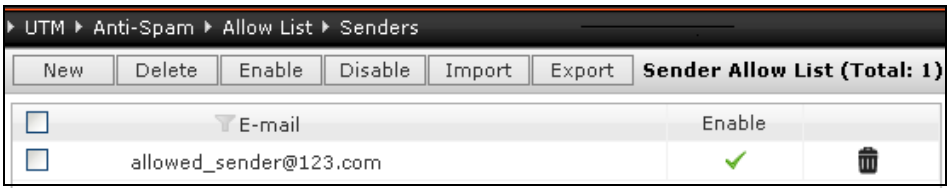
3. After you add server protection policies enabling anti-virus, requests from clients in subnet 30.1.1.0/24 will not be inspected for virus.

3. Configure Anti-Spam

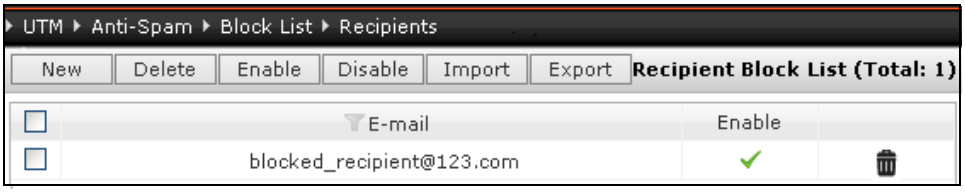
1. Choose **UTM > Anti-Spam > Allow List > IP Addresses**.
2. Add an allowed IP address 20.1.1.100.



3. Then e-mails sent to or from this IP address will be allowed after the corresponding mail server protection policy is enabled.
4. Choose **UTM > Anti-Spam > Allow List > Senders**.
5. Add an allowed sender e-mail address allowed_sender@123.com.



6. Then e-mails sent from this e-mail address will be allowed after the corresponding mail server protection policy is enabled.
7. Choose **UTM > Anti-Spam > Block List > Recipients**.
8. Click **New** and add a recipient address blocked_recipient@123.com.



9. Then e-mails sent to this e-mail address will be blocked.
10. Configure the spam word list. The same as Example 2.

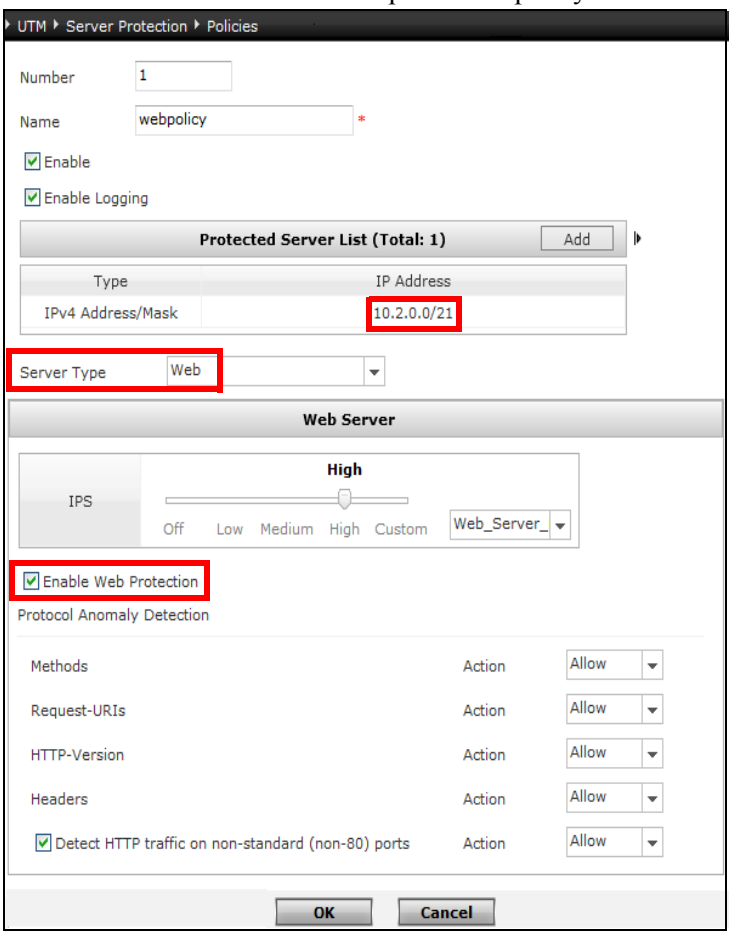
4. Create Server Protection Policies

1. Choose **UTM > Server Protection > Policies**.
2. Choose **LAN** from the **Zone** drop-down list, and click **On** to enable the server protection function. Create the following policies:

- 4.1. Web Server Protection Policy
- 4.2. Mail Server Protection Policy
- 4.3. FTP Server Protection Policy
- 4.4. DNS Server Protection Policy

4.1. Web Server Protection Policy

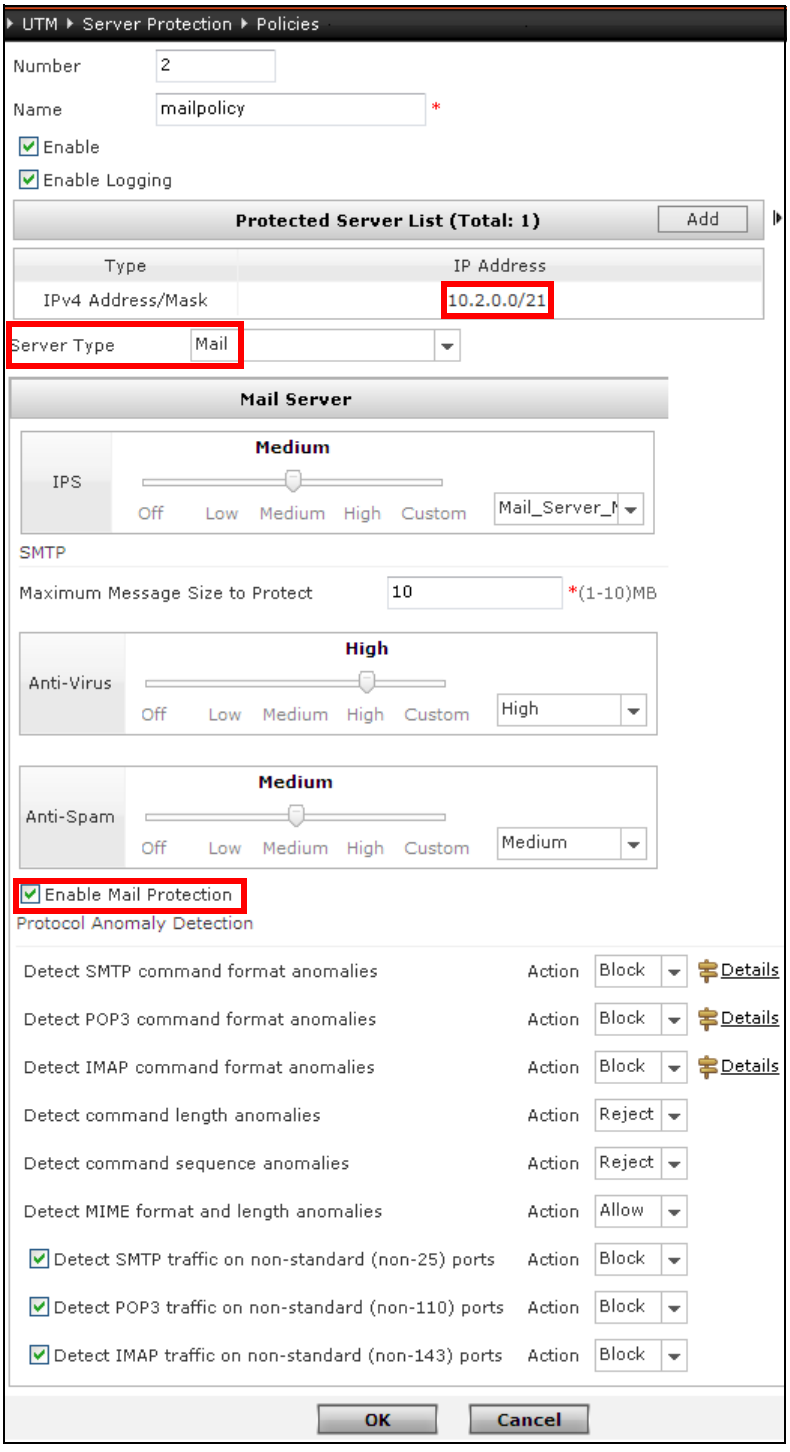
3. Click **New** to create a server protection policy for the Web servers within LAN as follows:



4. Click **OK**.

4.2. Mail Server Protection Policy

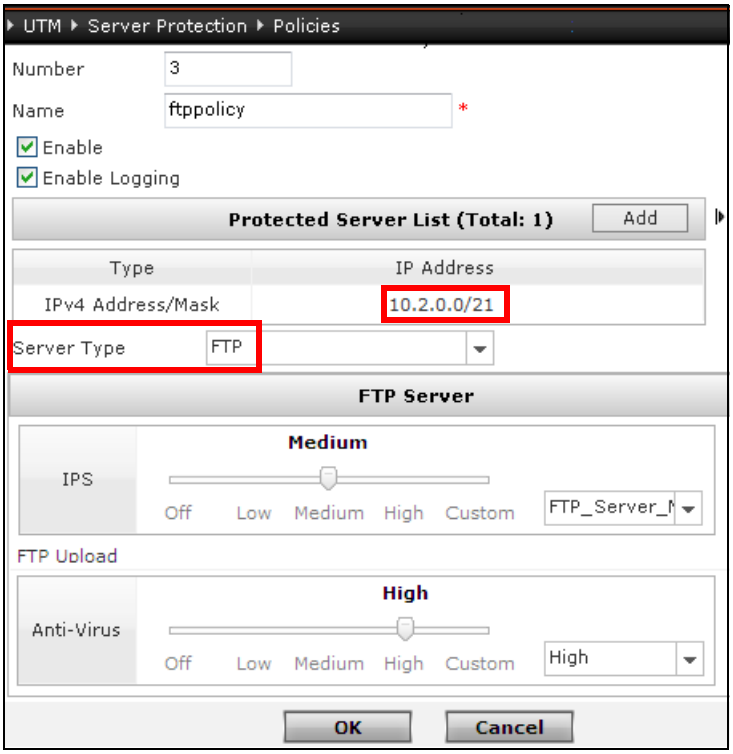
5. Create another server protection policy for the mail servers within LAN as follows:



6. Click **OK**.

4.3. FTP Server Protection Policy

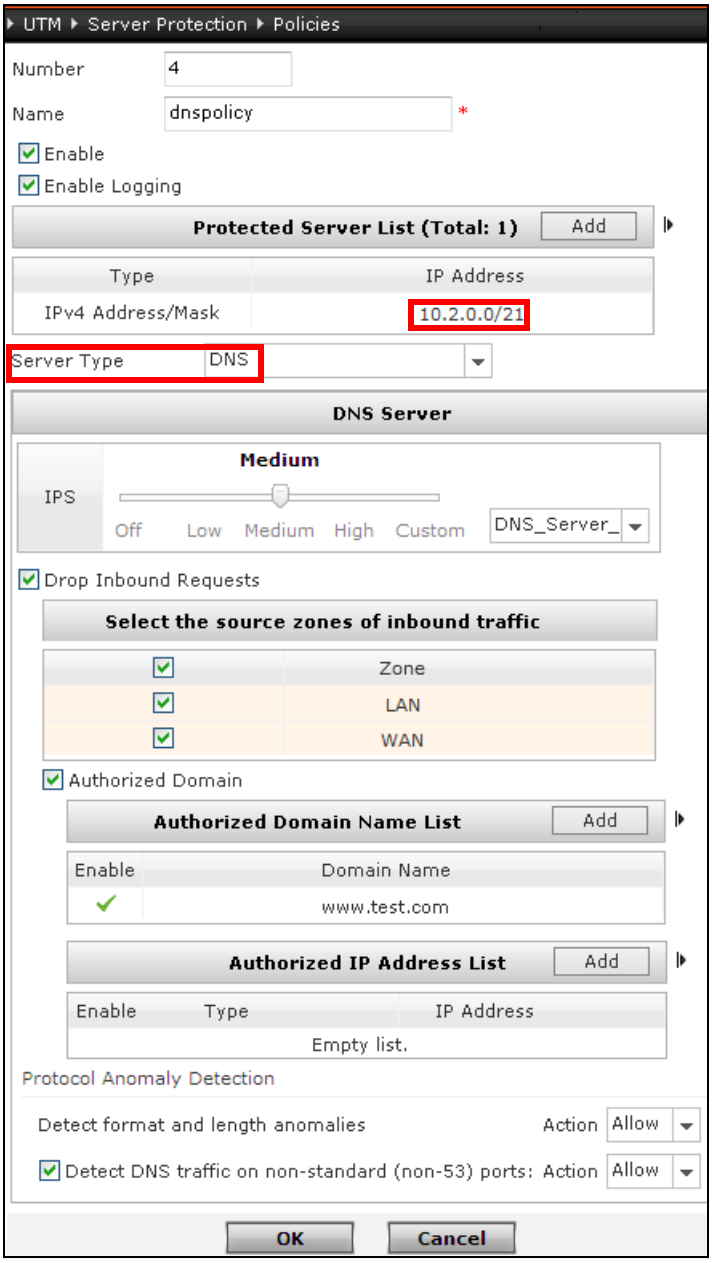
7. Create a server protection policy for the FTP servers within LAN as follows:



8. Click **OK**.

4.4. DNS Server Protection Policy

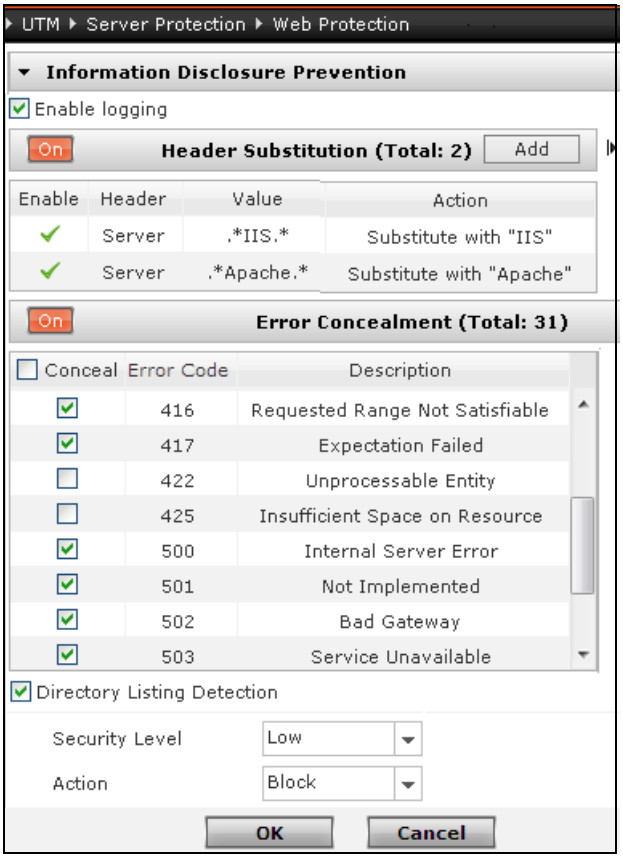
9. Create a server protection policy for the DNS servers within LAN as follows:

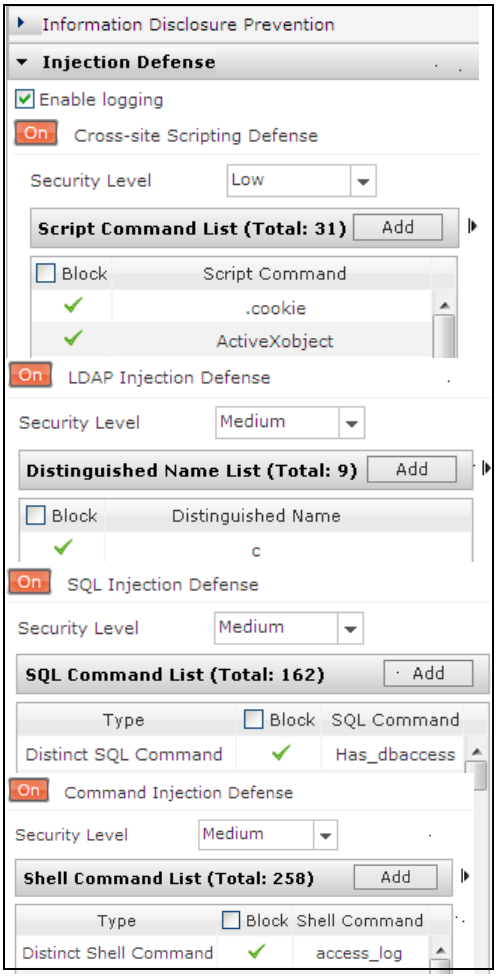


10. Click **OK**.

5. Configure Web Protection

1. Choose **UTM > Server Protection > Web Protection**.
2. Enable all functions of Information Disclosure Prevention and enable the logging function.





3. Click **OK**.

6. Configure Mail Protection

1. Choose **UTM > Server Protection > Mail Protection**.
2. Enable Information Disclosure Prevention and the logging function.

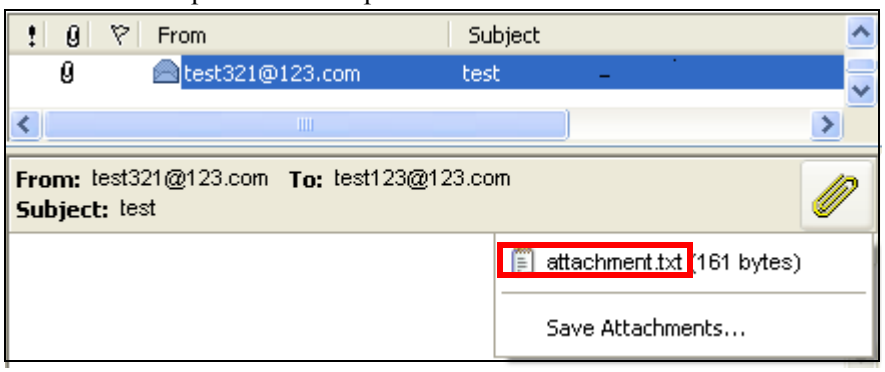
3. Click **OK**.
4. Click .

7. Monitor Server Protection

- 7.1 Monitor AV
- 7.2 Monitor AS
- 7.3 Monitor IPS

7.1 Monitor AV

1. When e-mail attachments are detected to be infected by virus or reaching restriction limits, FGX will replace it with a predefined or user-defined notification message attachment.



   - When the nesting levels of an archive attached reach the limitation (20), the replacing attachment contains the following notification message:

```
The nesting levels of the archive file exceeds the limit(20). 21.7z is blocked.
```

   - When an attachment file is detected to be infected by virus, the replacing attachment contains the following notification message:

```
The attachment eicar.com is stripped.
<<Dangerous attachment has been stripped.   The file "eicar.com" has been stripped
because of a virus. It was infected with the "Eicar-Test-Signature.UNOFFICIAL" virus. >>
```

2. When detecting that an attachment of an e-mail message or a file downloaded from an FTP server is infected, FGX will block files (except for passing oversized files according to the High profile used by policies) and generate alerts.
3. Choose **Monitor > Alerts/Logs > Anti-Virus Alerts**, and view the generated alert logs.
   - When virus signature scanned:

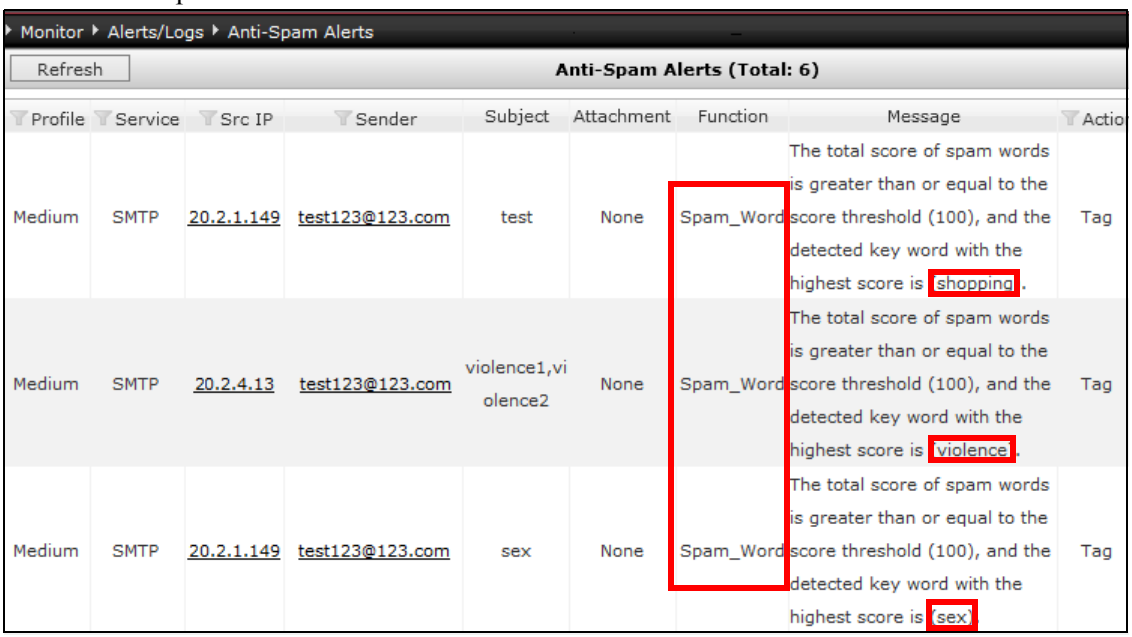
- When file is oversized:

- When archive's nesting levels exceed the limit:

7.2 Monitor AS

1. In server protection, e-mails matching the allow list will be allowed and those matching the block list will be blocked, but FGXwill not send notification e-mails to the clients as in client protection.
2. Choose **Monitor > Alerts/Logs > Anti-Spam Alerts**, and view the generated logs.

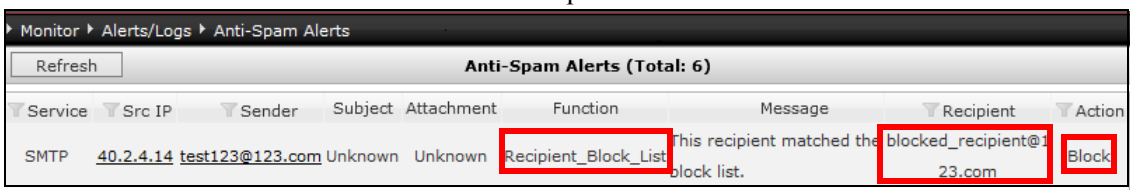
- When spam words detected:



- When detects emails sent to or from allowed IP addresses:

- When detects emails sent from allowed senders:

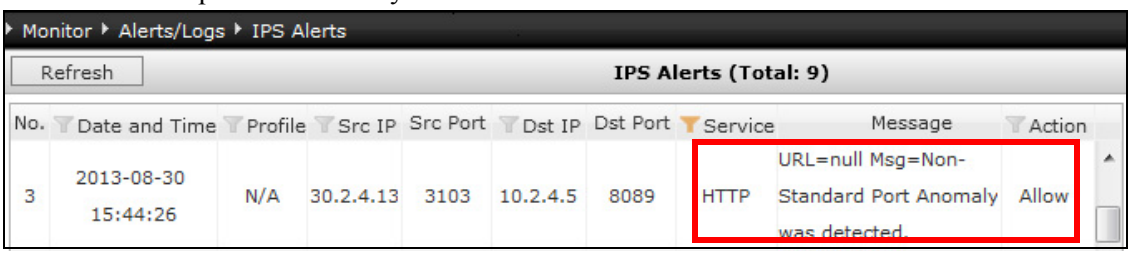
- When detects emails sent to blocked recipients:



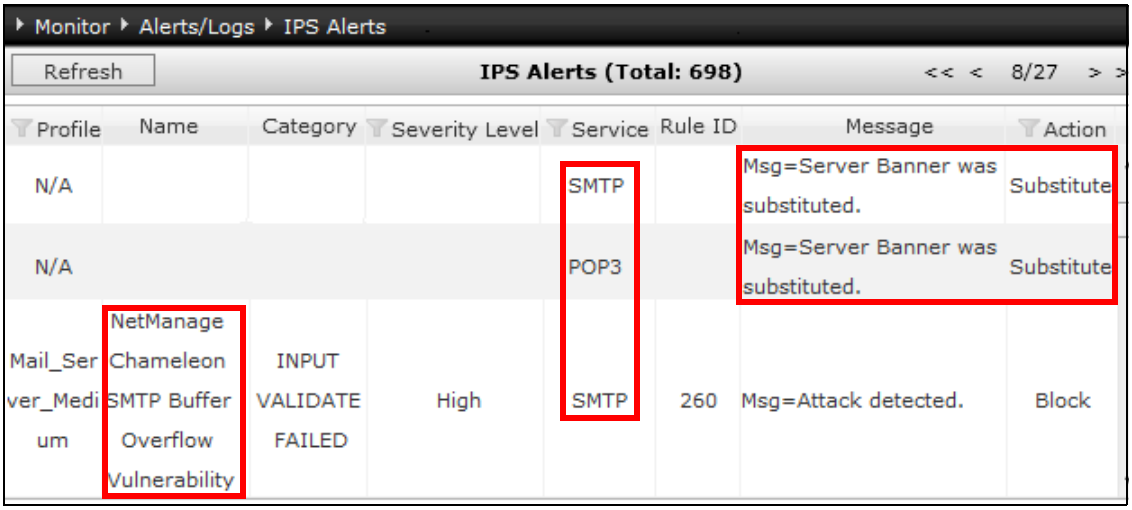
3. Click the hyperlinks on the monitoring page to change anti-spam settings if you find fault reports.

7.3 Monitor IPS

1. Choose **Monitor > Alerts/Logs > IPS Alerts**, and view the generated logs.
2. View HTTP protocol anomaly detection alerts:

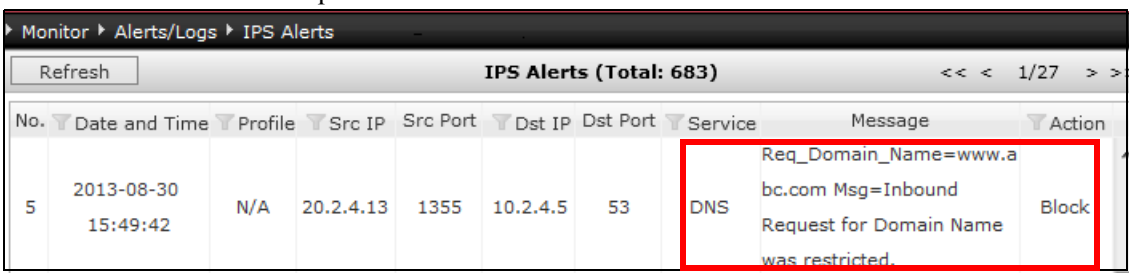


3. View mail (SMTP & POP3) protocol anomaly detection and server protection alerts:



4. View FTP server protection alerts:

5. View DNS inbound request restriction alerts:



10.5. Parameter reference

This section lists parameters for:

- 10.5.1. Overview
- 10.5.2. Export Control
- 10.5.3. Client Protection
- 10.5.4. Server protection
- 10.5.5. Anti-Virus
- 10.5.6. Anti-Spam
- 10.5.7. IPS
- 10.5.8. Notification Messages

10.5.1. Overview

Overview page shows the UTM information of all zones.

Table 170 Parameters of UTM Overview Page

Column	Description
Zone	The zone on which UTM information is configured.
Export Control	Control the outgoing traffic, including: • **Application Control**—control typical application traffic to the Internet. • **URL Filtering**—filter URLs (block high-risk or inappropriate websites). • **DNS Control**—block DNS queries for unauthorized domain names. • **Page Filtering**—filter the content of web pages.
Protection	Protect clients or servers of specified zones.

10.5.2. Export Control

Export control is used to control user traffic on the outgoing zones for security. This section includes:

- 10.5.2.1. (Export Control) Policies
- 10.5.2.2. Application Control
- 10.5.2.3. URL Filtering
- 10.5.2.4. DNS Domain Blacklist
- 10.5.2.5. Page Filtering

10.5.2.1. (Export Control) Policies

Export control policies include application control policies, URL filtering policies, DNS domain blacklist switch, and page filtering switch.

10.5.2.1.1. Application Control Policies

Application control policies define which applications should be inspected for security. You can enable or disable application control policies per zone.

The following describes how FGX checks packets against application control policies:

1. Determine the policy with the highest priority (lowest number) that matches the source zone, IP address and source user. If no match, then pass the packet without application control.
2. If the profile of the matching policy contains:
   a. a matching application entry, then process the packet/session as specified in the entry.
   b. no matching entry, then process the packet/session according to the default action for unlisted applications.

Note: If the application is not in the Application List (cannot be identified by FGX), allow the packet and the session it belongs to without application control.

Table 171 Parameters of Application Control Policies

Parameter	Description
On/Off	Enable or disable application control for a specified zone.
No.	Application control policy priority. 1-80,000. 1 is highest priority. If the number of a new policy already exists, the new policy will be inserted above the existing one. If the number is not specified, it will be added to the end of the policy list.
Name	Application control policy name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces.
Src Zone	Any by default.

Table 171 Parameters of Application Control Policies (*continued*)

Parameter	Description
Src IP	Can be: • **Any** (default) • **Any IPv4 Address** • **Any IPv6 Address** • **Use the Following List—**user-specified IP addresses, up to 4,096 IP addresses or address ranges.
Src User	Can be: • **Any** (default)**—**authenticated or unauthenticated users. • **Any Authenticated User** • **Use the Following List—**Can include externally authenticated users not created on FGX. Each policy can have up to 4,096 source users.
Profile	Shows the name of the profile used by an application control policy.
Log	Logging is enabled for an application control policy by default.
Enable	Application control policy is enabled by default.

Note: To view the monitoring information on Application Control, choose **Monitor > Alerts/ Logs > Application Control Alerts**.

10.5.2.1.2. URL Filtering Policies

URL filtering policies define traffic to which URLs are allowed or denied. You can create and enable or disable URL filtering policies per zone.

The following describes how FGX checks packets against URL filtering policies:

1. Determine the policy with the highest priority (lowest number) that matches the source zone, IP address and source user. If no match, then pass the packet without URL filtering.
2. If the matching policy contains the packet URL in the (in order of descending priority)
   a. whitelist: pass the packet.
   b. blacklist: block the packet.
   c. URL category list: process the packet as specified for the matching category.
   d. no matching category, then process the packet according to the default action for unknown categories.

Table 172 Parameters of URL Filtering Policies

Parameter	Description
On/Off	Enable or disable URL filtering for a specified zone.
No.	URL filtering policy priority. 1-80,000. 1 is highest priority. If the number of a new policy already exists, the new policy will be inserted above the existing one. If the number is not specified, it will be added to the end of the policy list.

Table 172 Parameters of URL Filtering Policies (*continued*)

Parameter	Description
Name	URL filtering policy name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces.
Src Zone	Any by default.
Src IP	Can be: • **Any** (default) • **Any IPv4 Address** • **Any IPv6 Address** • **Use the Following List—**user-specified IP addresses, up to 4,096 IP addresses or address ranges.
Src User	The user can be any of the following types: • **Any** (default) • **Any Authenticated User** • **Use the Following List—**Can include externally authenticated users not created on FGX. Each policy supports up to 4,096 users.
Profile	Shows the name of the profile used by a URL filtering policy.
Log	Logging is enabled for a URL filtering policy by default.
Enable	URL filtering policy is enabled by default.

Note: To view the monitoring information on URL Filtering, choose **Monitor > Alerts/Logs > URL Filtering Alerts**.

10.5.2.2. Application Control

Application control controls the outgoing traffic of applications. This section includes:

- 10.5.2.2.1. Application Control Profiles
- 10.5.2.2.2. Custom Applications
- 10.5.2.2.3. Application List
- 10.5.2.2.4. (Application List) Update

Note: To view the monitoring information on Application Control, choose **Monitor > Alerts/ Logs > Application Control Alerts**.

10.5.2.2.1. Application Control Profiles

An application control profile lists applications to control and specifies the action for each application. FGX supports up to 1,024 application control profiles in all Vsys, and each profile supports up to 4,096 applications or filter-based application categories.

Table 173 Parameters of Application Control Profiles

Parameter	Description
Name	Application control profile name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces.
In Use	Click to view the policies using an application control profile. An application control profile can be used by multiple application control policies. Profiles in use cannot be deleted.
Description	Application control profile description. 0-255 UTF-8 characters. Cannot contain ? ” ' \ < > or &.
Default action for applications not in the following application list	Block (default) and Pass.
Application List	The list supports up to 256 entries. • **Number—**priority of an application in an application control profile. The smaller the number, the higher the priority. If the number of a new application entry already exists, the new entry will be inserted above the existing one. If the number is not specified, it will be added to the end of the application list. • **Type—**method you add applications, Filter (default) and Application. You can add multiple applications by setting filter parameters. You can also add a single application by name. • **Application Name—**the name of an application or filter parameters. • **Action—**Pass and Block (default).

10.5.2.2.2. Custom Applications

In application control profiles you can configure applications to control. By default, applications are matched according to RFC standards. For specific applications, you can add custom matching conditions. Adding custom applications can speed up the forwarding of application data. Custom applications have a higher matching priority than the predefined applications.

A "custom application" restricts application control for a specific application by specifying the destination IP address, transport protocol, and destination port. One application can be specified with a single application protocol (DNS, SIP, etc.). The destination IP address, transport protocol, and the destination port of a custom application cannot be the same as those of another at the same time. The custom application list contains up to 10,240 groups of destination IP addresses and destination ports.

Table 174 Parameters of Custom Applications

Parameter	Description
Application	The application you want to add custom matching conditions for (any application in the application list).
Application Protocol	The application layer protocol used by a custom application, including DNS, FINGER, FTP, H.323, HTTP, IMAP, MS-RPC, MSSQL, MYSQL, NETBIOS, NNTP, ORACLE, POP2, POP3, RTSP, SIP, SMB, SMTP, SNMP, SSL, SUN-RPC, TELNET, TFTP, Tuxedo, WINS, and X11.
Dst IP	The destination IP address of a custom application.
Transport Protocol	The transport layer protocol used by a custom application, TCP (default) and UDP.
Dst Port	The destination port of a custom application,1-65,535.

10.5.2.2.3. Application List

The application list shows the RFC standard name, category, subcategory, technology, and risk level of all applications FGX can identify. Filters are **Any** by default. Click **Search** to view all applications that FGX can identify.

Table 175 Parameters of Application List

Parameter	Description
Category	The category of a predefined application in the application list, such as Business Applications, Communication, General-Internet, Multi-Media, and Networking. Any indicates any category.
Subcategory	The subcategory of a predefined application in the application list, such as Audio-Streaming, Auth-Service, Content-Sharing, Database, Email, Encrypted-Tunnel, Erp-Crm, File-Sharing, Game, General-Business, Instant-Messaging, Internet-Conferencing, Internet-Proxy, Internet-Utility, IP-Protocol, Management, Network Service, Office-Programs, Photo-Video, Remote-Access, Routing, Social-Networking, Software-Update, Storage-Backup, Voip, and Web-Posting. Any indicates any subcategory.
Technology	The technology used by a predefined application in the application list, such as Browser-Based, Client-Server, Network-Protocol, and Peer-to-Peer. Any indicates any technology.
Risk	The risk level of a predefined application in the application list.  ,  ,  ,  , and  are from the lowest to the highest. Any indicates any risk level.
Clear Filters	Reset all filter conditions and clear the search result.
Search	Search for applications matching filter conditions.
Search Results	Shows applications matching the filter conditions. Put mouse cursor on an application name to view the application description.

10.5.2.2.4. (Application List) Update

FGX uploads rule update packages manually or automatically to overwrite the current applications in the system. An uploaded update takes effect without rebooting FGX. Rollback is not supported.

Limitations to application list update:

- License—The application control function and application list update require FW license.
- Vsys—Application list updates can be done only in the root system. All virtual systems share the same application list.

Table 176 Parameters of Application List Update History

Parameter	Description
Rule Base	The name of the application list rule base is Application-Control. Cannot be changed.
Rule Version	The most recent rule version of the application list base.
Engine Version	The engine version of the application list base.
Last Update	Time of last update
Show/Export Update History	Click to view or export the update history of the application list base. FGX supports up to 50 records.

Table 177 Parameters of Application List Update Mode

Parameter	Description
Update Server Address	The URL address of the update server in an automatic update. It can be an IPv4 address, IPv6 address, or a domain name. Default is update.nsdcloud.net/autoupdate.
Update Mode (Automatic)	The method of performing an automatic update.
Schedule	The schedule for FGX to perform automatic update. The automatic update starts at the specified time and will be done within two hours. By default, an automatic update is done every day at 22:00.
Update Immediately	Click it for FGX to get an update package from the specified update server and install it.
Upload Package	Upload a local update package.

10.5.2.3. URL Filtering

UTM URL filtering controls user access to URLs. This section includes:

- 10.5.2.3.1. (URL Filtering) General Settings
- 10.5.2.3.2. (URL Filtering) Profiles
- 10.5.2.3.3. URL Blacklists & Whitelists
- 10.5.2.3.4. (URL Category) Update

Note: To view the monitoring information on URL Filtering, choose **Monitor > Alerts/Logs > URL Filtering Alerts**.

10.5.2.3.1. (URL Filtering) General Settings

Table 178 Parameters of URL Filtering General Settings

Parameter	Description
When URL filtering engine fails	Set the action for FGX to take when URL filtering engine fails. The actions include Allow (default) and Block.
URL Category Search	Enter the URL of which you want to search for the category and click **Search** to view the category or categories of the URL.

10.5.2.3.2. (URL Filtering) Profiles

A URL filtering profile specifies (from highest to lowest priority):

1. a whitelist
2. a blacklist
3. URL categories
   a. Action for specific URL categories
   b. Default action (allow/block) for URLs of unknown categories

FGX supports up to 1,024 URL filtering profiles in all Vsys.

Table 179 Parameters of URL Filtering Profiles

Parameter	Description
Name	URL filtering profile name. 1-63 UTF-8 characters. Cannot be ? , ” ' \ < > & # or spaces.
In Use	Click to view the policies using a URL filtering profile. A URL filtering profile can be used by multiple URL filtering policies. Profiles in use cannot be deleted.
Description	URL filtering profile description. 0-255 UTF-8 characters. Cannot contain ? ” ' \ < > or &.
URL Whitelist	Check it and choose a URL whitelist.
URL Blacklist	Check it and choose a URL blacklist.
URL Category	Enable URL category filtering. • **Default action for URLs of unknown categories—**Allow (default) and Block. • **URL Category List—**Enable or disable URL categories and set the action to each URL category. If a URL matches an enabled URL category, the URL request will be processed according to the action (Allow or Block) set for this category. URLs of disabled URL categories are allowed.

10.5.2.3.3. URL Blacklists & Whitelists

Check request to a URL against URL whitelists and then blacklists. The whitelist has a higher priority. URL blacklists and whitelists can be used by URL filtering profiles.

Each Vsys supports up to eight blacklists and eight whitelists. FGX supports up to 8,000 URLs in all whitelists and 8,000 URLs in all blacklists.

When an HTTP session request to a URL is blocked during URL filtering, a notification message will be sent to the client as a response from the server. For more information, see 10.5.8. Notification Messages.

Table 180 Parameters of URL Blacklists & Whitelists

Parameter	Description
Name	URL blacklist or whitelist name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces. A blacklist and a whitelist cannot have the same name.
Type	The type of a URL list, Blacklist or Whitelist.
Entries	The number of URLs in a URL blacklist or whitelist.
In Use	Click to view the profiles using a URL blacklist or whitelist. A URL blacklist or whitelist can be used by multiple profiles.
Description	URL blacklist or whitelist description. 0-255 UTF-8 characters. Cannot contain ? ” ' \ < > or &.
URL List	Add URLs to a new URL blacklist or whitelist. • **URL—**IP address or a domain name. Wildcards are allowed. 2-255 characters. • **Description—**0-255 UTF-8 characters. Cannot contain ? ” ' \ < > or &. • **Enable—**enable or disable a URL.
Import	Import a URL blacklist or whitelist A blacklist or whitelist with the same name as any existing one cannot be added. When a URL in the imported blacklist or whitelist is already on an existing blacklist or whitelist, the system will prompt whether to add the URL. Duplicate URLs are only imported once. File requirements include: • **File type—**text • **File format—**one URL in each line • **File extension—**.txt

10.5.2.3.4. (URL Category) Update

FGX uploads rule update packages manually or automatically to overwrite the current URL categories. An uploaded update takes effect without rebooting FGX. Rollback is not supported.

Limitations to URL category update:

- License—URL category update requires UFOL license.
- Vsys—URL filtering rule updates can be done only in the root system. All virtual systems share the same URL categories.

Table 181 Parameters of URL Filtering Rule Update History

Parameter	Description
Rule Base	The name of the URL filtering rule base is URL Filtering. Cannot be changed.
Rule Version	The most recent rule version of the URL filtering rule base.
Engine Version	The engine version of the URL filtering rule base.
Last Update	Time of last update.
Show/Export Update History	Click to view or export the update history of the URL filtering rule base. FGX supports up to 50 records.

Table 182 Parameters of URL Filtering Rule Update Mode

Parameter	Description
Update Server Address	The URL address of the update server in an automatic update. It can be an IPv4 address, IPv6 address, or a domain name. Default is update.nsdcloud.net/urlrule.
Update Mode (Automatic)	The method of performing an automatic update.
Schedule	The schedule for FGX to perform automatic update. The automatic update starts at the specified time and will be done within two hours. By default, an automatic update is done every day at 22:00.
Update Immediately	Click it for FGX to get an update package from the specified update server and install it.
Upload Package	Upload a local update package in a manual update.

10.5.2.4. DNS Domain Blacklist

UTM blocks DNS queries for domain names matching the DNS domain blacklist on the outgoing interface. For DNS domain blacklist configurations to take effect, you also must enable DNS domain blacklist for the corresponding zone on Export Control Policies page.

Table 183 Parameters of DNS Domain Blacklist

Parameter	Description
Enable Logging	Enable logging for the DNS domain blacklist.
Domain Blacklist	Settings include: • **Domain Name**—The domain name for which DNS requests will be dropped. The domain blacklist contains up to 2,048 domain names. • **Fuzzy Match**—block DNS queries for a domain name which partly matches a domain name in the domain blacklist. It is disabled by default. • **Enable**—enable or disable a DNS domain blacklist entry.

Note: To view the monitoring information on the DNS domain blacklist, choose **Monitor > Alerts/Logs > IPS Alerts**.

10.5.2.5. Page Filtering

UTM page filtering on the outgoing interface filters the content of HTTP response pages. Page filtering filters web pages that contain user-specified key words. If the user-specified score threshold is reached, the web page will be processed according to the specified action. For page filtering configurations to take effect, you also must enable page filtering for the corresponding zone on Export Control Policies page.

Table 184 Parameters of Page Filtering

Parameter	Description
Score Threshold	The maximum total score of all key words allowed. 100-1,000. Default is 1,000. If the total score of the key words detected in a web page exceeds the specified threshold, process the web page according to the user-specified action.
When the total score of words in a Web page exceeds the score threshold	Allow and Block.
Enable Logging	Enable logging on page filtering.
Word Filtering	List of word filtering rules. The list supports up to 4,096 word filtering rules per Vsys. • **Word—**key word filtered in web pages. 2-32 UTF-8 characters, non-case sensitive. • **Score—**the corresponding score of a key word to be filtered. 1-100. • **Description—**key word description. 0-255 UTF-8 chars. Cannot be ? ” ' \ < > or &. • **Enable—**check to enable a key word.

Note: To view the monitoring information on page filtering, choose **Monitor > Alerts/Logs > IPS Alerts**.

10.5.3. Client Protection

This section includes:

- 10.5.3.1. (Client Protection) Policies
- 10.5.3.2. (Client Protection) Trusted Server List
- 10.5.3.3. (Client Protection) Trusted Mail Address List
- 10.5.3.4. DNS Cache Poisoning Defense

10.5.3.1. (Client Protection) Policies

FGX determines the highest priority (lowest policy number) client protection policy that matches a packet according to the source IP address and source user. The packet is processed as specified in the policy. If there is no matching policy, client protection (IPS, anti-virus, anti-spam, protocol anomaly detection, and DNS cache poisoning defense) is not performed.

Each zone supports up to 1,024 client protection policies.

Table 185 Parameters of Client Protection Policies

Parameter	Description
On/Off	Enable or disable client protection for a specified zone.
No.	Client protection policy priority. 1-1,024. 1 is highest priority. If the number of a new policy already exists, the new policy will be inserted above the existing one. If the number is not specified, it will be added to the end of the policy list.
Name	Client protection policy name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces.
Src IP (Client IP Address)	The IP addresses of protected clients within a specified zone. Can be: • **Any** (default) • **Any IPv4 Address** • **Any IPv6 Address** • **Use the Following List—**user-specified IP addresses, up to 4,096 IP addresses or address ranges. IPv4 and IPv6 addresses cannot be added to the same client protection policy.
Src User	The user from whom packets are sent. Can be one of the following: • **Any** (default) • **Any Authenticated User** • **Use the Following List—**Can include externally authenticated users not created on FGX. Each client protection policy can have up to 4,096 source users.
IPS	Disabled by default. Set the IPS inspection level, Low, Medium, High, and Custom. IPS inspection includes attack signature detection and protocol restriction. For details, see 10.5.7. IPS.

Table 185 Parameters of Client Protection Policies (*continued*)

Parameter	Description
Protected Application	The applications protected by a client protection policy. Can be: • **Mail (POP3, IMAP)** • **FTP (FTP Download)** • **Web (HTTP Download)** • **DNS (DNS Cache Poisoning Defense)**
Anti-Virus	Disabled by default. Set the anti-virus scanning level, Low, Medium, High, and Custom. Configure the anti-virus scanning level for HTTP Download, FTP Download, POP3, and IMAP. For details, see 10.5.5. Anti-Virus.
Anti-Spam	Disabled by default. Set the anti-spam inspection level, Low, Medium, High, and Custom. Configure the anti-spam inspection level for POP3 only. For details, see 10.5.6. Anti-Spam.
Log	Logging is enabled for a client protection policy by default.
Enable	Client protection policy is enabled by default.
Maximum Message Size to Protect	1-10 MB. Default is 10. Configure for POP3 and IMAP. Anti-virus scanning and anti-spam inspection are not performed on mail message parts which exceed the maximum size. Mail size restriction takes effect only when the anti-virus or anti-spam function is enabled and the e-mail does not match any allow list or block list.
Protocol Anomaly Detection	Identify traffic that deviates from RFC specifications. Detect the following anomalies for POP3 and IMAP traffic: • **Detect response format anomalies** • **Detect response length anomalies** • **Detect MIME format and length anomalies** Detect format and length anomalies on the following parts of HTTP download traffic: • **HTTP-Version** • **Reason-Phrase** • **Status-Code** • **Headers** Detect anomalies for DNS traffic: • **Detect format and length anomalies**
DNS Cache Poisoning Defense	Enable or disable DNS cache poisoning defense. For details, see 10.5.3.4. DNS Cache Poisoning Defense.

10.5.3.2. (Client Protection) Trusted Server List

A trusted server list defines the servers trusted within a specified zone. The trusted server list is matched before client protection policies are matched. If the client traffic packet matches a trusted server (1) zone, (2) server type, (3) server IP address / domain name, then the remaining session packets are passed without client protection. Each zone can have one trusted server list (empty and disabled by default) and each list supports up to 32 entries.

Table 186 Parameters of Trusted Server List

Parameter	Description
On/Off	Enable or disable trusted server list for a specified zone.
Name	Trusted server policy name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces.
Zone	The trusted server zone.
IP Address/Domain (Server IP Address)	The IP address or domain name of a trusted server. Can be: • **Any** (default) • **Any IPv4 Address** • **Any IPv6 Address** • **Use the Following List—**user-specified IP addresses or domain names, up to 4,096 IP addresses or address ranges.
Server Type	Can be: • **Any** (default) • **Use the Following List—**includes Web Server, FTP Server, Mail Server, DNS Server, and Other Server.

10.5.3.3. (Client Protection) Trusted Mail Address List

The trusted mail address list is matched after client protection policies are matched but before anti-spam inspection is performed. If the recipient or sender address of an e-mail sent to a protected client can be found in the zone trusted mail address list, the e-mail will not be inspected for client protection. The trusted mail address list in client protection inspects IMAP and POP3 traffic. Each zone can have one trusted mail address list (empty and disabled by default) up to 128 trusted mail addresses or domain names.

Table 187 Parameters of Trusted Mail Address List (Client Protection)

Parameter	Description
On/Off	Enable or disable the trusted mail address list for a specified zone.
Mail Address	The e-mail address or domain name of a trusted server. Anonymous senders are allowed and indicated by "(null)."

10.5.3.4. DNS Cache Poisoning Defense

DNS cache poisoning defense protects clients from DNS cache poisoning attacks. Configure DNS cache poisoning defense globally for all zones and then enable or disable it in a client protection policy per zone.

Table 188 Parameters of DNS Cache Poisoning Defense

Parameter	Description
Enable Logging	Enable logging on DNS cache poisoning defense. You also must enable logging and DNS cache poisoning in the corresponding client protection policies.
Enable DNS Query Scrambling Protection	Randomizes the IDs of DNS requests sent by the protected client to defend against attacks using the DNS request ID sequence.
Detect Frequently Mismatched Replies	It is enabled by default. • **Maximum Mismatched Replies—**1-65,535. Default is 50. When the maximum number of mismatched replies is reached, an attack is considered to occur. • **Interval—**the interval for detecting mismatched replies. 1-60 seconds. Default is 5.

Note: To view the monitoring information on DNS cache poisoning defense, choose **Monitor > Alerts/Logs > IPS Alerts**.

10.5.4. Server protection

This section includes:

- 10.5.4.1. (Server Protection) Policies
- 10.5.4.2. (Server Protection) Trusted Client List
- 10.5.4.3. (Server Protection) Trusted Mail Address List
- 10.5.4.4. Web Protection
- 10.5.4.5. Mail Protection

10.5.4.1. (Server Protection) Policies

FGX determines the highest priority (lowest policy number) server protection policy that matches a packet according to server IP and server type. The packet is processed as specified in the policy. If there is no matching policy, server protection is not performed. Each zone supports up to 128 server protection policies.

Table 189 Parameters of Server Protection Policies

Parameter	Description
On/Off	Enable or disable server protection for a specified zone.
No.	Server protection policy priority. 1-1,024. 1 is highest priority. If the number of a new policy already exists, the new policy will be inserted above the existing one. If the number is not specified, it will be added to the end of the policy list.
Name	Server protection policy name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces.
Server IP	The IP addresses of protected servers, up to 4,096 IP addresses or address ranges.
Server Type	The types of protected servers, including Web, Mail, FTP, Telnet, DNS and Other.
IPS	Enable or disable (Off by default) IPS inspection. IPS inspection levels are Low, Medium, High, and Custom. Configure IPS inspection levels for Web, Mail, FTP, Telnet, DNS, and other servers. For details, see 10.5.7. IPS.
Anti-Virus	Enable or disable (Off by default) anti-virus scanning. Anti-virus scanning levels are Low, Medium, High, and Custom. Configure anti-virus scanning levels for FTP Upload and SMTP. For details, see 10.5.5. Anti-Virus.
Anti-Spam	Enable or disable (Off by default) anti-spam inspection. Anti-spam inspection levels are Low, Medium, High, and Custom. Configure the anti-spam inspection level for SMTP only. For details, see 10.5.6. Anti-Spam.
Protection	Enable web protection in web server protection policies or mail protection in mail server protection policies. For details, see 10.5.4.4. Web Protection and 10.5.4.5. Mail Protection.
Log	Logging is enabled for a server protection policy by default.
Enable	Server protection policy is enabled by default.

FGX UTM provides different protection for different servers:

Table 190 Parameters of Server Protection Policy Advanced Configurations

Type	IPS	AV	AS	Protection	Policy-specific settings
Web	Yes	--	--	**10.5.4.4. Web Protection**—globally configured and enabled per policy.	**Protocol Anomaly Detection**—Identify HTTP upload traffic that deviates from RFC specifications.
Mail	Yes	Yes	Yes	**10.5.4.5. Mail Protection**—globally configured and enabled per policy.	• **Maximum Message Size to Protect**—1-10 MB. Default is 10. Anti-virus scanning and anti-spam inspection are not performed on mail message parts which exceed the maximum size. Message size restriction takes effect only when the anti-virus or anti-spam function is enabled and the e-mail does not match any allow or block lists. • **Protocol Anomaly Detection**—Identify SMTP, POP3, and IMAP traffic that deviates from RFC specifications.
FTP Upload	Yes	Yes	--	--	--
Telnet	Yes	--	--	--	• **Command Filtering**—inspects Telnet traffic from ANSI, Xterm, VT100, and VT152 terminals. When the command filtering function is enabled, character strings will be recombined and then will be checked against the user-defined command block list. • **User-Defined Command Block List**—supports up to 512 user-defined commands. A user-defined command is composed of letters, digits, and underscores. 1-64 characters.
DNS	Yes	--	--		• **Drop Inbound Requests**—If enabled, inbound DNS requests that are not from authorized/listed zones will be dropped. If you want to allow DNS requests for some specific IP addresses or domain names from the restricted zones, you can enable **Authorized Domain** and add the allowed IP addresses and domain names. • **Protocol Anomaly Detection**—Identify DNS traffic that deviates from RFC specifications.
Other	Yes	--	--	--	--

10.5.4.2. (Server Protection) Trusted Client List

A trusted client list defines trusted clients within a specified zone. It is matched before server protection policies. All traffic sent from the trusted clients to the protected servers will not be inspected for server protection check: IPS, AV, and AS. Each zone has one trusted client list (empty and disabled by default) and each list can have up to 32 entries.

Table 191 Parameters of Trusted Client List

Parameter	Description
On/Off	Enable or disable trusted client list for a specified zone.
Name	Trusted client policy name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces.
Zone	The trusted client zone.
IP Address (Client IP Address)	The IP address of a trusted client. Can be: • **Any** (default) • **Any IPv4 Address** • **Any IPv6 Address** • **Use the Following List—**user-specified IP addresses.
Source User	Can be: • **Any** (default) • **Any Authenticated User** • **Use the Following List—**Can include externally authenticated users not created on FGX. Each trusted client list can have up to 4,096 source users.

10.5.4.3. (Server Protection) Trusted Mail Address List

A trusted mail address list in server protection defines the trusted e-mail addresses within a specified zone. It is matched after server protection policies but before anti-spam inspection. If the recipient or sender of an e-mail sent to a protected server is on the trusted mail address list, the e-mail will not be inspected for server protection: IPS (attack signature detection and MIME part stripping), AV, and AS. The trusted mail address list in server protection is defined for SMTP traffic. Each zone has one trusted mail address list (empty and disabled by default), up to 128 trusted mail addresses or domain names.

Table 192 Parameters of Trusted Mail Address List (Server Protection)

Parameter	Description
On/Off	Enable or disable trusted mail address list for a specified zone.
Mail Address	The e-mail address or domain name of a trusted client. Anonymous senders are allowed and indicated by "(null)."

10.5.4.4. Web Protection

Web protection is configured globally for the system, and you can enable or disable it in web server protection policies per zone. This section includes:

- 10.5.4.4.1. Information Disclosure Prevention
- 10.5.4.4.2. Injection Defense

10.5.4.4.1. Information Disclosure Prevention

FGX filters traffic of both the server and client sides to provide information disclosure protection for web servers:

- **Header substitution**—replaces sensitive information such as the server name or version number in HTTP headers to protect web servers.
- **Error concealment**—conceals error information about web servers.

  The error information returned by a web server can contain sensitive information about the web server.
- **Directory listing detection**—blocks directory listing traffic to prevent information disclosure or unauthorized access. There are low, medium, and high levels of directory listing detection.

Table 193 Three Levels of Directory Listing Detection

Level	Content to Detect	Drop the response if
Low	only suspicious responses (that contains a URL ending with a slash or a backslash.)	• The name of the requested directory is found in the title of the HTML page. • There is a link to the parent directory on the HTML page.
Medium	all HTTP responses	(same as Low level)
High	all HTTP responses	the words “parent directory” appear in the HTML page within a link that points to the parent directory.

Table 194 Parameters of (Web Server) Information Disclosure Prevention

Parameter	Description
Enable Logging	Enable logging on information disclosure prevention. You also must enable logging and web protection in the corresponding server protection policies.
Header Substitution	A maximum of 32 header substitution rules are allowed. • **Header—**the header to be checked. 1-32 characters. Cannot contain control characters and the following characters: ( ) < > @ , ; : \ “ / [ ] ? = { } SP and HT. • **Value—**the header value that will be replaced. It supports regular expressions. 1-32 characters. • **Action—**select Delete or Substitute. The data you enter to replace the header value is 1-32 characters and cannot be CRLF, SP, or HT. • **Enable—**check to enable a header substitution entry.
Error Concealment	Conceals error information.
Directory Listing Detection	Disabled by default. • **Security Level—**select High, Medium, or Low (default). • **Action—**select Allow or Block to set the action when directory listing attributes are detected.

10.5.4.4.2. Injection Defense

FGX prevents the following injection attacks:

- **Cross-site scripting—**attacks where malicious attackers to inject code into URLs to obtain user identity information or certificate cookies or to trick users into providing a certificate. Typical cross-site scripting attacks inject malicious scripts into HTTP requests which will be unknowingly sent by users to trusted servers.
- **LDAP injection—**attacks that construct LDAP statements based on the information provided by users. An LDAP attack is launched by changing LDAP statements so Web applications can run with invalid permissions, allowing attackers to modify, add, or delete user-input information. FGX examines whether the links submitted to Web applications contain any illegal LDAP queries in the Form field and the URL. LDAP injection includes:
  - **Filter injection** (system defined)**—**if the checked part contains ampersands (&), vertical bars, exclamation points, or parentheses, it is considered an illegal LDAP query.
  - **DN injection—**if the checked part contains any RDN (Relative Distinguished Name) fields, such as ?xxx=, &xxx=, |xxx=, !xxx=, (xxx=,)xxx=, and xxx=), it is considered an LDAP injection attack.
- **SQL injection—**attacks where attackers add SQL codes to URLs or Form fields to gain sensitive information or make changes or cause damage to databases.
- **Command injection—**a kind of attacks in which attackers inject system level commands into URLs or Form fields on the web server. If commands are successfully executed, attackers can log on to the web server as authorized users.

FGX provides three levels of attack defense for each injection attack type.

Table 195 Three Levels of Cross-Site Scripting Defense

Attack Type	Level	Field to check	Blocks HTTP requests comprising
Cross-Site Scripting	Low	URL (path + query). form	script commands
	Medium	URL (path + query), form	HTML tags (< and >)
	High	URL (path + query), form	HTML tags (< and >), or other unicode formats of HTML tags (such as &lt, &gt, &#60, and &#62)
LDAP Injection	Low	URL (path), form	filter injection keywords
	Medium	URL (path), form	filter injection and DN injection keywords
	High	URL (path + query), form	filter injection and DN injection keywords
SQL Injection	Low	URL (path), form	Distinct SQL commands
	Medium	URL (path), form	Non-Distinct SQL commands
		URL (path + query), form	Distinct SQL commands
	High	URL (path + query), form	Distinct or Non-Distinct SQL commands
Command Injection	Low	URL (path), form	Distinct Shell commands
	Medium	URL (path), form	Non-Distinct Shell commands
		URL (path + query), form	Distinct Shell commands
	High	URL (path + query), form	Distinct Shell or Non-Distinct Shell commands

Table 196 Parameters of (Web Server) Injection Defense

Parameter	Description
Enable Logging	Enable logging on injection defense. You also must enable logging and web protection in the corresponding server protection policies.
Cross-Site Scripting Defense	The Script Command List supports up to 64 entries. • **Security Level—**select High, Medium, or Low (default). • **Script Command—**the command to be checked, including user-defined commands. It can be composed of digits, letters, and special characters except spaces and question marks. 1-32 characters. • **Block—**check to block specified command.
LDAP Injection Defense	The Distinguished Name List supports up to 32 entries. • **Security Level—**select High, Medium (default), or Low. • **Distinguished Name—**the key word for LDAP injection detection. It can be composed of digits, letters, and special characters except spaces and question marks. 1-32 characters. • **Block—**check to block specified command.
SQL Injection Defense	The SQL Command List supports up to 256 entries. • **Security Level—**select High, Medium (default), or Low. • **Type—**select Distinct SQL Command or Non-Distinct SQL Command. • **SQL Command—**the command to be checked in SQL injection detection. It can be composed of digits, letters, and special characters except spaces and question marks. 1-120 characters. • **Block—**check to block specified command.
Command Injection Defense	The Shell Command List supports up to 512 entries. • **Security Level—**select High, Medium (default), or Low. • **Type—**select Distinct Shell Command or Non-Distinct Shell Command. • **Shell Command—**the command to be checked in Shell command injection detection. It can be composed of digits, letters, and special characters except spaces and question marks. is 1-120 characters. • **Block—**check to block specified command.

10.5.4.5. Mail Protection

Some server replies may involve information about server configurations used to launch attacks. FGX replaces those parts in the replies from SMTP, POP3, and IMAP servers with user-specified information. FGX provides mail protection to protect mail servers from information disclosure.

Mail protection is configured globally for the system, and you can enable or disable it in server protection policies per zone.

Table 197 Parameters of (Mail Server) Information Disclosure Prevention

Parameter	Description
Enable Logging	Check to enable logging. You also must enable logging and mail protection in the corresponding server protection policies.
Substitute SMTP Server Banner with	UTF-8 0-256 characters.
Substitute POP3 Server Banner with	UTF-8 0-256 characters.
Substitute IMAP Server Banner with	UTF-8 0-256 characters.

10.5.5. Anti-Virus

Traffic matching client or server protection policies requiring anti-virus scanning undergoes anti-virus scanning based on file type. If viruses are detected, FGX will process (pass or block) the traffic according to the user-specified action and generate anti-virus alerts. FGX supports real-time updates of anti-virus rules.

By default, FGX scans the following content:

- Traffic of application layer protocols, HTTP, SMTP, POP3, IMAP, and FTP
- Files of specific types
- Archives

The actions to process traffic include:

- **Pass—**forwards a file directly
- **Block—**blocks different content for different protocols:
  - **FTP—**blocks data connections
  - **HTTP—**blocks HTTP sessions
  - **SMTP, POP3, and IMAP—**strips anomalous attachments and sends notification messages to the client
- **Scan—**performs anti-virus scanning

Note: To view the monitoring information on anti-virus scanning, choose **Monitor > Alerts/ Logs > Anti-Virus Alerts**.

This section includes:

- 10.5.5.1. (AV) General Settings
- 10.5.5.2. Trusted URLs
- 10.5.5.3. Trusted Web Servers
- 10.5.5.4. Trusted Clients
- 10.5.5.5. (Anti-Virus) Profiles
- 10.5.5.6. (Anti-Virus Rule) Update

10.5.5.1. (AV) General Settings

The general settings take effect only when you enable Anti-Virus in client or server protection policies. This section includes:

- 10.5.5.1.1. Heuristic Scanning
- 10.5.5.1.2. Archive Scanning
- 10.5.5.1.3. Scan Settings

10.5.5.1.1. Heuristic Scanning

FGX heuristic scanning detects potentially dangerous behavior. FGX supports two kinds of heuristic scanning: phishing scanning and algorithm-based virus detection.

Table 198 Parameters of Heuristic Scanning

Parameter	Description
Enable Heuristic Scanning	Enable or disable (default) heuristic scanning.
When a virus is detected by the AV engine	The actions include **Block file** (default) and **Pass file**.

10.5.5.1.2. Archive Scanning

Table 199 Parameters of Archive Scanning

Parameter	Description
Maximum nesting levels	Maximum number of nesting levels within an archive. 1-20. Default is 20.
Maximum files within an archive	Maximum number of files within an archive. 1-15,000. Default is 10,000.
When either limit is exceeded	Actions include **Block file** (default) and **Pass file without scanning**.

10.5.5.1.3. Scan Settings

By default, FGX performs anti-virus scanning on traffic of application layer protocols, HTTP, FTP, SMTP, POP3, and IMAP. If trickling for HTTP, FTP, SMTP, POP3, and IMAP traffic is enabled, FGX sends a specified amount of cached data not yet scanned to the client at a specified interval, so that client session timeout can be avoided while the anti-virus engine is scanning large files.

Table 200 Parameters of AV Scan Settings

Parameter	Description
Trickling	Enabled for HTTP, FTP, SMTP, POP3, and IMAP by default. • **Interval—**the interval sending data to a client. 1-900 seconds. Default is 10. • **Amount—**the amount of data sent to a client at each interval during trickling. 1-10,240 bytes. Default is 1.
When a virus is detected by the AV engine	The actions include **Block file** (default) and **Pass file**.
When the AV engine is overloaded or the scan fails	The actions include **Block all files** and **Pass all files without scanning** (default).
When the AV engine fails to initialize	The actions include **Block all files** and **Pass all files without scanning** (default).

10.5.5.2. Trusted URLs

If the URL of an HTTP session is found in the trusted URL list, no further anti-virus scanning will be performed on the HTTP session. The trusted URL list has a maximum of 512 URLs.

Table 201 Parameters of The Trusted URL List

Parameter	Description
URL	URL address (IPv4/v6 address or domain name) from which HTTP sessions will not undergo further anti-virus scanning.
Enable/Disable	Enable or disable a trusted URL entry.
Import/Export	Import/export trusted URL list from/to a text file. Each line in the file contains a URL and status (for example "www.test.com enable"). URL's already in the list will not be imported.

10.5.5.3. Trusted Web Servers

If the destination IP address of an HTTP session is found in the trusted web server list, no further anti-virus scanning will be performed on the HTTP session. The trusted Web server list has a maximum of 512 IP addresses.

Table 202 Parameters of The Trusted Web Server List

Parameter	Description
IP Address	IP addresses (IPv4/Mask or IPv6/Prefix) of servers from which HTTP traffic will not undergo further anti-virus scanning.
Enable/Disable	Enable or disable a trusted Web server entry.
Import/Export	Import/export trusted web server list from/to a text file. Each line in the file contains an IP address and status (for example "192.168.1.64/27 enable"). IP's already in the list will not be imported.

10.5.5.4. Trusted Clients

If the source IP address of an HTTP session is found in the trusted client list, no further anti-virus scanning will be performed on the HTTP session. The trusted client list has a maximum of 512 IP addresses.

Table 203 Parameters of The Trusted Client List

Parameter	Description
IP Address	IP addresses (IPv4/Mask or IPv6/Prefix) of clients from which HTTP traffic will not undergo further anti-virus scanning.
Enable/Disable	Enable or disable a trusted client entry.
Import/Export	Import/export trusted client list from/to a text file. Each line in the file contains an IP address and status (for example "192.168.1.64/27 enable"). IP's already in the list will not be imported.

10.5.5.5. (Anti-Virus) Profiles

FGX provides three pre-defined anti-virus profiles: Low, Medium, and High, which cannot be modified or deleted. Anti-virus profiles can be configured in the root system only, and a maximum of 32 profiles are supported.

Table 204 Parameters of Anti-Virus Profiles

Parameter	Description
Name	Anti-virus profile name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces. Default profile names indicate their levels.
In Use	Click to view the policies using the anti-virus profile. An anti-virus profile can be used by multiple client or server protection policies. Profiles in use cannot be deleted.
Description	Anti-virus profile description. 0-255 UTF-8 characters. Cannot contain ? ” ' \ < > or &.
Maximum File Size to Scan	The maximum size of a file that can be scanned. Default is 1 MB. 1-10 MB.
When the file is oversized	The action to process a file when it is larger than the specified maximum size (for an archive file, the size refers to the size after extraction).
File Type	File types that can be identified by FGX. The description cannot be modified.
Action	The action (Scan, Pass, or Block) to process a file according to the file type.
Enable examination of file type signatures	File type scanning based on file type signatures has a higher priority than file type scanning based on file extension names. If enabled, identify the file type according to the file signature scanning result.
When file type is unrecognized	The action (Scan, Pass, or Block) taken on unrecognized files.

Table 205 Default Anti-Virus Profiles

Parameter	Low	Medium	High
Description	Only binary executable files scanned.	File types known easily infected scanned.	All files scanned.
Maximum File Size to Scan	1 MB	1 MB	10 MB
When file is oversized	Pass file without scanning	Pass file without scanning	Pass file without scanning
Enable examination of file type signatures	Disabled	Enabled	Enabled
When file type is unrecognized	Pass	Scan	Scan

10.5.5.6. (Anti-Virus Rule) Update

FGX uploads rule update packages manually or automatically to overwrite the current anti-virus rules. An uploaded update takes effect without rebooting FGX. Rollback is not supported.

Limitations to anti-virus rule update:

- License—Anti-virus rule update requires AVUP license.
- Vsys—Anti-virus rule updates can be done only in the root system. All virtual systems share the same rules.

Table 206 Parameters of Anti-Virus Rule Base

Parameter	Description
Rule Base	The name of the anti-virus rule base is Anti-Virus. Cannot be changed.
Rule Version	The most recent version of rules in the anti-virus rule base.
Engine Version	The engine version of the anti-virus rule base.
Last Update	Time of last update
Show/Export Update History	Click to view or export the update history of the anti-virus rule base. FGX supports up to 50 records.

Table 207 Parameters of Anti-Virus Rule Update Mode

Parameter	Description
Update Server Address	The URL address of the update server. It can be an IPv4 address, IPv6 address, or a domain name. Default is update.nsdcloud.net/virusrule.
Update Mode (Automatic)	The method of performing an automatic update.
Schedule	The schedule for FGX to perform automatic update. The automatic update starts at the specified time and will be done within two hours. By default, an automatic update is done every day at 22:00.
Update Immediately	Click it for FGX to get an update package from the specified update server and install it.
Upload Package	Upload a local update package.

10.5.6. Anti-Spam

FGX UTM provides anti-spam function. FGX only performs anti-spam inspection on traffic that has matched a client or server protection policy requiring for anti-spam inspection. Anti-spam settings take effect only when you enable anti-spam in client or server protection policies.

Note: To view the monitoring information on anti-spam inspection, choose **Monitor > Alerts/ Logs > Anti-Spam Alerts**.

This section includes:

- 10.5.6.1. (Anti-Spam) General Settings
- 10.5.6.2. Allow List
- 10.5.6.3. Block List
- 10.5.6.4. Spam Word List
- 10.5.6.5. (Anti-Spam) Profiles
- 10.5.6.6. (Anti-Spam Rule) Update

10.5.6.1. (Anti-Spam) General Settings

The general settings take effect only when you enable Anti-Spam in client or server protection policies. This section includes:

- 10.5.6.1.1. Rule Settings
- 10.5.6.1.2. Scan Settings

10.5.6.1.1. Rule Settings

If an incoming e-mail message matches an anti-spam rule, a spam score (system-defined for the rule) is added to the total score of the message. When the total score of the e-mail message reaches the user-specified score threshold (specified in anti-spam profiles), FGX performs the user-specified action. For more information, see 10.5.6.5. (Anti-Spam) Profiles.

Anti-spam rules are predefined for SMTP and POP3 traffic. These rule sets can be enabled but cannot be edited. They have little effect on system performance.

Table 208 Parameters of Rule Settings

Parameter	Description
Enable DNS Rules	Disabled by default. If you enable DNS rules, FGX will perform DNS checking during anti-spam inspection.
Rule Settings	Enable or disable anti-spam rules. All are enabled by default.

Table 209 Anti-Spam Rule Sets

Rule Set Name	Description
advance_fee	This rule set defines tests against financial fraud spam, such as Nigerian 419 scams.
body_tests	This rule set defines most tests against message bodies, spam clearinghouses, message languages, and message locales.
compensate	Tests in this rule set are intended to compensate for common false positives in header tests and are "nice" tests (with negative spam scores).
dnsbl_tests	This rule set defines tests against many different DNS blacklists.
drugs	This rule set comprises body tests that look for common indicators of online pharmacy spam.
dynrdns	This rule set defines rules used to test IP addresses and domain names of DNS relay agents which an e-mail passes by.
fake_helo_tests	This rule set defines a set of rules used to test for forged host names in HELOs.
freemail	This rule set defines rules for tests against free-mail domain names. If the “from-address” of an e-mail message is a free mail domain name and the “Reply-to” address is another free mail domain name (or a free mail domain name is contained in the message body), then this message is probably a spam message.
freemail_domains	This rule set defines free-mail domain names to inspect. The defined domain names will be inspected only when both “freemail” and “freemail_domains” are enabled.
head_tests	This rule set comprises most of the tests against message headers. This includes tests for blacklisted and whitelisted addresses in the From and To headers.
html_tests	This rule set comprises body tests that target messages that comprise HTML markup. Certain types of markup are very commonly seen in spam interesting reading.
imageinfo	This rule set defines rules for image tests.
meta_tests	This rule set comprises meta tests. Meta tests are tests that combine other tests.
net_tests	This rule set comprises network tests against domain names in Host headers of message headers.
phrases	This rule set comprises body tests that look for common phrases that appear in spam, such as “dear friend” and “million dollars”. Most of them are either instructions for how you can be removed from the mailing list or claims that the message conforms to a bill that putatively regulates unsolicited email.
ratware	This rule set comprises tests that look for tell-tale signs of specialized mail programs known to be used by spammers (ratware or spamware). Most of them are tests of message headers.
uri_tests	This rule set comprises most of the tests against URIs that appear in messages.
vbounce	This rule set is a rule set used to catch "backscatter". Backscatter is a mail you didn't ask to receive, generated by legitimate, non-spam-sending systems in response to spam.
bayes	This rule set comprises tests that act on the results of the Bayesian classifier. Bayes is a self-learning algorithm based on statistics. FGX can study the scanned spam and determine the probability that the subsequent messages are spam. This is the general class used to train a learning classifier with new samples of spam and ham mail, and classify based on prior training.

Table 209 Anti-Spam Rule Sets (*continued*)

Rule Set Name	Description
dkim	This rule set defines rules for DKIM inspection. DKIM (Domain Keys Identified Mail) is a method for associating a domain name to an e-mail message, thereby allowing a person, role, or organization to claim some responsibility for the message. Technically DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication.
adsp_override_dkim	This rule set defines default policies for DKIM inspection. DKIM inspection takes effect only when both “dkim” and “adsp_override_dkim” are enabled.
hashcash	Hashcash is a payment system for e-mail where CPU cycles are used as the basis for an e-cash system. This plugin makes it possible to use valid hashcash tokens added by mail programs as a bonus for messages.
replace	This rule set defines rules for tests against spam words which have been replaced by spammers. For example, if “credit” is set as a spam word, spammers may replace it with “Credit”, “C R E D I T”, or “<C><R><E><D><I><T>” to bypass anti-spam inspection. Rules in this rule set are used to detect such words.
spf	This rule set defines rules for SPF verification tests. SPF (Sender Policy Framework) is a technology which prevents sender address forgery.
whitelist_spf	This rule set defines default whitelists for SPF verification. The defined whitelists will take effect only when both “spf” and “whitelist_spf” are enabled.
textcat	This rule set defines rules for language tests. If the language is not one set by FGX, a corresponding score will be added to the message.
uribl	This works by analyzing message text and HTML for URLs, extracting the domain names from those, querying their NS records in DNS, resolving the host names used therein, and querying various DNS blacklists for those IP addresses. This is quite effective.
awl	This plugin module provides support for the auto-whitelist. It keeps track of the average score for senders. Senders are tracked using a combination of their From: address and their IP address. It then uses that average score to reduce the variability in scoring from message to message and modifies the final score by pushing the result towards the historical average. This improves the accuracy of filtering for most email.
whitelist	The rules in this rule set set up default whitelists for several large well-known addresses and companies, such as Amazon.com.
whitelist_dkim	This rule set provides default whitelists for DKIM inspection.
active	Rules marked active, and their dependencies (if they are meta rules).
update	Updated anti-spam rules.

10.5.6.1.2. Scan Settings

Table 210 Parameters of Scan Settings

Parameter	Description
When the anti-spam engine times out	The actions include **Block all e-mail** and **Allow all e-mail without scanning** (default).
When the anti-spam engine is overloaded or the scan fails	The actions include **Block all e-mail** and **Allow all e-mail without scanning** (default).

10.5.6.2. Allow List

Allow lists are matched before block lists. If an IP address or e-mail address is on the IP, sender, or recipient allow list, the e-mail will not undergo further anti-spam processing. Each Vsys has one IP allow list, one sender allow list, and one recipient allow list. This section includes:

- 10.5.6.2.1. IP Allow List
- 10.5.6.2.2. Sender Allow List
- 10.5.6.2.3. Recipient Allow List

10.5.6.2.1. IP Allow List

The IP allow list is defined for SMTP traffic.

Table 211 Parameters of IP Allow List

Parameter	Description
IP Address	The source IP address of an SMTP connection, up to 512 IPv4 or IPv6 addresses.
Type	IPv4 and IPv6.
Enable/Disable	Enable or disable an IP allow list entry.
Import/Export	Import IP addresses from an external text file (.txt) to the existing IP allow list (can not import files with the same file name) or export all IP allow list address to an external file. Each line in the file lists an IP address and "enable" or "disable". For example, "10.1.1.1 enable".

10.5.6.2.2. Sender Allow List

The sender allow list is defined for SMTP and POP3 traffic.

Table 212 Parameters of Sender Allow List

Parameter	Description
E-mail	The sender address, up to 512 e-mail addresses or domain names. Anonymous senders are allowed and indicated by "(null)."
Enable/Disable	Enable or disable a sender allow list entry.
Import/Export	Import e-mail addresses or domain names from an external text file (.txt) to the existing sender allow list (can not import files with the same file name) or export all sender allow list entries to an external file. Each line in the file lists an e-mail address or domain name and "enable" or "disable". For example, "user1@test.com enable".

10.5.6.2.3. Recipient Allow List

The recipient allow list is defined for SMTP and POP3 traffic.

Table 213 Parameters of Recipient Allow List

Parameter	Description
E-mail	The recipient address, up to 512 e-mail addresses or domain names.
Enable/Disable	Enable or disable a recipient allow list entry.
Import/Export	Import e-mail addresses or domain names from an external text file (.txt) to the existing recipient allow list (can not import files with the same file name) or export all recipient allow list entries to an external file. Each line in the file lists an e-mail address or domain name and "enable" or "disable". For example, "user1@test.com enable".

10.5.6.3. Block List

Block lists are matched after allow lists. If an IP address or e-mail address is on the IP, sender, or recipient block list, the e-mail will be blocked directly. Each Vsys has one IP block list, one sender block list, and one recipient block list. This section includes:

- 10.5.6.3.1. IP Block List
- 10.5.6.3.2. Sender Block List
- 10.5.6.3.3. Recipient Block List

10.5.6.3.1. IP Block List

The IP block list is defined for SMTP traffic.

Table 214 Parameters of IP Block List

Parameter	Description
IP Address	The source IP address of an SMTP connection, up to 512 IPv4 or IPv6 addresses.
Type	IPv4 and IPv6.
Enable/Disable	Enable or disable an IP block list entry.
Import/Export	Import IP addresses from an external text file (.txt) to the existing IP block list (can not import files with the same file name) or export all IP block list addresses to an external file. Each line in the file lists an IP address and "enable" or "disable". For example, "10.1.1.1 enable".

10.5.6.3.2. Sender Block List

The sender block list is defined for SMTP and POP3 traffic.

Table 215 Parameters of Sender Block List

Parameter	Description
E-mail	The sender address, up to 512 e-mail addresses or domain names. Anonymous senders are allowed and indicated by "(null)."
Enable/Disable	Enable or disable a sender block list entry.
Import/Export	Import e-mail addresses or domain names from an external text file (.txt) to the existing sender block list (can not import files with the same file name) or export all sender block list entries to an external file. Each line in the file lists an e-mail address or domain name and "enable" or "disable". For example, "user1@test.com enable".

10.5.6.3.3. Recipient Block List

The recipient block list is defined for SMTP and POP3 traffic.

Table 216 Parameters of Recipient Block List

Parameter	Description
E-mail	The recipient address, up to 512 e-mail addresses or domain names.
Enable/Disable	Enable or disable a recipient block list entry.
Import/Export	Import e-mail addresses or domain names from an external text file (.txt) to the existing recipient block list (can not import files with the same file name) or export all recipient block list entries to an external file. Each line in the file lists an -email address or domain name and "enable" or "disable". For example, "user1@test.com enable".

10.5.6.4. Spam Word List

A spam word list is configured for SMTP and POP3 traffic. If spam words in the e-mail body and subject reaches the user-specified threshold, the e-mail will be performed as spam. Otherwise, the e-mail will be forwarded or will undergo other inspections such as anti-virus scanning.

Table 217 Parameters of The Spam Word List

Parameter	Description
Score Threshold	The maximum score of all spam words allowed. 100-1,000. Default is 100. If the total score of spam words in an e-mail message exceeds the specified score threshold, the e-mail will be treated as spam.
When the total score of spam words in an e-mail exceeds the score threshold	The actions include **Block e-mail**, **Allow e-mail**, and **Tag e-mail** (default). If the action is Block e-mail: • For SMTP traffic, FGX only disconnects the SMTP connection. • For POP3 traffic, FGX blocks the e-mail body message, replaces the e-mail subject to a notification message, and sends commands to the mail server for deleting the spam e-mail.
Spam Word List	Add spam words to be scanned. The settings include: • **Word—**spam words to be filtered. 2-32 characters. A spam word can be composed of any UTF-8 characters and it is non-case sensitive. The list supports up to 256 spam words. • **Location—**Subject and Body. • **Score—**1-100. If a spam word instance is found, the corresponding score will be added. • **Enable—**enable or disable a spam word entry.
Import/Export	Import spam words from an external text file (.txt) to the existing spam word list (can not import files with the same file name) or export all spam words to an external file. Each line in the file lists a spam word and its location, score, and status (enable or disable). For example, "test Subject, Body 100 enable".

10.5.6.5. (Anti-Spam) Profiles

Anti-spam profiles define the spam score threshold and the action.

Table 218 Parameters of Anti-Spam Profiles

Parameter	Description
Name	Anti-spam profile name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces. Default profile names also indicate protection levels.
In Use	Click to view the policies using an anti-spam profile. An anti-spam profile can be used by multiple client or server protection policies. Profiles in use cannot be deleted.
Description	Anti-spam profile description. 0-255 UTF-8 characters. Cannot contain ? ” ' \ < > or &.
Score	The score threshold used to determine whether an e-mail is spam. Each anti-spam rule has a score. Once a rule is matched, the corresponding score will be added. When the total score exceeds the user-defined score threshold, the e-mail will be processed as spam according to the user-defined action.
Action	The action to process an e-mail when spam is detected. The actions include: • **Tag** (default)**—**adds the user-specified tag to the subject of the e-mail and forward the tagged e-mail. • **Allow—**forwards the e-mail directly. • **Block—**blocks the connection the e-mail belongs to. For SMTP traffic, FGX only disconnects the SMTP connection. For POP3 traffic, FGX blocks the e-mail body message, replaces the e-mail subject to “The Mail is blocked due to Anti-Spam rules”, and sends commands to the mail server for deleting the spam e-mail.
Subject Tag	The content used to tag an e-mail when the total score of it exceeds the score threshold. It can be composed of any UTF-8 characters. It has a maximum length of 16 characters. The default subject tag is [SPAM].

FGX provides three default profiles: Low, Medium, and High. They cannot be modified or deleted. Anti-spam profiles can be configured in the root system only, and a maximum of 32 profiles are supported.

Table 219 Default Anti-Spam Profiles

Parameter	Low	Medium	High
Description	E-mail score greater than or equal to 10.	E-mail score greater than or equal to 5.	E-mail score greater than or equal to 3.
Score	10	5	3
Action	Tag	Tag	Tag
Subject Tag	[SPAM]	[SPAM]	[SPAM]

10.5.6.6. (Anti-Spam Rule) Update

FGX uploads rule update packages manually or automatically to overwrite the current anti-spam rules. An update takes effect without rebooting FGX. Rollback is not supported.

Limitations to anti-spam rule update:

- License—Anti-spam rule update requires ASOL license.
- Vsys—Anti-spam rule updates can be done only in the root system. All virtual systems share the same rules.

Table 220 Parameters of Anti-Spam Rule Base

Parameter	Description
Rule Base	The name of the anti-spam rule base. The name of the anti-spam rule base is Anti-Spam, and it cannot be changed.
Rule Version	The most recent version of rules in the anti-spam rule base.
Engine Version	The engine version of the anti-spam rule base.
Last Update	The time the last update was done.
Show/Export Update History	Click to view and export the update history of the anti-spam rule base. FGX supports up to 50 records.

Table 221 Parameters of Anti-Spam Rule Update Mode

Parameter	Description
Update Server Address	The URL address of the update server in an automatic update. It can be an IPv4 address, IPv6 address, or a domain name. It is update.nsdcloud.net/antispamrule by default.
Update Mode (Automatic)	The method of performing an automatic update, including Install updates automatically and Never check for updates.
Schedule	The schedule for FGX to perform automatic updates. The automatic update starts at the specified time and will be done within two hours. By default, an automatic update is done every day at 22:00.
Update Immediately	Click it for FGX to get an update package from the specified update server and install it.
Upload Package	Upload a local update package.

10.5.7. IPS

FGX provides attack signature detection and protocol restriction for client and server traffic.

Note: To view the monitoring information on IPS, choose **Monitor > Alerts/Logs > IPS Alerts**.

This section includes:

- 10.5.7.1. (IPS) Profiles
- 10.5.7.2. Protocol restriction
- 10.5.7.3. (Attack Signature Rule) Update

10.5.7.1. (IPS) Profiles

An IPS profile is a set of attack signature rules. You can configure different IPS profiles and enable or disable protocol restriction for different protocols in IPS profiles. IPS profiles are used in client or server protection policies. Client IPS profiles are used in client protection policies, and server IPS profiles are used in server protection policies.

FGX provides 21 default IPS profiles that cannot be modified or deleted. You can also create custom IPS profiles. IPS profiles can be configured in the root system only, and a maximum of 63 profiles are supported, including the default ones.

FGX provides attack signature detection based on protocol analysis and can identify attacks according to their specific characteristics. FGX attack signature detection involves attack signature rules, all characteristics (signatures) of a kind of attacks. FGX can detect certain kinds of attacks according to attack signature rules and allow or block matching traffic according to user-specified action.

Table 222 Parameters of IPS Profiles

Parameter	Description
Name	An IPS profile name. 1-63 UTF-8 characters. Cannot contain ? , ” ' \ < > & # or spaces. Default IPS profiles are named with “_Low”, “_Medium”, and “_High”, which indicate the protection levels. • **Low—**only protect against attacks of High severity level. • **Medium**—protect against attacks of High and Medium severity levels. • **High**—protect against all levels of attacks.
Type	The type of an IPS profile, Client and Server. • If you choose Client, you can only configure attack signature rules whose target is Client or Both. • If you choose Server, you can only configure attack signature rules whose target is Server or Both.
In Use	Click  to view the policies using an IPS profile. An IPS profile can be used by multiple client or server protection policies. Profiles in use cannot be deleted.
Description	IPS profile description. 0-255 UTF-8 characters. Cannot contain ? ” ' \ < > &.

Table 222 Parameters of IPS Profiles (*continued*)

Parameter	Description
Server Type	The server type of a server IPS profile, Web, Mail, FTP, Telnet, DNS, and Other. This option is available only when the type is Server.
Protocol Restriction	Enable or disable protocol restriction for an IPS profile. • In a client IPS profile, you can enable or disable protocol restriction for the following: SMTP, POP3, IMAP, and DNS. • In a server IPS profile, you can enable or disable protocol restriction for the following: Web (HTTP), Mail (SMTP, POP3, IMAP), and DNS.
Attack Signature Rule List	Set attack signature rules for a new IPS profile.
Allow/Block	Set the action of an attack signature rule you choose for an IPS profile. If you set the action as Allow for an enabled rule, FGX will allow the traffic matching the rule.
Enable/Disable	Enable or disable an attack signature rule you choose for an IPS profile.

Table 223 Attack Signature Rules

Parameter	Description
ID	The ID of an attack signature rule. It cannot be edited.
Name	The name of an attack signature rule. It cannot be edited.
Service	The protocol corresponding to an attack signature rule. It cannot be edited.
Severity Level	Severity level of attacks, including High, Medium, Low, and Info. It cannot be edited. Severity levels are the basis for FGX to generate logs and for you to perform audit in syslog, e-mail, SNMP trap, or local syslog mode. The relationships between severity levels and security levels are High-Critical, Medium-Error, Low-Warning, and Info-Notification.
Category	The category to which an attack signature rule belongs, such as BACKDOOR/TROJAN, BUFFER OVERFLOW, CODE INJECTION, DESIGN ERROR, INPUT INVALIDATE FAILED, MALWARE, and UNKOWN. It cannot be edited.
Target	The target of an attack, including Client, Server, and Both. It cannot be edited.
OS & APP	The operating system and applications corresponding to an attack signature rule. It cannot be edited.
CVE	The serial number of Common Vulnerabilities & Exposures (CVE). It cannot be edited.
Bugtraq	The bugtraq number. It cannot be edited.
Description	The brief description of an attack signature rule. It cannot be edited.
Enable	Used to enable or disable an attack signature rule.
Action	The action for processing packets matching an attack signature rule, including: • **Allow—**indicates that actions are set as Allow for all signatures of this rule. • **Block—**indicates that actions are set as Block for all signatures of this rule.

10.5.7.2. Protocol restriction

Protocol restriction refers to restriction on application layer protocols. Attacks may be launched by taking advantage of protocol vulnerabilities. FGX provides protocol restriction settings for both server protection (SP) and client protection (CP). Protocol restriction is configured globally for the system, and you can enable or disable it in IPS profiles. Once you modify the global settings of protocol restriction and save the changes, these last saved settings will overwrite the previous settings.

FGX provides the following protocol restriction:

- 10.5.7.2.1. HTTP Protocol Restriction
- 10.5.7.2.2. SMTP Protocol Restriction
- 10.5.7.2.3. POP3 Protocol Restriction
- 10.5.7.2.4. IMAP Protocol Restriction
- 10.5.7.2.5. DNS Protocol Restriction

10.5.7.2.1. HTTP Protocol Restriction

HTTP protocol restriction can only be enabled in IPS profiles of the Web server type.

Table 224 Parameters of HTTP Protocol Restriction

Parameter	Description
Level	Protocol restriction level, Low, Medium (default), High, and Custom.
Enable Logging	Enable logging on HTTP protocol restriction. You also must enable logging in the corresponding server protection policies.
Maximum Headers	• **Value—**1-1,024. • **Action—**the action (Allow and Block) when the number of headers exceeds the value.
Maximum URL Length	• **Value—**1-2,048 bytes. • **Action—**the action (Allow and Block) when URL length exceeds the value.
Maximum Request Body Length	• **Value—**1-65,535 bytes. • **Action—**the action (Allow and Block) when request body length exceeds the value.
Maximum Header Length	• **Value—**1-2,048 bytes. • **Action—**the action (Allow and Block) when header length exceeds the value.
Header Length Restriction	• **Header Name—**up to 32 headers. • **Maximum Length—**1-2,048 bytes. This value should be smaller than the general maximum HTTP header length. • **Enable—**If the length of a header exceeds the specified length, it will be blocked.
Request Method Block List	Block HTTP traffic of selected commands
Block non-ASCII Headers	If there are non-ASCII characters detected in a header, the connection will be blocked.
Block non-ASCII characters in Form fields	If there are non-ASCII characters detected in a Form field, the connection will be blocked.

Table 225 Default Settings of HTTP Protocol Restriction

Parameter	Low	Medium	High	Custom
Enable Logging	Enabled	Enabled	Enabled	Enabled
Maximum Headers	500, Block	300, Block	100, Block	300, Allow
Maximum URL Length	2000 Bytes, Block	1500 Bytes, Block	1000 Bytes, Block	2048 Bytes, Allow
Maximum Request Body Length	Disabled	Disabled	50000 Bytes, Block	Disabled
Maximum Header Length	1500 Bytes, Block	1000 Bytes, Block	600 Bytes, Block	2048 Bytes, Allow
Header Length Restriction	On, empty list	On, empty list	On, empty list	On, empty list
Request Method Block List	On, empty list	On, block the following: PURGE, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, BMOVE, BDELETE, BPROPFIND, BPROPPATCH, BCOPY, SEARCH, SUBSCRIBE, UNSUBSCRIBE, POLL, REPORT, PATCH, VERSION-CONTROL, CHECKOUT, UNCHECKOUT, CHECKIN, UPDATE, LABEL, MKWORKSPACE, MKACTIVITY, BASELINE-CONTROL, MERGE	On, block the following: PUT, CONNECT, TRACE, PURGE, OPTIONS, DELETE, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, BMOVE, BDELETE, BPROPFIND, BPROPPATCH, BCOPY, SEARCH, SUBSCRIBE, UNSUBSCRIBE, POLL, REPORT, PATCH, VERSION-CONTROL, CHECKOUT, UNCHECKOUT, CHECKIN, UPDATE, LABEL, MKWORKSPACE, MKACTIVITY, BASELINE-CONTROL, MERGE	On, block the following: PURGE, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, BMOVE, BDELETE, BPROPFIND, BPROPPATCH, BCOPY, SEARCH, SUBSCRIBE, UNSUBSCRIBE, POLL, REPORT, PATCH, VERSION-CONTROL, CHECKOUT, UNCHECKOUT, CHECKIN, UPDATE, LABEL, MKWORKSPACE, MKACTIVITY, BASELINE-CONTROL, MERGE
Block non-ASCII Headers	Disabled	Disabled	Enabled	Disabled
Block non-ASCII characters in Form fields	Disabled	Disabled	Enabled	Disabled

10.5.7.2.2. SMTP Protocol Restriction

Table 226 Parameters of SMTP Protocol Restriction for Server Protection

Parameter	Description
Level	Protocol restriction level, Low, Medium (default), High, and Custom.
Enable Logging	Enable logging on SMTP protocol restriction. You also must enable logging in the corresponding server protection policies.
Maximum Command Length	• **Value—**1-1,024 bytes. • **Action—**the action (Allow, Block, and Reject) when command length exceeds the value.
Maximum Parameter Length	• **Value—**1-512 bytes. • **Action—**the action (Allow, Block, and Reject) when parameter length exceeds the value.
Maximum NOOP Commands	• **Value—**1-128. • **Action—**the action (Allow and Block) when it appears more than the specified times in a single session.Noop command does not execute any operation, but continuous Noop commands may be attacks.
Maximum Commands	• **Value—**1-256. • **Action—**the action (Allow and Block) when it appears more than the specified times in a single session.
Maximum Unknown Commands	• **Value—**1-128. • **Action—**the action (Allow and Block) when it appears more than the specified times in a single session.
Block Unknown Commands	Block unknown SMTP commands. User-defined commands are not unknown commands.
User-Defined SMTP Command List	Add up to 32 user-defined SMTP commands to allow. A user-defined SMTP command is 4-8 characters and cannot contain spaces or control characters.
Command Block List	Block selected SMTP commands
Add Received header when forwarding	Add the Received header when forwarding an e-mail message.
Strip MIME parts with multiple Content-type headers	Strip MIME parts comprising multiple Content-Type headers.
Strip MIME parts with multiple Encoding headers	Strip MIME parts comprising multiple Encoding headers.
Strip MIME parts with unknown Encoding headers	Strip MIME parts comprising headers in unknown Encoding format.
Strip all e-mail attachments	Strip all e-mail attachments.
Strip all fragmented e-mail messages	Strip all fragmented e-mail messages.
Block messages from recipients without a domain name	Block messages from recipients without a domain name.

Table 227 Parameters of SMTP Protocol Restriction for Client Protection

Parameter	Description
Enable Logging	Enable logging on SMTP protocol restriction. You also must enable logging in the corresponding client protection policies.
Maximum Response Length	• **Value—**1-2,048 bytes. • **Action—**the action (Allow and Block) when response length exceeds the value.

Table 228 Default Settings of SMTP Protocol Restriction

Type	Parameter	Low	Medium/Custom	High
Server Protection	Enable Logging	Enabled	Enabled	Enabled
	Maximum Command Length	512 Bytes, Reject	256 Bytes, Reject	128 Bytes, Block
	Maximum Parameter Length	512 Bytes, Reject	256 Bytes, Reject	128 Bytes, Block
	Maximum NOOP Commands	Disabled	10, Block	5, Block
	Maximum Commands	Disabled	Disabled	20, Block
	Maximum Unknown Commands	20, Block	10, Block	5, Block
	Block Unknown Commands	Disabled	Disabled	Enabled
	User-Defined SMTP Command List	On, empty list	On, empty list	On, empty list
	Command Block List	Off	On, block commands: NOOP	On, block commands: VRFY, EXPN, NOOP
	Add Received header when forwarding	Disabled	Enabled	Enabled
	Strip MIME parts with multiple Content-type headers	Enabled	Enabled	Enabled
	Strip MIME parts with multiple Encoding headers	Enabled	Enabled	Enabled
	Strip MIME parts with unknown Encoding headers	Disabled	Disabled	Enabled
	Strip all e-mail attachments	Disabled	Disabled	Enabled
	Strip all fragmented e-mail messages	Disabled	Disabled	Enabled
	Block messages from recipients without a domain name	Enabled	Enabled	Enabled
Client Protection	Enable Logging	Enabled	Enabled	Enabled
	Maximum Response Length	Disabled	512 Bytes, Block	512 Bytes, Block

10.5.7.2.3. POP3 Protocol Restriction

Table 229 Parameters of POP3 Protocol Restriction for Server Protection

Parameter	Description
Level	Protocol restriction level, Low, Medium (default), High, and Custom.
Enable Logging	Enable logging on POP3 protocol restriction (must also enable in the corresponding server protection policies.
Maximum Command Length	• **Value—**1-1,024 bytes. • **Action—**the action (Allow, Block, and Reject) when command length exceeds the value.
Maximum Parameter Length	• **Value—**1-512 bytes. • **Action—**the action (Allow, Block, and Reject) when parameter length exceeds the value.
Maximum NOOP Commands	• **Value—**1-128. • **Action—**the action (Allow and Block) when it appears more than the specified times.
Maximum Commands	• **Value—**1-256. • **Action—**the action (Allow and Block) when it appears more than the specified times.
Maximum Unknown Commands	• **Value—**1-128. • **Action—**the action (Allow and Block) when it appears more than the specified times.
Block Unknown Commands	Block unknown POP3 commands. User-defined commands are not unknown commands.
User-Defined POP3 Command List	Add up to 32 user-defined POP3 commands to allow. A user-defined POP3 command is 4-8 characters and cannot contain spaces or control characters.
Command Block List	Block selected POP3 commands.

Table 230 Parameters of POP3 Protocol Restriction for Client Protection

Parameter	Description
Enable Logging	Enable logging on POP3 protocol restriction (must also enable in corresponding client protection policies).
Maximum Response Length	• **Value—**1-2,048 bytes. • **Action—**the action (Allow and Block) when response length exceeds the value.

Table 231 Default Settings of POP3 Protocol Restriction

Type	Parameter	Low	Medium/Custom	High
SP	Enable Logging	Enabled	Enabled	Enabled
	Maximum Command Length	512 Bytes, Reject	255 Bytes, Reject	128 Bytes, Block
	Maximum Parameter Length	512 Bytes, Reject	40 Bytes, Reject	16 Bytes, Block
	Maximum NOOP Commands	Disabled	10, Block	5, Block
	Maximum Commands	Disabled	Disabled	20, Block
	Maximum Unknown Commands	20, Block	10, Block	5, Block
	Block Unknown Commands	Disabled	Disabled	Enabled
	User-Defined POP3 Command List	On, empty list	On, empty list	On, empty list
	Command Block List	Off	On, block commands: NOOP	On, block commands: NOOP
CP	Enable Logging	Enabled	Enabled	Enabled
	Maximum Response Length	Disabled	512 Bytes, Block	128 Bytes, Block

10.5.7.2.4. IMAP Protocol Restriction

Table 232 Parameters of IMAP Protocol Restriction for Server Protection

Parameter	Description
Level	Protocol restriction level, Low, Medium (default), High, and Custom.
Enable Logging	Enable IMAP protocol restriction logging (must enable corresponding server protection policies logging).
Maximum Command Length	• **Value—**1-2,048 bytes. • **Action—**the action (Allow, Block, and Reject) when command length exceeds value.
Maximum Parameter Length	• **Value—**1-1,024 bytes. • **Action—**the action (Allow, Block, and Reject) when parameter length exceeds the value.
Maximum Tag Length	• **Value—**1-512 bytes. • **Action—**the action (Allow, Block, and Reject) tag length exceeds the value.
Maximum NOOP Commands	• **Value—**1-128. • **Action—**the action (Allow and Block) when it appears more than the specified times.
Maximum Commands	• **Value—**1-256. • **Action—**the action (Allow and Block) when it appears more than the specified times.
Maximum Unknown Commands	• **Value—**1-128. • **Action—**the action (Allow and Block) when it appears more than the specified times.
Block Unknown Commands	Block unknown IMAP commands. User-defined commands are not unknown commands.
User-Defined IMAP Command List	Add up to 32 user-defined IMAP commands to allow. A user-defined IMAP command is 4-16 characters and cannot contain spaces or control characters.
Command Block List	Block selected IMAP commands.

Table 233 Parameters of IMAP Protocol Restriction for Client Protection

Parameter	Description
Enable Logging	Enable IMAP protocol restriction logging (must also enable logging in corresponding client protection policies).
Maximum Response Length	• **Value—**1-4,096 bytes. • **Action—**the action (Allow and Block) when response length exceeds the value.

Table 234 Default Settings of IMAP Protocol Restriction

Type	Parameter	Low	Medium/Custom	High
SP	Enable Logging	Enabled	Enabled	Enabled
	Maximum Command Length	1024 Bytes, Allow	512 Bytes, Reject	256 Bytes, Block
	Maximum Parameter Length	512 Bytes, Allow	256 Bytes, Reject	128 Bytes, Block
	Maximum Tag Length	Disabled	128 Bytes, Reject	64 Bytes, Block
	Maximum NOOP Commands	Disabled	20, Block	5, Block
	Maximum Commands	Disabled	Disabled	20, Block
	Maximum Unknown Commands	20, Block	10, Block	5, Block
	Block Unknown Commands	Disabled	Enabled	Enabled
	User-Defined IMAP Command List	On, empty list	On, empty list	On, empty list
	Command Block List	Off	Off	Off
CP	Enable Logging	Enabled	Enabled	Enabled
	Maximum Response Length	2048 Bytes, Allow	1024 Bytes, Block	512 Bytes, Block

10.5.7.2.5. DNS Protocol Restriction

Table 235 Parameters of DNS Protocol Restriction for Server Protection

Parameter	Description
Enable Logging	Enable logging on DNS protocol restriction. You also must enable logging in the corresponding server protection policies.
Authorized IP Address List	Set the authorized IP addresses for DNS zone transfer restriction. DNS requests from IP addresses not in the list will be dropped. The list supports up to 128 entries.

Table 236 Parameters of DNS Protocol Restriction for Client Protection

Parameter	Description
Enable Logging	Enable logging on DNS protocol restriction. You also must enable logging in the corresponding client protection policies.
Resource Record Restriction for UDP Only	Restrict resource records. Enable it and configure the following for **Maximum Answer Records**, **Maximum Authority Records**, and **Maximum Additional Records**: • **Value—**1-10. Default is 4. • **Action—**includes Allow (default) and Block.

10.5.7.3. (Attack Signature Rule) Update

FGX uploads rule update packages manually or automatically to overwrite the current attack signature rules. An uploaded update takes effect without rebooting FGX. Rollback is not supported.

Limitations to IPS attack signature rule update:

- License—Attack signature rule update requires IPSUP license.
- Vsys—Attack signature rule updates can be done only in the root system. All virtual systems share the same rules..

Table 237 Parameters of Attack Signature Rule Base

Parameter	Description
Rule Base	The names of the attack signature rule bases, including HTTP, DNS, FTP, IMAP, ORACLE, OTHERS, POP3, SIP, SMTP, TELNET, TFTP, and BACKDOOR. Cannot be modified.
Rule Version	The most recent version of rules in the attack signature rule base.
Engine Version	The engine version of the attack signature rule base.
Last Update	Time of last update
Show/Export Update History	Click to view or export the update history of the attack signature rule base. FGX supports up to 50 records.

Table 238 Parameters of Attack Signature Rule Update Mode

Parameter	Description
Update Server Address	The URL address of the update server in an automatic update. It can be an IPv4 address, IPv6 address, or a domain name. Default is update.nsdcloud.net/autoupdate.
Update Mode (Automatic)	The method of performing an automatic update.
Schedule	The schedule for FGX to perform automatic update. The automatic update starts at the specified time and will be done within two hours. By default, an automatic update is done every day at 22:00.
Update Immediately	Click it for FGX to get an update package from the specified update server and install it.
Upload Package	Upload a local update package.

10.5.8. Notification Messages

Notification messages are sent to clients as response from servers and they are used to replace the content blocked by AV, URL Filtering, protocol restriction, AS, or attack signature detection. Notification messages are classified into two types:

- **User-Defined Notification Messages**—can be configured through the WebUI.
- **System Notification Messages**—cannot be modified.

User-Defined Notification Messages

Table 239 Default Notification Messages

Situation	Format	Default Message
When a URL is blocked due to URL category	1-8192	<<The URL is blocked due to URL Category. URL: #URL# Category: #CATEGORYNAME#>>
When a URL is blocked due to URL blacklist	1-8192	<<The URL is blocked due to URL Blacklist. URL: #URL#>>
When HTTP downloads are infected by viruses	1-8192	<<High security alert!!! You are not permitted to download the file because it is infected with the virus "#VIRUS#". URL: #URL#>>
When an attachment is infected by viruses	1-512	<<Dangerous attachment has been stripped. The file "#FILENAME#" has been stripped because of a virus. It was infected with the "#VIRUS#" virus.>>
When an attachment is stripped due to protocol restriction	1-512	<<The attachment of this e-mail has been stripped.>>
When fields of an e-mail message are stripped due to protocol restriction	1-512	<<One or more MIME parts of this e-mail have been stripped.>>

System Notification Messages

System notification messages are classified into:

- Anti-Virus Attachment Replacement Messages

  In anti-virus scanning, attachments of an e-mail message are substituted by a file named "attachment.txt" containing a notification message when virus is detected and the action is Block. The system notification messages comprised in the replacement files are shown in the following table.

Table 240 System Notification Messages for Blocked Attachments

Function Name	Notification Message in the File (attachment.txt)
File size exceeds the limit	#FILENAME# oversizes the maximum file size (#Maximum_File_Size#).
File type is recognized	File type is recognized. The type of #FILENAME# is #File_Type#. #File_Type# file is blocked.
File type is unrecognized	File type is unrecognized. The type of #FILENAME# is Unknown. Unknown file is blocked.
Number of files within an archive exceeds the limit	The number of files within the archive file exceeds the limit (#Maximum_Files#). #FILENAME# is blocked.
Number of nesting levels exceeds the limit	The nesting levels of the archive file exceeds the limit (#Maximum_Nesting#). #FILENAME# is blocked.
AV engine is overloaded or the scan fails	The AV engine is overloaded or the scan failed. #FILENAME# is blocked.
AV engine times out	The AV engine times out. #FILENAME# is blocked.
AV engine fails to initialize	Failed to initialize the AV engine. #FILENAME# is blocked.

- Anti-Spam Subject Replacement Message

  For client traffic (POP3), when UTM detects spam and the action is Block, FGX will block the e-mail message and replace the subject to the following notification message:

  The Mail is blocked due to Anti-Spam rules.

- Attack Signature Replacement Message

  When threats are detected in files sent from the websites to a client, a system defined notification message is sent to the client, and FGX disconnects the connection and saves the URL of the web server in the cache for 600 seconds. FGX can save up to 1,000 URLs. When there are already 1,000 URLs, a new URL will replace the oldest one.

  The notification message is as follows:

  <HTML><BODY><h2>High security alert!!!</h2> The URL you requested was found at risk(Attack Signatures Name=#Attack_Signatures_Name#,CVE=#CVE#). URL=http://#URL# <BODY></HTML>.

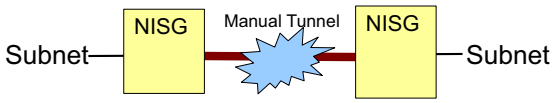
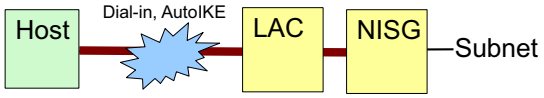
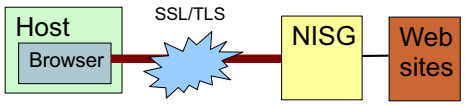
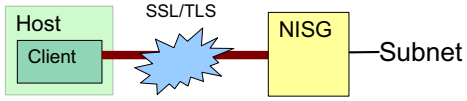
11 Virtual Private Network 2

FGX provides extensive VPN functionality. This chapter describes FGX VPN.

- **11.1. Concepts**. Introduces supported VPN types and features.
- **11.2. Configuration Basics**. Describes the basic steps for configuration and what to consider for each step.
- **11.3. Basic Examples**. Basic examples for the most commonly used functions.
- **11.4. Parameter Reference**. Describes in detail all VPN parameters.

11.1. Concepts

The following table shows an overview of the 5 main VPN types.

VPN scenario (FGX = site device)	Description (+ = advantages, - = disadvantages)
	■ **VPN type:** **Site-to-Site IPSec Manual Tunnel**. ■ **Features**. Manual security parameters (SA) configuration. Manual key creation and exchange. IP encapsulation, ESP/AH. ■ + Easy setup. ■ - Difficult to manage/scale. No peer/user authentication.
	■ **VPN type:** **Site to Site IPSec Auto IKE** ■ **Features**. Auto SA negotiation. Auto IKE key generation/exchange. Peer authentication (certificates/pre-shared key). ESP/AH. ■ + Much easier to use. Scalable. ■ - Configuration much more complex. Requires more computing power.
	■ **VPN type:** **Site to Remote Peer IPSec Auto IKE** ■ **Features:** L2TP/Xauth. Auto SA negotiation. Auto IKE key generation/exchange. Peer authentication (certificates/pre-shared key). ESP/AH. User authentication. ■ + Mobility, user authentication. ■ - Requires configuration on each host.
	■ **VPN type:** **Browser to Site Portal SSL/TLS** ■ **Features:** Auto ciphersuite negotiation. Auto key generation/ exchange. Peer authentication (certificates). User authentication username / password. ■ + Requires minimal configuration. ■ - Limited to HTTP/S, FTP, and SMTP sites.
	■ **VPN type:** **Client to Site SSL/TLS** ■ **Features:** Auto ciphersuite negotiation. Auto key generation/ exchange. Peer authentication (certificates/preshared key). User authentication username / password. ■ + Can access subnet. ■ - Requires SSL VPN client installation.

This section also describes VPN configuraiton in NAT and HA envrionments.

- **11.1.6. Site to Site IPSec VPN (tunnel mode) + NAT**. How to configure for NAT traversal.
- **11.1.7. VPN with Virtual Routers (HA)**. How to configure VPN in High Availability (HA) envrionment.

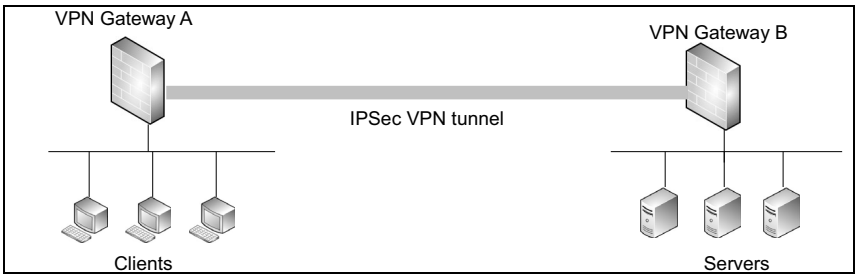
11.1.1. Site-to-Site IPSec Manual Tunnel

- 11.1.1.1. Requirements
- 11.1.1.2. Implementation (packet modifications)
- 11.1.1.3 IPSec SA Security Protocols and Working Modes

11.1.1.1. Requirements

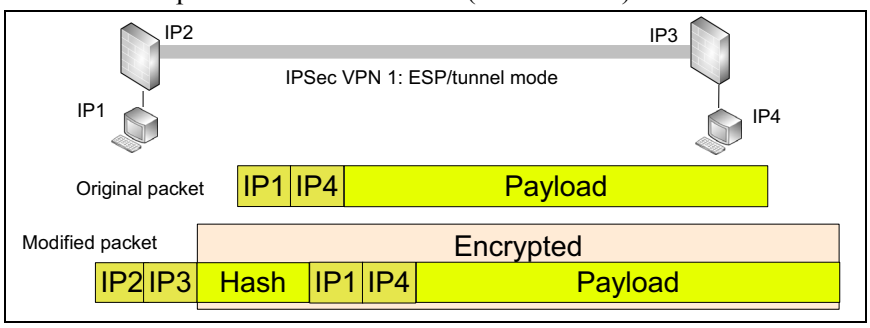
Use an IPSec manual tunnel when you require:

- Tunnel between VPN gateways, providing secure link between hosts (clients/servers).
- No configuration or installation on the hosts/servers.
- Simple configuration and no scalability.



11.1.1.2. Implementation (packet modifications)

IPSec modifies packets as shown below (tunnel mode).



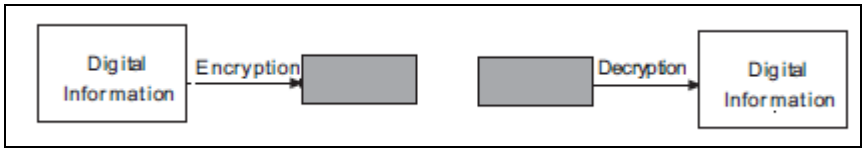
The above modifications provide：

- 11.1.1.2.1. Data Confidentiality (encryption; ESP mode)
- 11.1.1.2.2. Peer Confidentiality (tunnel mode; limited)
- 11.1.1.2.3. Data Integrity / Authentication (signed hash)
- 11.1.1.2.4. Anti-Replay

There is no peer authentication. However, it is assumed that only the authentic peer knows the encryption parameters and keys.

11.1.1.2.1. Data Confidentiality (encryption; ESP mode)

Encryption is symmetric, meaning that the same key to encrypt is used to descrypt.

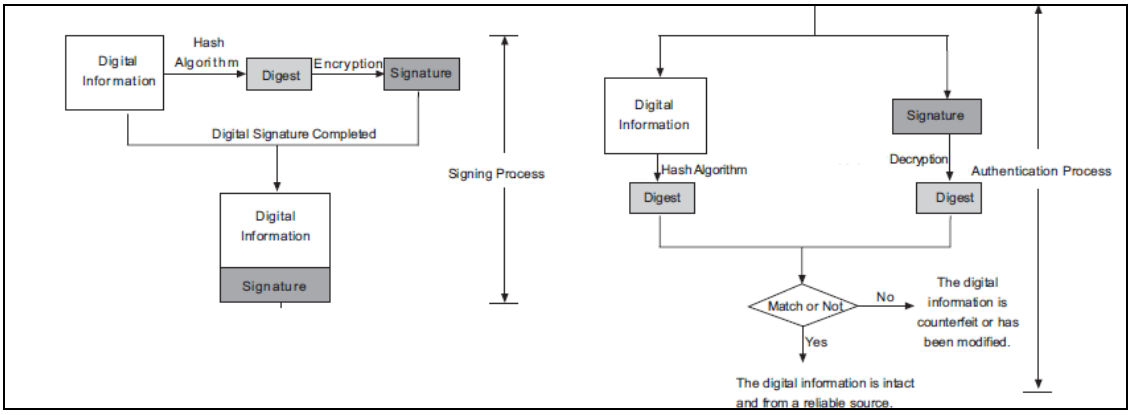


11.1.1.2.2. Peer Confidentiality (tunnel mode; limited)

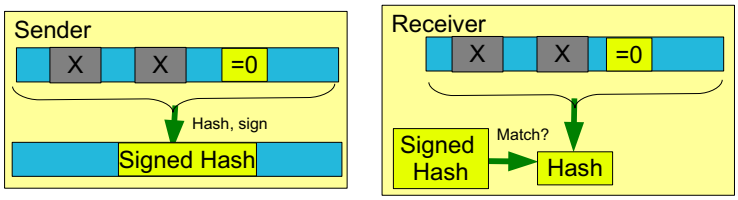
IP1 and IP4 are “hidden” within the encrypted modified packet, so the identities (IPs) of the source/destination are secure. However, IP2 and IP3 are not hidden, therefore the confidentiality is limited.

11.1.1.2.3. Data Integrity / Authentication (signed hash)

The following diagram shows how the original packet data can be hashed and signed.



The following diagram shows how only parts of the original packet are included in the hash.



11.1.1.2.4. Anti-Replay

The attacker may intercept ISAKMP packets and then later replays these packets to the destination to gain access to the destination. Anti-replay protection solves this problem by adding a simple sequence number to each IPSec packet header. The destination prevents replayed packets by dropping IPSEC packets with sequence number that falls outside of an anti-replay window.

11.1.1.3 IPSec SA Security Protocols and Working Modes

Security protocol (AH/ESP) and IPSec mode (transport/tunnel) configurations include:

- 11.1.1.3.1. ESP/Tunnel Mode
- 11.1.1.3.2. AH / Tunnel Mode
- 11.1.1.3.3. ESP / Transport
- AH/Transport

11.1.1.3.1. ESP/Tunnel Mode

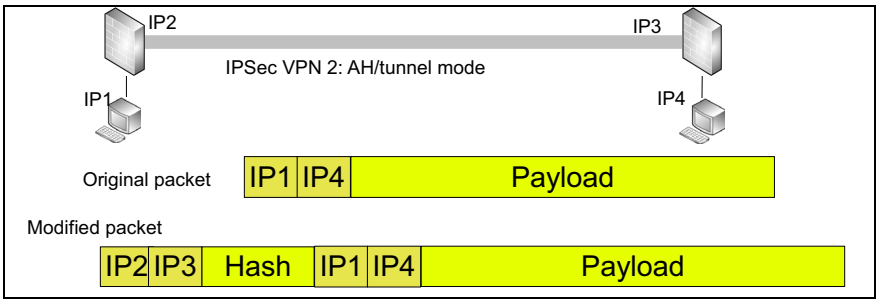
See the figure shown in 11.1.1.2. Implementation (packet modifications) shown on previous page. In tunnel mode, the device is the tunnel gateway and provides:

- Origin authentication
- Partial origin confidentiality (endpoints)
- Data integrity

11.1.1.3.2. AH / Tunnel Mode

In tunnel mode, the device is the tunnel gateway and provides:

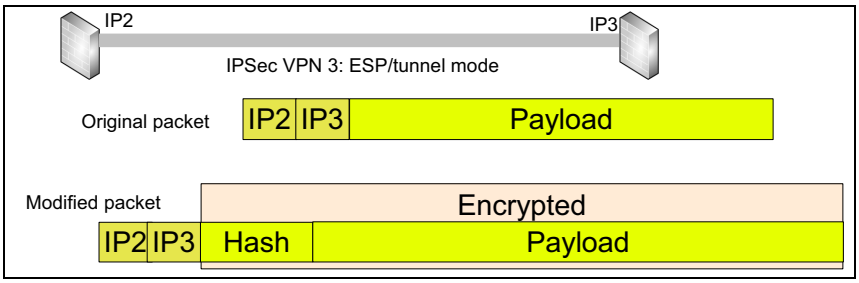
- Origin authentication
- Data integrity



11.1.1.3.3. ESP / Transport

In tranport mode, the device is the endpoints and provides:

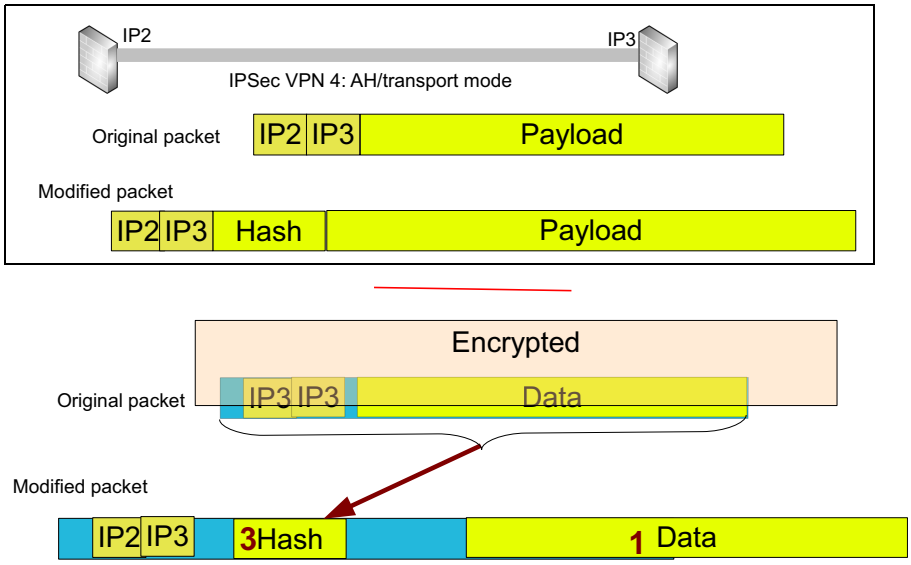
- Origin authentication
- Data integrity
- Data confidentiality (encryption).



AH/Transport

- Origin authentication

- Data integrity
- No encryption. Useful when confidentiality is not important or if the data must not be encrypted

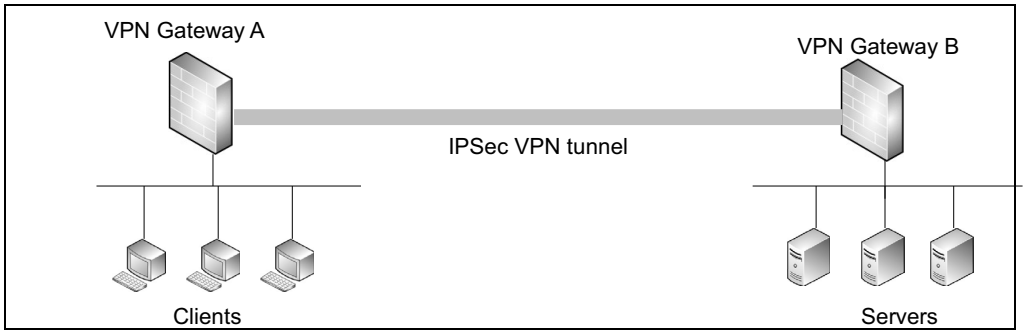


11.1.2. Site to Site IPSec Auto IKE

- 11.1.2.1. Requirements
- 11.1.2.2. Implementation

11.1.2.1. Requirements

The requirements scenario is basically the same as in **11.1.1.1. Requirements.**



Same requirements for

- Data confidentiality
- Peer confidentiality
- Data integrity
- Anti-replay

However, the following extra requirements

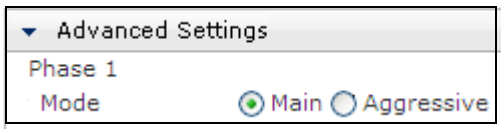
- **Auto key exchange**: Keeping track of all the keys is risky and required much effort. Auto IKE automates key exchange. Auto IKE requires more configuration but saves a lot of time in the long run, and enhances security.
- **Auto SA negotiation**: No need to determine complex security protocol details.
- **Peer authentication**: Using certificates or pre-shared key.

11.1.2.2. Implementation

- 11.1.2.2.1. Phase 1 Main Mode
- 11.1.2.2.2. Phase 1 Aggressive Mode
- 11.1.2.2.3. Phase 2 Quick Mode (CREATE_CHILD_SA)

11.1.2.2.1. Phase 1 Main Mode

In main mode, the initiator and responder of the IKE SA perform three bi-directional exchanges using six packets to complete the exchange in phase 1. Specify main mode in the UI.



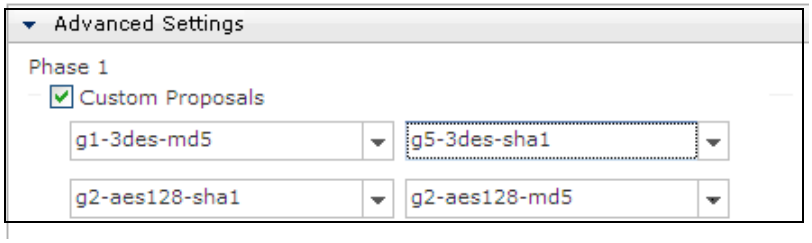
- 11.1.2.2.1.1. P1: Automated SA Determination (IKE_SA_INIT)
- 11.1.2.2.1.2. P1: Key Exchange
- 11.1.2.2.1.3. P1: Verify Initiator ID / Authenticate Messsages (IKE_AUTH)

11.1.2.2.1.1. P1: Automated SA Determination (IKE_SA_INIT)

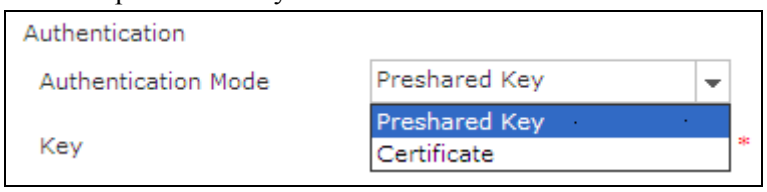
An initiator proposes one or more suites by listing supported algorithms that can be combined into suites in a mix-and-match fashion. Initiator and responder negotiate:

- IKE policies (SA parameters). encryption (3DES or AES), hash (MD5 or SHA-1), DH group (1,2,5), authentication mode (pre-shared key or certificates).
- The DH public value and the nonce value (used in DH exchange).

ID information (e.g., IP address, host name, FQDN).You can specify up to 4 custom SA proposals in UI.

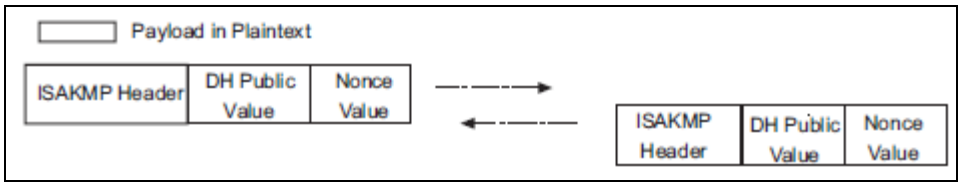


How to set pre-shared key/certificate authentication in the UI:



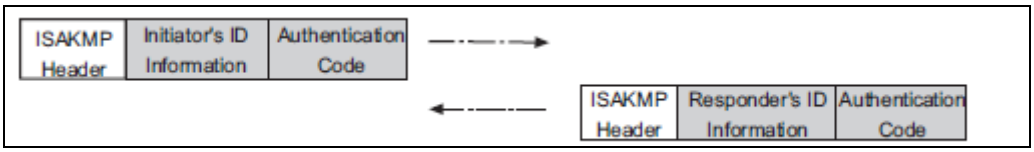
11.1.2.2.1.2. P1: Key Exchange

Two peers exchange DH public values to generate keys.



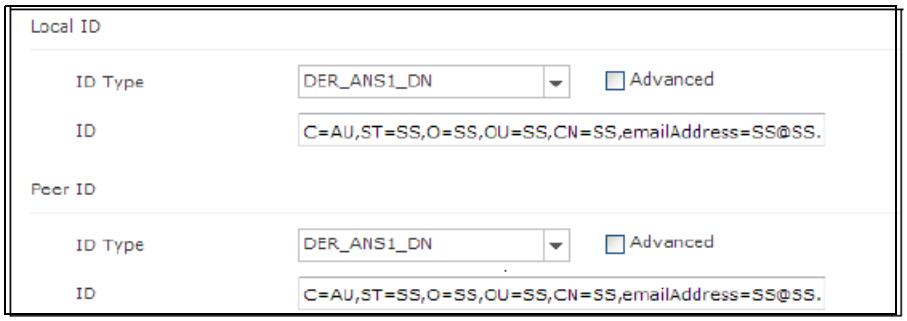
11.1.2.2.1.3. P1: Verify Initiator ID / Authenticate Messsages (IKE_AUTH)

The secret key can now be used to create a secure channel. .

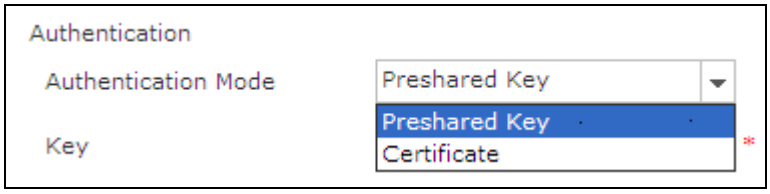


In the secure channel send

- ID infomation. Choose **VPN** > **IPSec VPN** > **Auto IKE** > **Advanced Settings** to specify in the UI.



- Authentication code (encrypt previous message exchanges to generate). Sign 1/2 above using pre-shared key or certificate to authenticate the sender. Choose **VPN** > **IPSec VPN** > **Auto IKE** to set the authentication mode in the UI. If Certificate is set, both peers must have each other's CA certificate:

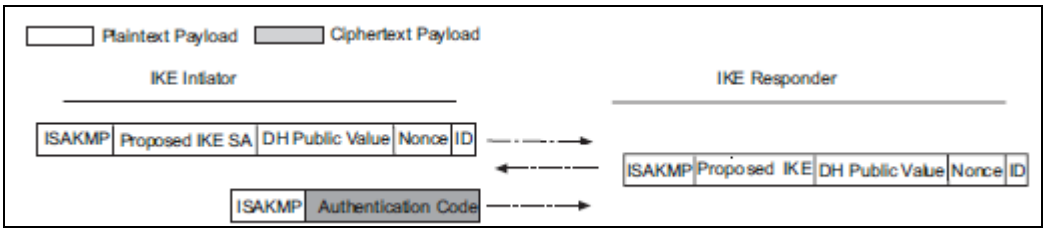


11.1.2.2.2. Phase 1 Aggressive Mode

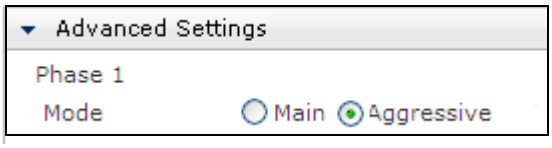
Aggressive mode completes the exchange using only three packets. quicker, but does not protect the ID infomation.

- The first two packets exchange IKE SA parameters, DH public value, nonce value, ID.
- The last packet is the authenticaiton code of the initiator.

The aggressive mode is quicker, but it does not secure the ID information.



Choose **VPN** > **IPSec VPN** > **Auto IKE** > **Advanced Settings** to set aggressive mode in the UI.



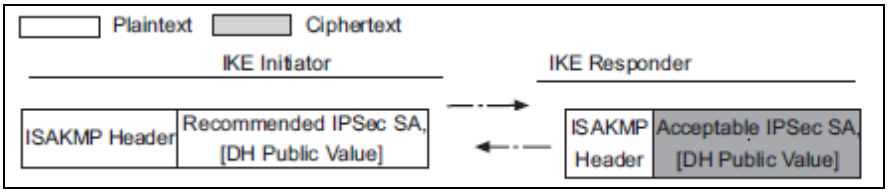
11.1.2.2.3. Phase 2 Quick Mode (CREATE_CHILD_SA)

The message exchange in phase 2 is protected by an IKE SA tunnel. That means the key generated in phase 1 is used to cipher the quick mode IKE response.

SA/keys: First 2 exchanges are used to negotiate IPSec SA strategy and to create keying material. The exchange information includes:

- Security protocol AH/ESP, DH group (specified if PFS enabled), encryption algorithm, and hash.
- DH public value and the ID information of the two peers (specified if PFS is enabled).

1. The accepted SA and DH public value from the responder are encrypted.



Choose **VPN** > **IPSec VPN** > **Auto IKE** > **Advanced Settings** to specify custom proposals.

2. The last exchange is used to verify the participation of the 2 peers in the whole phase, ensuring integrity of IKE negotiation. Authentication code is not encrypted.

11.1.3. Site to Remote Peer IPSec Auto IKE

- 11.1.3.1. Requirements.
- 11.1.3.2. Solution.

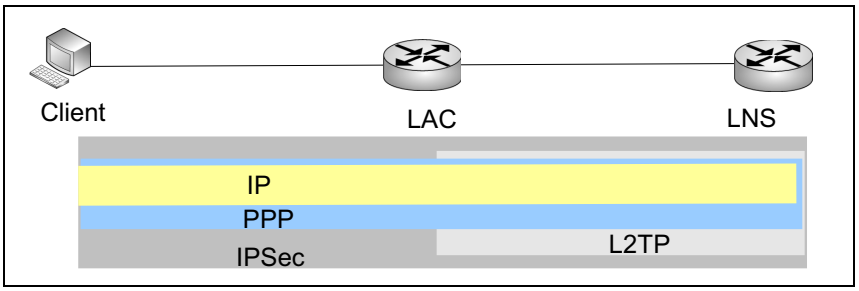
11.1.3.1. Requirements

Dial-in is used primarily for mobile workers to contact the office.
Site to remote peer requirements differ from the previous scenarios because of the following:

- No fixed IP.
- User must have a user account.
- If certificate is used for authentication, certificates must be generated and put on client machine.
- XAuth/L2TP authentication.

11.1.3.2. Solution

Tunnel Between Client / LNS. The client initiates a PPP session to the LAC. The LAC negotiates an L2TP tunnel with the LNS and forwards the client PPP session to the LNS. The client and LNS then negotiate an IPSec tunnel to encrypt the client PPP session.



This solution provides the following:

- Peer confidentiality: remote client IP is known, but changes.
- Peer authentication:certificates or pre-shared key
- User authentication:
  - IPSec VPN
  - local/external
  - Xauth/L2TP
- Payload encryption: ESP
- Payload integrity: HMAC/SHA-1

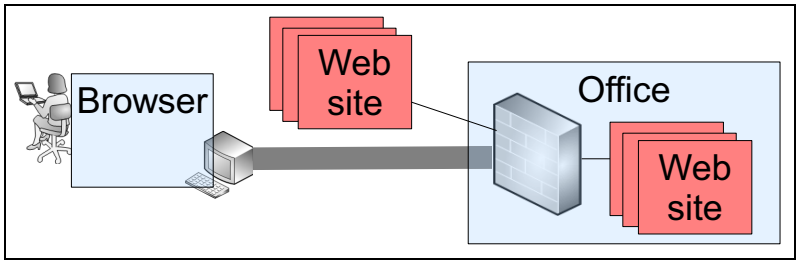
11.1.4. Browser to Site Portal SSL/TLS

- 11.1.4.1. Requirements
- 11.1.4.2. Solution
- 11.1.4.3. Implementation

11.1.4.1. Requirements

User requirements:

- Secure connection from his computer outside the office to websites inside (access work emials, log on to EHR system, ask for leaves, and so on.) and outside the office.
- No need to install a client or configure anything.
- “outside the office” FGX limit the websites to only approved websites and provides security features to prevent malicious conent from these websites.
- Authorized users can add websites to the list.

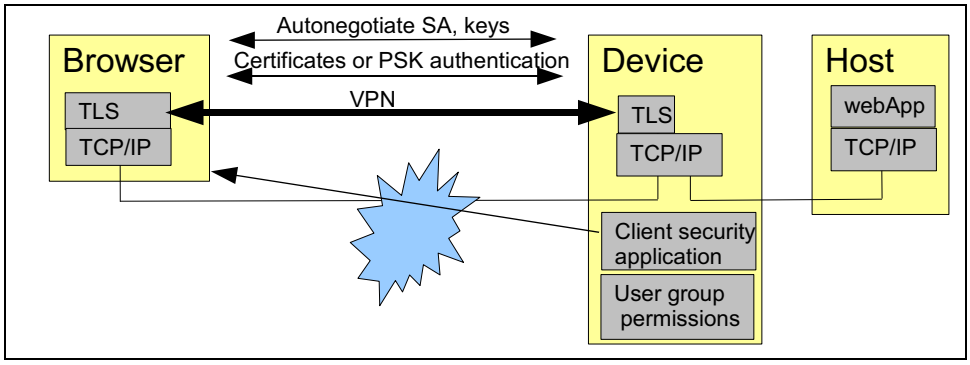


Security requirements

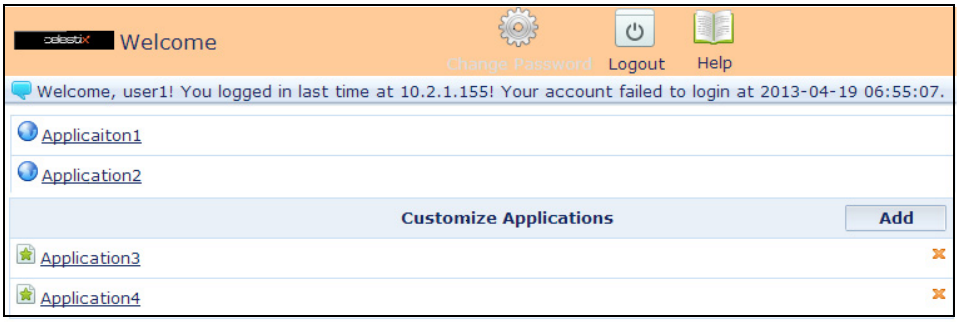
- Auto key exchange
- Bulk encryption algorithm (including secret key length)
- MAC algorithm
- Certificates (for peer authentication)
- User authentication (username/password)

11.1.4.2. Solution

The following shows the basic solution.



The user sees the following in the browser.



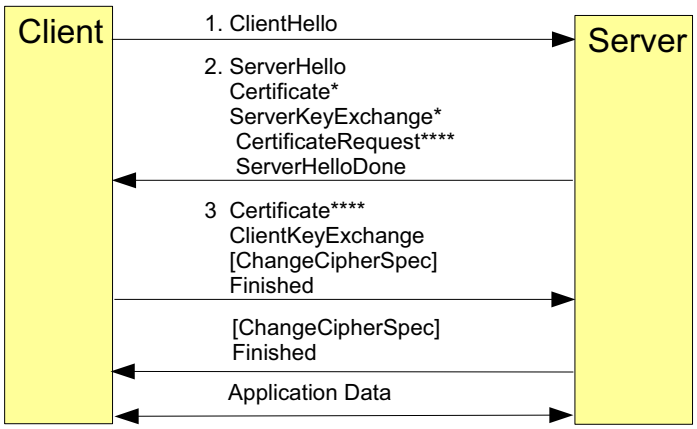
The security mechanisms for the above configuration include:

- Peer confidentiality: None
- Peer authentication: server / SSL client built-in certificates
- User authentication: local/external
- Payload encryption: Yes
- Payload integrity: Yes

11.1.4.3. Implementation

- SSL implementation is quite similar to 11.1.2.2.1. Phase 1 Main Mode. There are 3 basic parts.

The message flow is shown below for a full handshake..



* Indicates optional or situation-dependent messages that are not always sent.
**** = client authentication.

11.1.5. Client to Site SSL/TLS

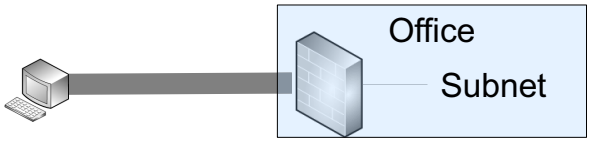
- 11.1.5.1. Requirements
- 11.1.5.2. Solution

This configuration uses a client instead of a browser, but the ciphersuite determination, key and certificate exchange are basically the same as in 11.1.4.3. Implementation.

11.1.5.1. Requirements

A user wants :

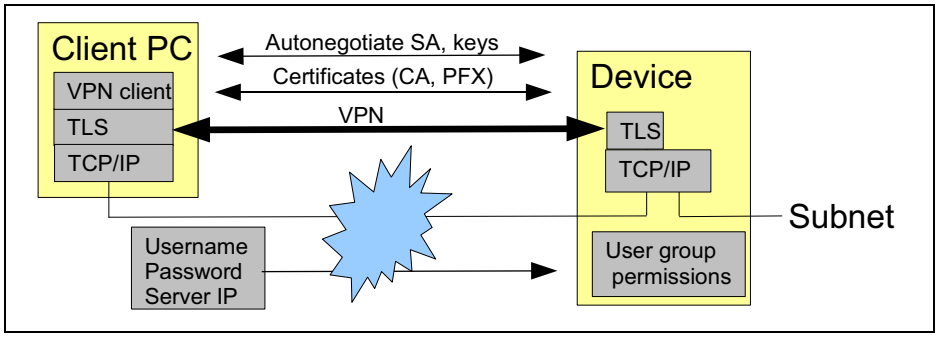
- Secure connection from his computer outside the office to the office network.
- No browser. Client installation is OK.
- No IPSec complexity.
- Auto ciphersuite (SA) negotiation.



Security requirements:

- Key exchange
- Bulk encryption algorithm (including secret key length)
- MAC algorithm
- Certificates (for peer authentication)
- User authentication (username/password)

11.1.5.2. Solution



Following describes the security mechanisms for the above configurations.

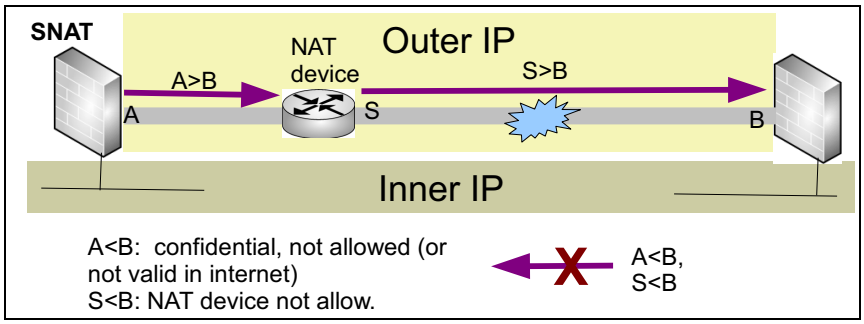
- Peer confidentiality: None
- Peer authentication: Server / SSL client built-in certificates
- User authentication: Local/external (username/password)
- Payload encryption: Yes
- Payload integrity: Yes

11.1.6. Site to Site IPSec VPN (tunnel mode) + NAT

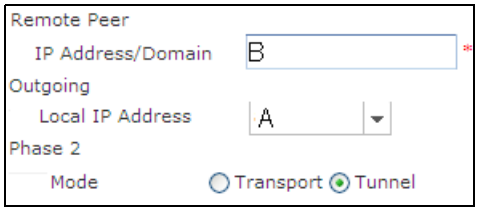
- 11.1.6.1. SNAT
- 11.1.6.2. DNAT
- 11.1.6.3. MIP

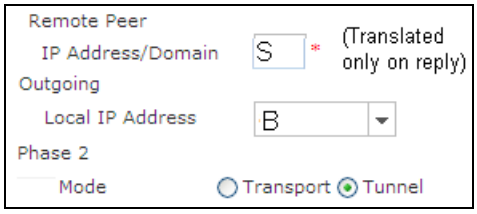
11.1.6.1. SNAT

The following diagram shows the initial packet source (A, S) and destination (B) addresses.VPN tunnel can be inititated from gateway A and cannot be initiated from B because of the SNAT rule.



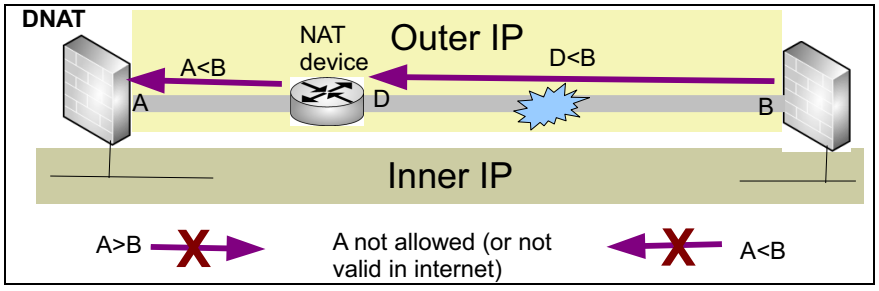
The following shows the configuration (**VPN** > **IPSec VPN** > **Auto IKE**) on both devices in Auto IKE tunnels.



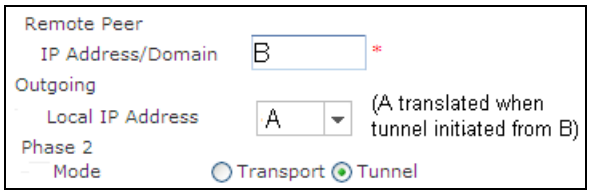


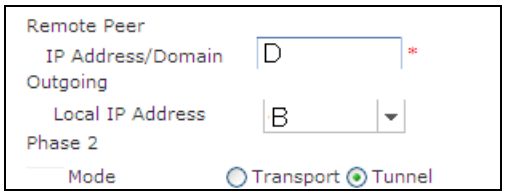
11.1.6.2. DNAT

The following diagram shows the initial packet source (B) and destination (D, A) addresses. The VPN tunnel can be initiated from either direction. The outgoing packets from gateway A is not protected.



The following shows the configuration (**VPN** > **IPSec VPN** > **Auto IKE**) on both devices.

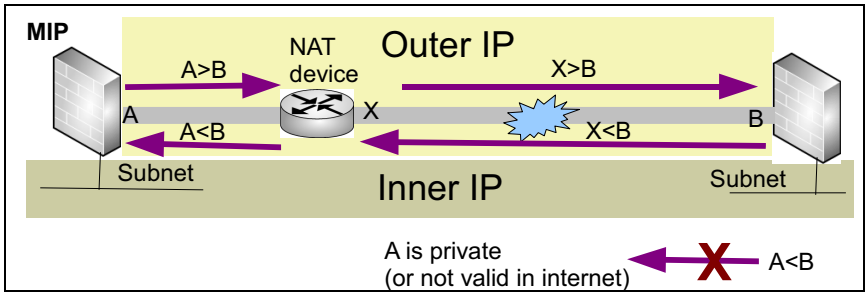




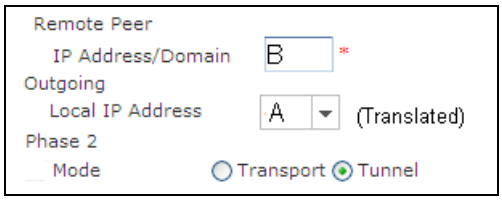
11.1.6.3. MIP

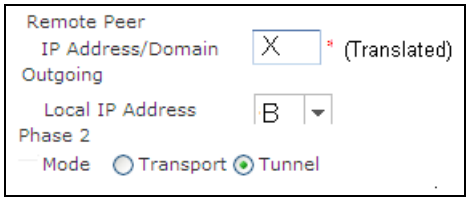
The VPN tunnel can be initiated in either direction. The following diagram shows:

- Initial packet source (A,X) and destination (B) addresses.
- Initial packet source (B) and destination (X, A) addresses.



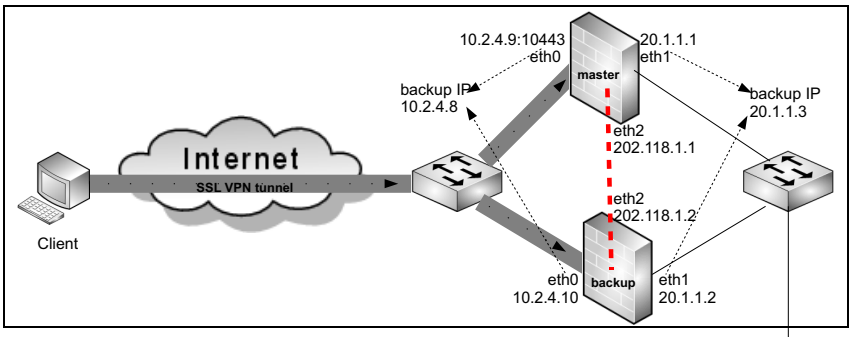
The following shows the configuration (**VPN** > **IPSec VPN** > **Auto IKE**) on both devices.



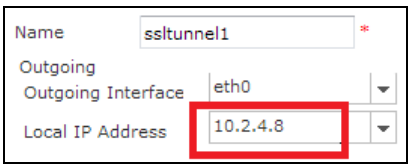


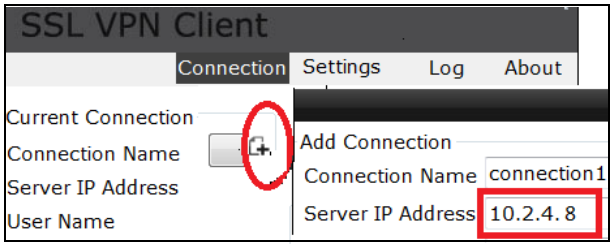
11.1.7. VPN with Virtual Routers (HA)

Same as regular HA, just specify IP as the HA IP.



Specify the VR IP address in the SSL VPN tunnel and client connection dialogs.





11.2. Configuration Basics

This section describes the basic configuration procedure. For your scenario you will do only a subset of the steps listed below.

- 11.2.1. Site to Site IPSec Manual SA (example 1)
- 11.2.2. Site to Site IPSec Auto IKE (example 2)
- 11.2.3. Site to remote peer IPSec AutoIKE (example 3)
- 11.2.4. SSL VPN Web Portal (example 4)
- 11.2.5. SSL VPN Tunnel (example 5)

11.2.1. Site to Site IPSec Manual SA (example 1)

- **11.2.1.1. Pre-Planning**.
- **11.2.1.2. Configuration Steps**.

11.2.1.1. Pre-Planning

Both sides of the VPN must have the required SA parameters (shown in 1.2. Create Manual Tunnel (Authentication/Encryption)), possibly including

- ESP encryption algorithm / key
- ESP authentication algorithm / key
- ESP local / remote SPI
- AH authentication algorithm / key
- AH local / remote SPI.

11.2.1.2. Configuration Steps

1. Create tunnel. Create the tunnel on both devices in **VPN** > **Manual IKE** (for an example, see 1.2. Create Manual Tunnel (Authentication/Encryption).
2. Specify tunnel in route or access policy. On both devices, route packets to the tunnel using **Network** > **Routing** > **Default Routing, Network** > **Routing** > **Policy-Based Routing**, or Firewall / Access Policies (for an example, see 1.3. Route Tunnel).
3. Operation. After configuration is complete, the tunnel is operating. For an example of tunnel monitoring, see 1.4. Monitor Tunnel.

11.2.2. Site to Site IPSec Auto IKE (example 2)

- **11.2.2.1. Pre-Planning**.
- **11.2.2.2. Configuration Steps**.

11.2.2.1. Pre-Planning

For both devices you will require the following information

- **NAT** (is there a NAT device in front of a device)
- Remote static / dynamic IP address, permanent
- Outgoing Interface/Local IP Address
- **Pre-shared key** or **certificates** for peer authentication
- **Subnets** on both sides that will use the tunnel

Advanced settings (usually you use the default settings).

- P1 proposals, main/aggressive, lifetime
- P2 proposals, replay protection, transport / tunnel, lifetime
- **Dead peer detection** (DPD)
- **Local / peer ID** (IPV4_ADDR, etc.)

11.2.2.2. Configuration Steps

1. Import Certificates. Choose **System** > **Certificates** > **CA Certificates** to import a CA certificate. Choose **System** > **Certificates** > **Local Certificates** to import a local certificate.
2. Create IKE Tunnel. Choose **VPN** > **Auto IKE** to create an IKE tunnel (for an example, see 2.2. Create Auto IKE tunnel).
3. Specify tunnel in route or access policy. On both devices, route packets to the tunnel using **Network** > **Routing** > **Default Routing, Network** > **Routing** > **Policy-Based Routing**, or Firewall / Access Policies (for an example, see 1.3. Route Tunnel).
4. Operation. After configuration is complete, the tunnel is operating. For an example of tunnel monitoring, see 2.4. Monitor Tunnel.

11.2.3. Site to remote peer IPSec AutoIKE (example 3)

- 11.2.3.1. Pre-Planning.
- 11.2.3.2. Configuration Steps.

11.2.3.1. Pre-Planning

You may have to configure the following information:

VPN gateway:

- NAT traversal (if there is a NAT device in front of the client or the gateway).
- Remote peer type, outgoing interface/IP.
- Peer authentication: Pre-shared key or certificate. If certificate, then you need the local and peer CA certificate on FGX, and you also need a certificate for the remote client.
- Local and remote subnet IP addresses.

Advanced Settings (usually you use the default settings):

- Optional: P1/P2 IPSec proposals, P1 main/aggressive, P2 transport/tunnel, replay protection, P1/P2 lifetimes. DPD.
- Local and peer ID (IPV4_ADDR, FQDN, etc.)
- Users: specific timeout, multiple logins, password, assigned IP (none, static, IP address pool). DNS/WINS IP's.
- User authentication:
  - Authentication servers
  - XAuth, L2TP
  - WebAUTH (passive/active)

VPN client:

If certificate is used for authentication, you have to import peer's CA and user's local certificates.

11.2.3.2. Configuration Steps

1. Create the certificates or pre-shared keys. For an example see Example 4. SSL VPN Portal. Export peer certificate and install on peer.
2. Configure the remote peer. For an example see 3.2. Configure Remote PC client.
3. Choose **System** > **Authentication** > **Users** to create a new user. For an example, see 3.3. Create IPSec VPN User).
4. Choose **VPN** > **Auto IKE** to create an IKE tunnel. For an example, see 3.4. Create Auto IKE Tunnel.
5. Dial-in with the client. For an example see 3.5. Dialin.

11.2.4. SSL VPN Web Portal (example 4)

- **11.2.4.1. Pre-Planning**.
- **11.2.4.2. Configuration Steps**.

11.2.4.1. Pre-Planning

You need to determine:

- Users:
  - username, specific timeout, multiple logins, password, assigned IP (none, static, IP address pool). DNS/WINS IP's.
  - User authentication: Authentication servers (local/external), XAuth, L2TP, WebAUTH (passive/active).
- SSL VPN gateway:
  - User groups
  - Address pools
  - Applications (URLs)
  - Portal templates (web page design, content, and logo).
  - Portal services: service binding (interfaces, IP's), user groups, portal page, session timeouts, login threshold, verification settings, SSL configuration (certificates, versions, level), client security demands, access allow list, default user authority.

11.2.4.2. Configuration Steps

1. Create / import server SSL certificate. This process is the same as 4.4. Import CA/Local Certificates for IPSec VPN configuraiton.
2. Create SSL VPN Users / groups / ip address pool. Choose **System** > **Authentication** > **Users** to open the **Users** page. Choose **VPN** > **SSL VPN** > **User Groups** to create an SSL VPN user group. For an example see 4.2. Create an IP Address Pool, VPN User, Group.
3. Create applications / templates. Choose **VPN** > **SSL VPN** > **SSL VPN Web Portal** > **Applications** to open the **Applications** page. Choose **VPN** > **SSL VPN** > **SSL VPN Web Portal** > **Portal Templates** to open the **Portal Templates** page. For an example see 4.3. Create SSL VPN Applications, Template.
4. Create SSL VPN Portal Services. For an example see 4.5. Create SSL VPN Services.
5. Operation: 1. Client PC: Install add-in. 2. View. 3. Create custom applications. For an example see 4.6. Access Applications with SSL VPN.

11.2.5. SSL VPN Tunnel (example 5)

- 11.2.5.1. Pre-Planning.
- 11.2.5.2. Configuration Steps.

11.2.5.1. Pre-Planning

You need to determine:

- Users:
  - username, specific timeout, multiple logins, password, assigned IP (none, static, IP address pool), DNS/WINS IP's.
  - User authentication: Authentication servers (local/external), XAuth, L2TP, WebAuth (passive/active).
- User groups
- Address pools

The above is the same as SSL VPN portal. See 11.2.4.1. Pre-Planning.

SSL VPN tunnel specific:

- Remote peer user group.
- Outgoing interfaces, IPs.
- Allowed subnets.

11.2.5.2. Configuration Steps

1. Client install/ configure. To access with an SSL VPN tunnel, the SSL VPN client software should be installed at the client's side. For information about SSL VPN client, see *CELESTIX FGX Integrated Security Software v4.2 SSL VPN Windows Client Users' Guide* or *CELESTIX FGX Integrated Security Software v4.2 SSL VPN Android Client Users' Guide*. For an example see e 5.2. Remote PC: Install Client Software / Add Client Connection.
2. Address pool, users, groups. For an example see e 5.3. Create IP Address Pool, VPN User, Group.
3. Create an SSL VPN Tunnel. Choose **VPN** > **SSL VPN** > **SSL VPN Tunnels** > **Tunnels** to open the **Tunnels** page. For an example see 5.4. Create an SSL VPN Tunnel.
4. Operation. Choose **Monitor** > **Online Users** > **SSL VPN Users** to view online SSL VPN user info. For an example see 5.5. Connect to SSL VPN Server.

11.3. Basic Examples

This document then describes step-by-step how to do hands-on examples:

- **Example 1. Site to Site Manual Tunnel**. How to create a manual tunnel between 2 sites. In the example each site is emulated as a VM on your PC. This is the first example because in many ways its the simplest example, because all parameters are configured manually.
- **Example 2. Site to Site Auto IKE Tunnel**. How to create a tunnel using the automated key generation/management and security management. Although more complex, the techniques in example 2 are much more practical for most real-life applications than those in example 1.
- **Example 3. Site to Remote Peer IPSec Auto IKE**. How to create a tunnel between a Windows client and an FGX device.
- **Example 4. SSL VPN Portal**. How to create a VPN portal that allows remote users to securely open restricted websites.
- **Example 5. SSL VPN Tunnel**. How to create a VPN tunnel between a VPN client and an FGX device.

NAT

- **Example 6. SNAT Traversal (IPSec VPN)**. How to configure IPSec Auto IKE tunnel when there is a NAT device between VPN gateways.

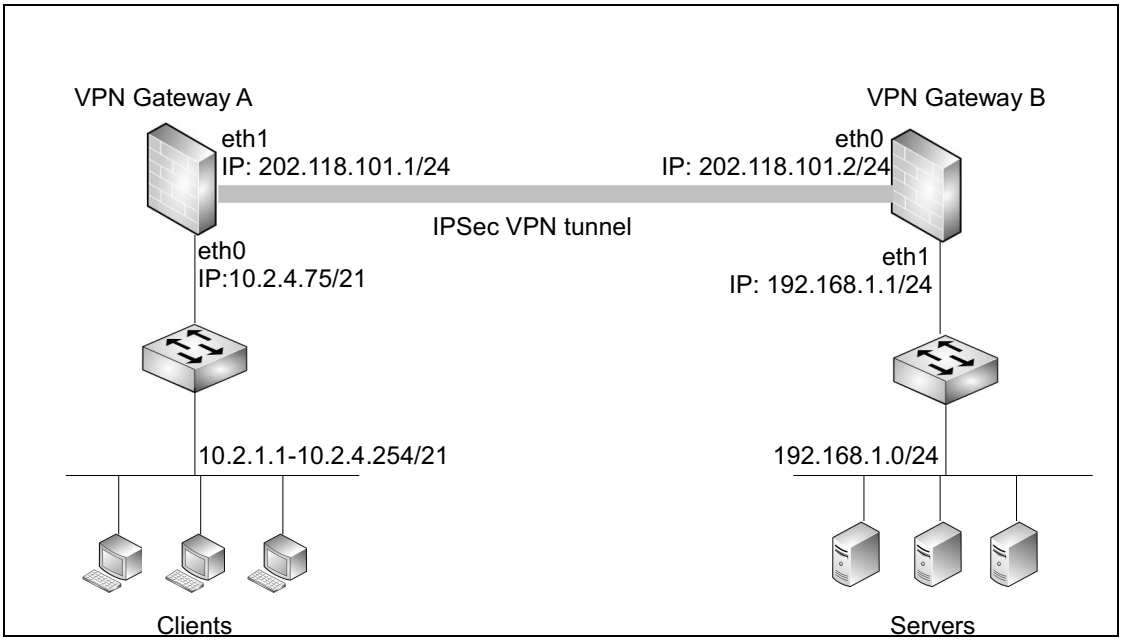
HA

- **Example 7. HA Synchronization (SSL VPN client)**. How to configure SSL VPN tunnel in an HA environment.
- **Example 8. IPSec VPN Tunnel Group (for auto IKE tunnel only)**. How to configure an IPSec VPN tunnel to ensure that the VPN connection between the peers will not be interrupted when the working tunnel fails.

Example 1. Site to Site Manual Tunnel

Scenario

Two offices in different cities require secure link.



Security Requirements

- Encrypted data.
- Internal IP's remain secret.
- Simple setup and maintenance.

Configuration Steps

- 1.1. Configure I/F IP Addresses/Default Route/Default Policy
- 1.2. Create Manual Tunnel (Authentication/Encryption)
- 1.3. Route Tunnel
- 1.4. Monitor Tunnel

1.1. Configure I/F IP Addresses/Default Route/Default Policy

1.1.1. Configure I/F IP Addresses

VPN Gateway A:

1. Choose **Network** > **Interfaces** and configure eth0 and eth1 interfaces:
   - eth0: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 10.2.4.75/21.
   - eth1: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 202.118.101.1/24
2. Click **OK**.

VPN Gateway B:

Configure VPN Gateway B in the same way:

- eth0: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 202.118.101.2/24.
- eth1: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 192.168.1.1/24.

CLI

VPN Gateway A:

```
FGX@root> configure mode override
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] working-type layer3-interface
FGX@root-system-if-eth0] ip address 10.2.4.29 255.255.248.0
FGX@root-system-if-eth0] exit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] working-type layer3-interface
FGX@root-system-if-eth1] ip address 202.118.101.1 255.255.255.0
FGX@root-system-if-eth1] end
FGX@root> save config
```

VPN Gateway B:

Same as the VPN Gateway A with the following changes:

```
FGX@root-system-if-eth0] ip address 202.118.101.2 255.255.248.0
FGX@root-system-if-eth1] ip address 192.168.1.1 255.255.255.0
```

1.1.2. Configure Default Route

VPN Gateway A:

1. Choose **Network** > **Routing** > **Default Routing** and create a default route with

   Type = IPv4 Address, Destination IPv4 Address = 0.0.0.0, Mask Length = 0, Metric = 1, Outgoing Interface/ Gateway = Normal, Interface = eth1, Gateway = 202.118.101.2.
2. Click **OK**.

VPN Gateway B:

Configure VPN Gateway B in the same way.

IPV4 address, destination = 0.0.0.0, mask length = 0, metric = 1, outgoing interface = eth0, gateway = 202.118.101.1.

CLI

VPN Gateway A:

```
FGX@root-system] route 0.0.0.0 0.0.0.0 interface eth1 gateway
202.118.101.2
FGX@root-system] exit
FGX@root> save config
```

VPN Gateway B:

```
FGX@root-system] route 0.0.0.0 0.0.0.0 interface eth0 gateway
202.118.101.1
FGX@root-system] exit
FGX@root> save config
```

1.1.3. Configure Default Policy

VPN Gateway B:

Choose **Firewall** > **Default Policy Settings** and configure the action of default inter-zone policies as **Permit**.

CLI

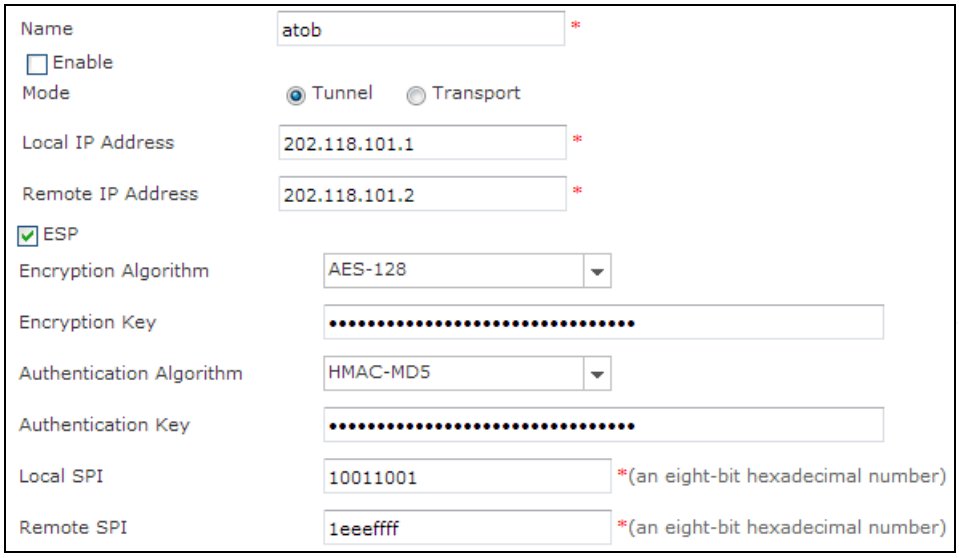
```
FGX@root-system] policy default inter-zone access permit
FGX@root-system] exit
FGX@root> save config
```

Note: No default access policy is required for VPN Gateway A because an access policy will be customized later in 1.3. Route Tunnel to be used together with the manual tunnel.

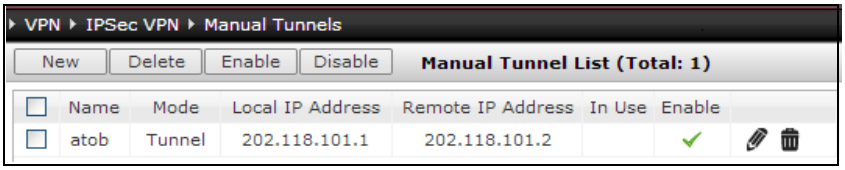
1.2. Create Manual Tunnel (Authentication/Encryption)

VPN Gateway A

1. Choose **VPN** > **Manual IKE** to open the **Manual IKE** page.
2. Click **New** and configure as follows (do not enable tunnel):



3. Click OK. Enable the tunnel. Save the configuration.

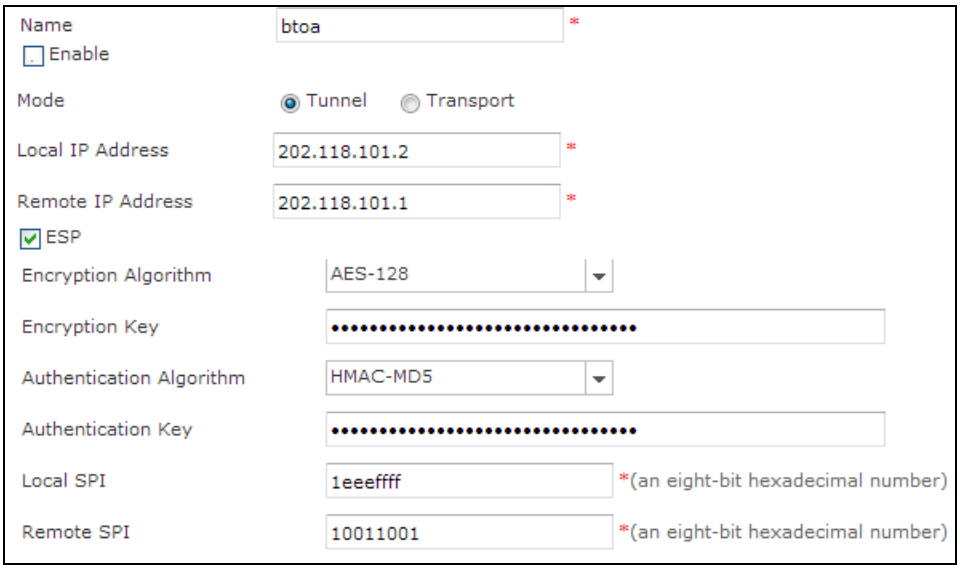


CLI

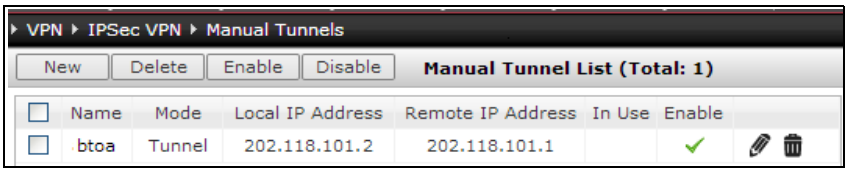
```
FGX@root-system-vpn] tunnel atob manual gateway remote-ip
202.118.101.2 local-ip 202.118.101.1 esp 10011001 1eeeffff auth
hmac-md5 key 6c6a79b4357c6c6a6c6a79b4357c6c6a encrypt aes128 key
6c6a79b4357c6c6a6c6a79b4357c6c6a mode tunnel enable
```

VPN Gateway B:

1. Choose **VPN** > **Manual IKE** to open the **Manual IKE** page.
2. Click **New** and configure as follows (do not enable tunnel):



3. Click OK. **Enable the tunnel.** Save the configuration.



CLI

```
FGX@root-system-vpn] tunnel btoa manual gateway remote-ip
202.118.101.1 local-ip 202.118.101.2 esp 1eeeffff 10011001 auth
hmac-md5 key 6c6a79b4357c6c6a6c6a79b4357c6c6a encrypt aes128 key
6c6a79b4357c6c6a6c6a79b4357c6c6a mode tunnel enable
```

1.3. Route Tunnel

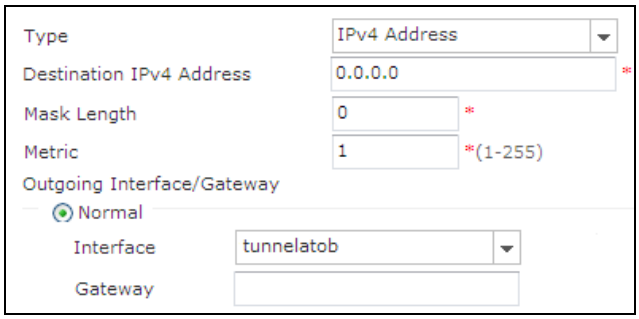
There are four ways of selecting the tunnel for the packets. This section demonstrates:

- 1.3.1. Default Route
- 1.3.2. Static Route
- 1.3.3. Routing Policy / Route (Default or Static)
- 1.3.4. Firewall Access policy

1.3.1. Default Route

By default packets are routed through the tunnel.

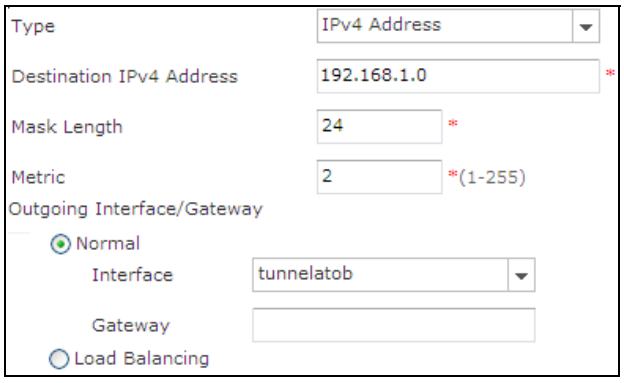
VPN Gateway A:



1.3.2. Static Route

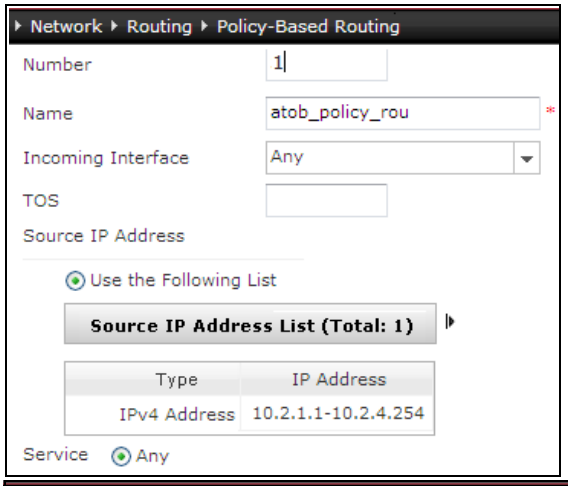
Only packets matching the destination IP addressses are routed through the tunnel.

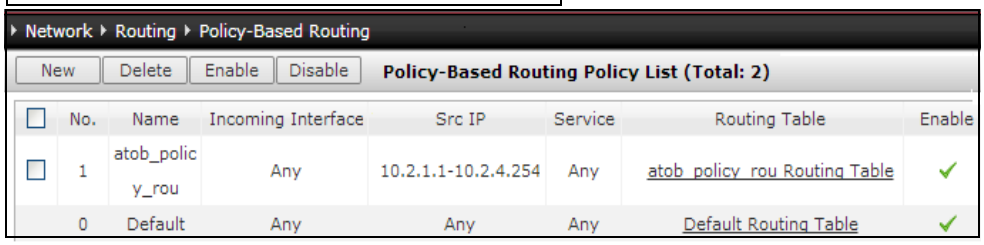
VPN Gateway A:

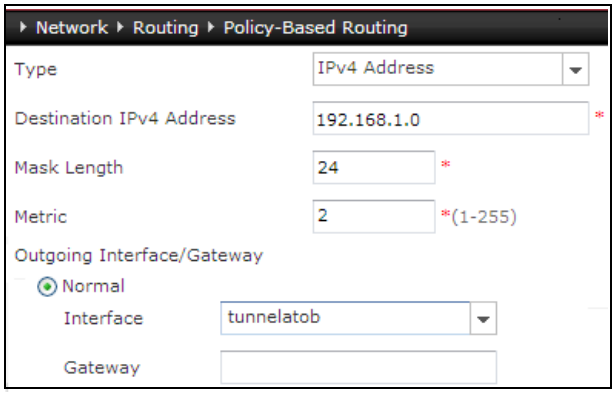


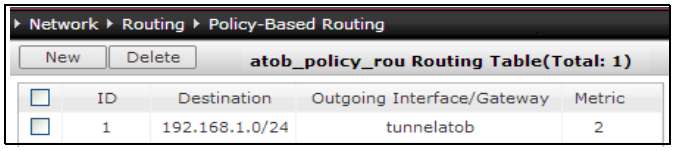
1.3.3. Routing Policy / Route (Default or Static)

VPN Gateway A:


Network ▸ Routing ▸ Policy-Based Routing
Number
1
Name
atob_policy_rou
*
Incoming Interface
Any
TOS
Source IP Address
Use the Following List
Source IP Address List (Total: 1)
Type
IP Address
IPv4 Address
10.2.1.1-10.2.4.254
Service
Any


Network ▸ Routing ▸ Policy-Based Routing
New
Delete
Enable
Disable
Policy-Based Routing Policy List (Total: 2)
No.
Name
Incoming Interface
Src IP
Service
Routing Table
Enable
1
atob_policy_rou
Any
10.2.1.1-10.2.4.254
Any
atob_policy_rou Routing Table
0
Default
Any
Any
Any
Default Routing Table

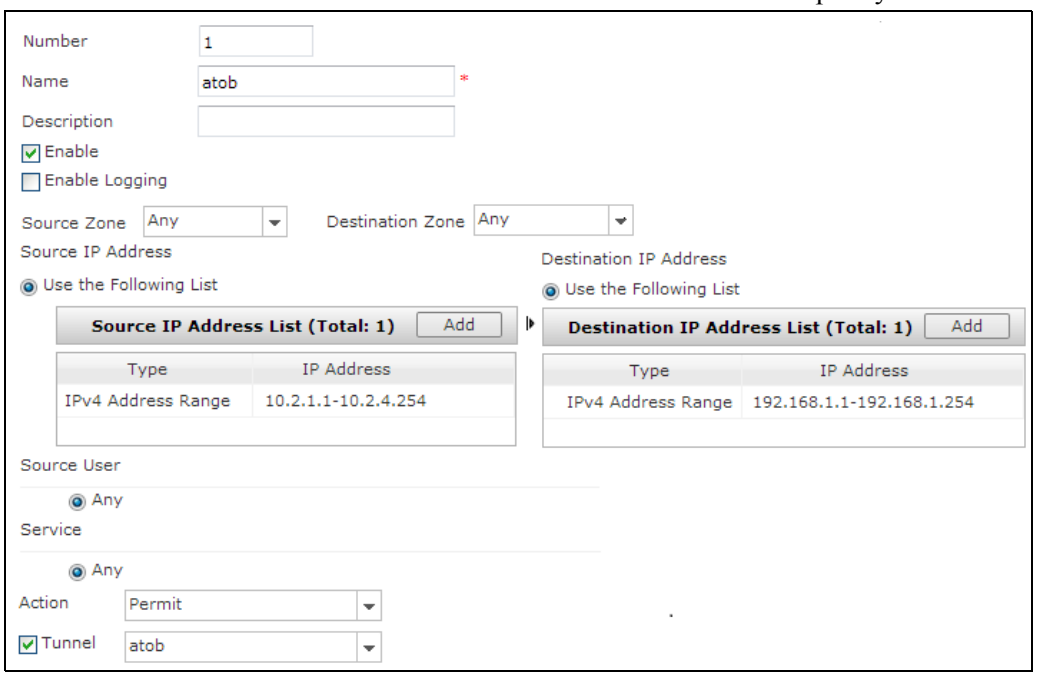

Network ▸ Routing ▸ Policy-Based Routing
Type
IPv4 Address
Destination IPv4 Address
192.168.1.0
*
Mask Length
24
*
Metric
2
*(1-255)
Outgoing Interface/Gateway
Normal
Interface
tunnelatob
Gateway


Network ▸ Routing ▸ Policy-Based Routing
New
Delete
atob_policy_rou Routing Table(Total: 1)
ID
Destination
Outgoing Interface/Gateway
Metric
1
192.168.1.0/24
tunnelatob
2

1.3.4. Firewall Access policy

VPN Gateway A:

Choose **Firewall** > **Access Policies** and click **New** to create an access policy.



CLI

```
FGX@root-system] policy access 1to2 any 10.2.1.1-10.2.4.254 any
192.168.1.1-192.168.1.254 any any permit enable
FGX@root-system] policy access 1to2 tunnel atob
FGX@root-system] exit
FGX@root> save config
```

1.4. Monitor Tunnel

On both sides: Choose **Monitor > VPN Tunnel > Manual Tunnels** to open the Manual Tunnels page and view the information of the VPN tunnel.

VPN Gateway A/B:

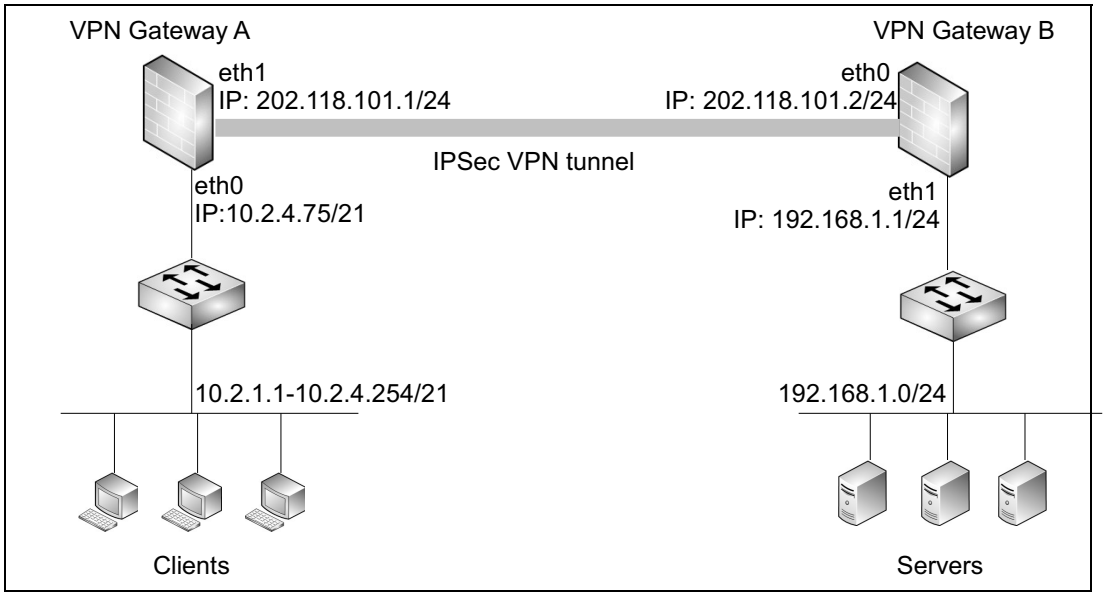
Basic Information	
Name	atob
Local IP Address	202.118.101.1
Remote IP Address	202.118.101.2
Mode	Tunnel
ESP	true
Auth ALG	hmac-md5
ENC ALG	aes128
Local SPI	10011001
Remote SPI	1eeeffff
AH	false

Basic Information	
Name	btoa
Local IP Address	202.118.101.2
Remote IP Address	202.118.101.1
Mode	Tunnel
ESP	true
Auth ALG	hmac-md5
ENC ALG	aes128
Local SPI	1eeeffff
Remote SPI	10011001
AH	false

Example 2. Site to Site Auto IKE Tunnel

Scenario

The following diagram shows a basic IKE site-to-site IPSec VPN tunnel.



Security Requirements:

- Auto SA negotiation
- IKE negotiation of keys
- Preshared key or certificates for peer authentication

Configuration Steps

- 2.1. Configure I/F IP Addresses, Default Route / Access Policy
- 2.2. Create Auto IKE tunnel
- 2.3. Route Tunnel
- 2.4. Monitor Tunnel

2.1. Configure I/F IP Addresses, Default Route / Access Policy

2.1.1. Configure I/F IP Addresses

VPN Gateway A:

1. Choose **Network** > **Interfaces** and configure eth0 and eth1 interfaces:
   - eth0: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 10.2.4.75/21.
   - eth1: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 202.118.101.1/24.
2. Click OK.

VPN Gateway B:

Configure the remote peer in the same way:

- eth0: On, Layer 3, MTU=1500, Static IP, Primary IP address = 202.118.101.2/24.
- eth1: On, Layer 3, MTU=1500, Static IP, Primary IP address = 192.168.1.1/24

CLI

VPN Gateway A:

```
FGX@root> configure mode override
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] working-type layer3-interface
FGX@root-system-if-eth0] ip address 10.2.4.75 255.255.248.0
FGX@root-system-if-eth0] exit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] working-type layer3-interface
FGX@root-system-if-eth1] ip address 202.118.101.1 255.255.255.0
FGX@root-system-if-eth1] exit
FGX@root> save config
```

VPN Gateway B:

Same as the VPN Gateway A with the following changes:

```
FGX@root-system-if-eth0] ip address 202.118.101.2 255.255.248.0
FGX@root-system-if-eth1] ip address 192.168.1.1 255.255.255.0
```

2.1.2. Configure Default Route

VPN Gateway A:

1. Choose **Network** > **Routing** > **Default Routing** and create a default route with

   Type = IPv4 Address, Destination IPv4 Address = 0.0.0.0, Mask Length = 0, Metric = 1, Outgoing Interface/ Gateway = Normal, Interface = eth1, Gateway = 202.118.101.2.
2. Click OK.

VPN Gateway B:

Configure VPN Gateway B in the same way.

IPV4 Address, Destination = 0.0.0.0, Mask Length = 0, Metric = 1, Outgoing Interface = eth0, Gateway = 202.118.101.1

CLI

VPN Gateway A:

```
FGX@root-system] route 0.0.0.0 0.0.0.0 interface eth1 gateway
202.118.101.2
FGX@root-system] exit
FGX@root> save config
```

VPN Gateway B:

```
FGX@root-system] route 0.0.0.0 0.0.0.0 interface eth0 gateway
202.118.101.1
FGX@root-system] exit
FGX@root> save config
```

2.1.3. Configure Access Policy

VPN Gateway A:

1. Choose **Firewall** > **Access Policies** and create a policy:
   - Number =1, Name = 1to2, Enable checked
   - Source Zone = Any, Source IP Address = Use the following List, Source IP Address List Type = IPv4 Address Range= 10.2.1.1-10.2.4.254
   - Source User = Any
   - Destination Zone = Any, Destination IP Address = Use the following List, Destination IP Address List Type = IPv4 Address Range, IP Address = 192.168.1.1-192.168.1.254.
   - Service=Any, Action=Permit.
2. Click OK.

VPN Gateway B:

Choose **Firewall** > **Default Policy Settings** and set the action of default inter-zone policies as Permit. Custom access policies are not required.

CLI

VPN Gateway A:

```
FGX@root-system] policy access 1to2 any 10.2.1.1-10.2.4.254 any
192.168.1.1-192.168.1.254 any any permit enable
FGX@root-system] exit
FGX@root> save config
```

VPN Gateway B:

```
FGX@root-system] policy default inter-zone access permit
```

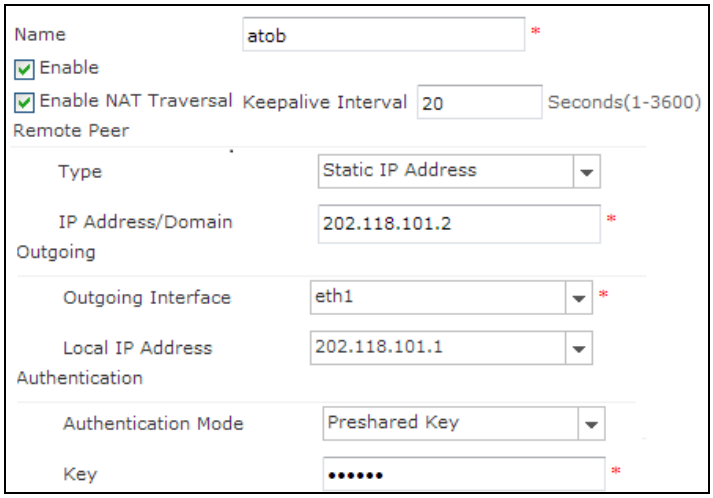
2.2. Create Auto IKE tunnel

- 2.2.1 Pre-Shared Key Authentication
- 2.2.2. Certificate Authentication

2.2.1 Pre-Shared Key Authentication

VPN Gateway A:

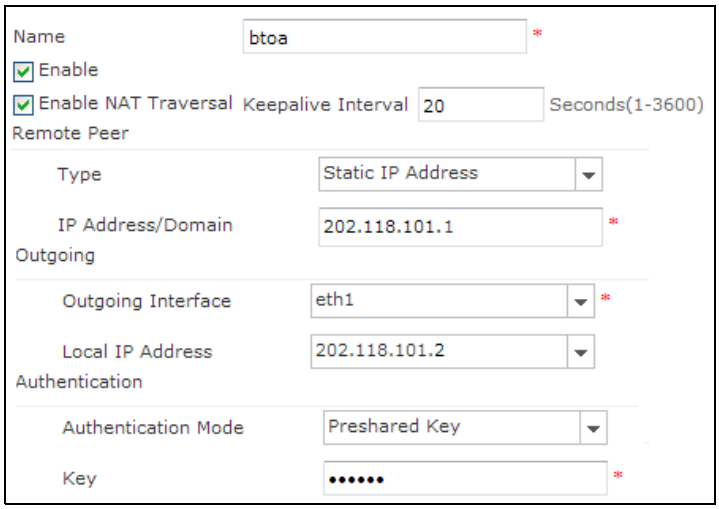
1. Choose **VPN** > **IPSec VPN** > **Auto IKE** to create a new tunnel.



2. Set local and remote subnets. Local Subnet=10.2.0.0/21, Remote Subnet =192.168.1.0/24.

VPN Gateway B:

1. Choose VPN > IPSec VPN > Auto IKE to create a new tunnel.



2. Set local and remote subnets. Local Subnet=192.168.1.0/24, Remote Subnet=10.2.0.0/21.

2.2.2. Certificate Authentication

- 2.2.2.1. Generate or Import Certificates

- Ex2.2.2.2. Create Auto IKE Tunnel with Certificates

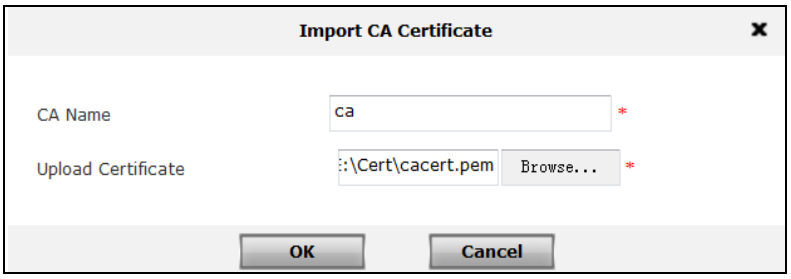
2.2.2.1. Generate or Import Certificates

If there is no available CA and local certificates, you can request a CA and local certificate from CA authority. For information about how to generate certificates, see 3.23.3 Example: Generate Certificates.

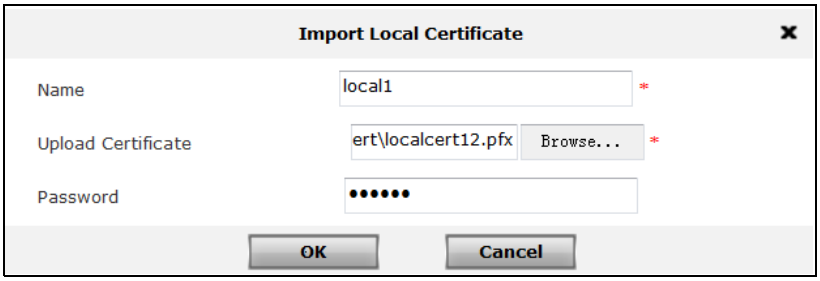
If you already have certificates, follow the steps below to import certificates.

VPN Gateway A:

1. Choose **System** > **Certificates** > **CA Certificates** to open the **CA Certificates** page.
2. Click **Import**.



3. Click **OK**.
4. Choose **System** > **Certificates** > **Local Certificates** to open the **Local Certificates** page.
5. Click **Import**.



6. Click **OK**.

VPN Gateway B:

Import the certificates in the same way.

Note: The remote peer must have the CA of the local and the local peer must have the CA of the remote. The CA certificates of the two peers can be the same. Each peer has its own local certificate.

CLI

VPN Gateway A:

```
FGX@root-system] import vpn certificate ca from x/zmodem CA
FGX@root-system] import vpn certificate local from x/zmodem local1
FGX@root-system] exit
FGX@root> save config
```

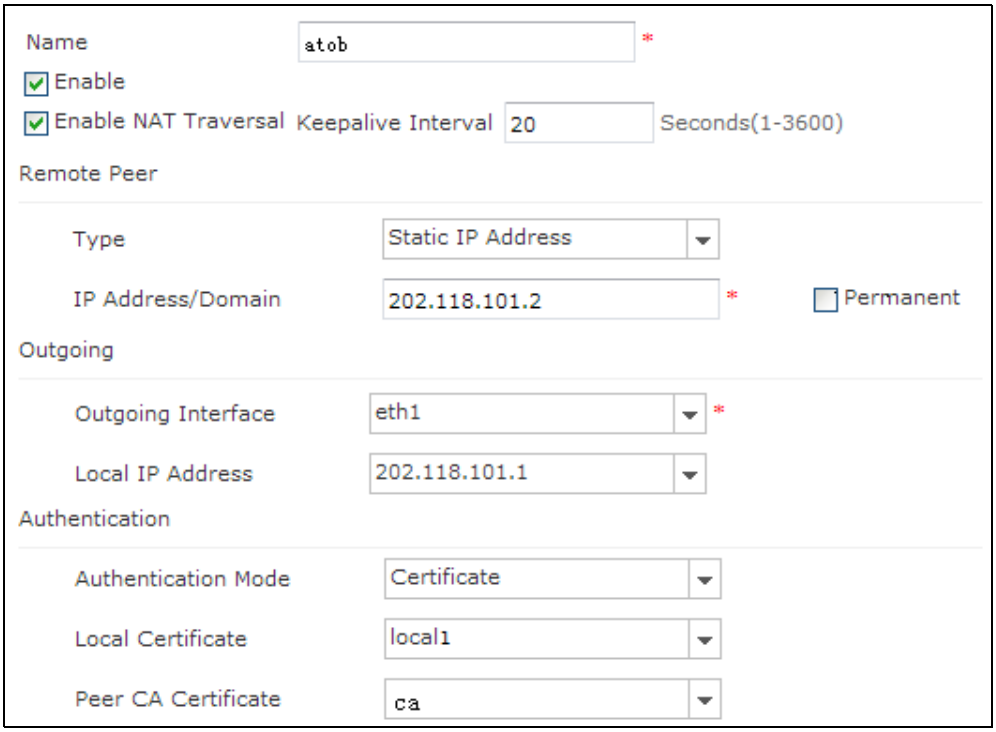
VPN Gateway B:

```
FGX@root-system] import vpn certificate ca from x/zmodem CA
FGX@root-system] import vpn certificate local from x/zmodem local2
FGX@root-system] exit
FGX@root> save config
```

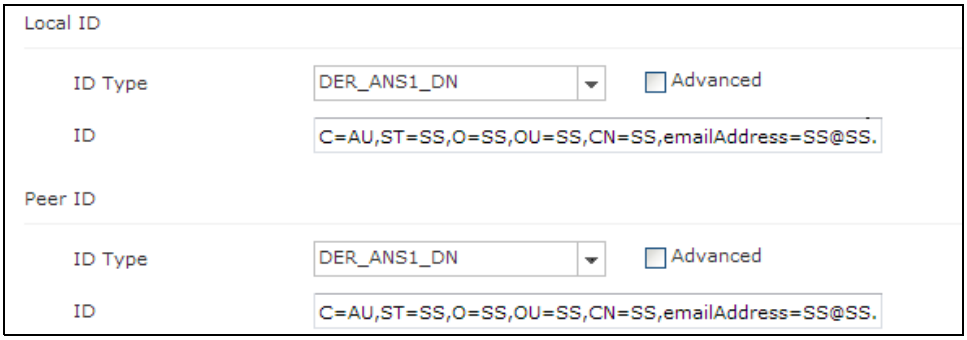
Ex2.2.2.2. Create Auto IKE Tunnel with Certificates

VPN Gateway A:

1. Choose **VPN** > **Auto IKE** to open the **Auto IKE** page.
2. Click **New** and configure as follows:



3. Click **Advanced Settings** and set the local and peer local ID values. The ID values are the subject information of the local certificates of both peers.



4. Click **OK**.

VPN Gateway B:

5. Configure the same for VPN Gateway B with the following differences:

   Name = btoa, Remote Peer IP address = 202.118.101.1, Outgoing Interface = eth0, Local IP Address = 202.118.101.2, Local Certificate = local2.

6. Configure the local and peer ID values as follows:

   - Local ID:

   ID Type=DER_ANS1_DN,
   ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com.

   - Peer ID:

   ID Type=DER_ANS1_DN,
   ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com.

CLI

VPN Gateway A:

```
FGX@root-system-vpn] tunnel atob gateway 202.118.101.2 interface eth1
202.118.101.1 certificate local1 CA enable
FGX@root-system-vpn]tunnel atob ike local-id asn1-dn
ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
FGX@root-system-vpn]tunnel atob ike peer-id asn1-dn
ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
FGX@root-system-vpn] end
FGX@root> save config
```

VPN Gateway B:

```
FGX@root-system-vpn] tunnel btoa gateway 202.118.101.1 interface eth1
202.118.101.2 certificate local2 CA enable
FGX@root-system-vpn]tunnel btoa ike local-id asn1-dn
ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
FGX@root-system-vpn]tunnel btoa ike peer-id asn1-dn
ID=C=AU,ST=SS,O=SS,OU=SS,CN=SS,emailAddress=SS@SS.com
FGX@root-system-vpn] end
FGX@root> save config
```

2.3. Route Tunnel

The same as 1.3. Route Tunnel.

2.4. Monitor Tunnel

Choose **Monitor** > **IPSec VPN Tunnel** > **Auto IKE** to open the **Auto IKE** page and view the information of the VPN tunnel.

VPN Gateway A/B:

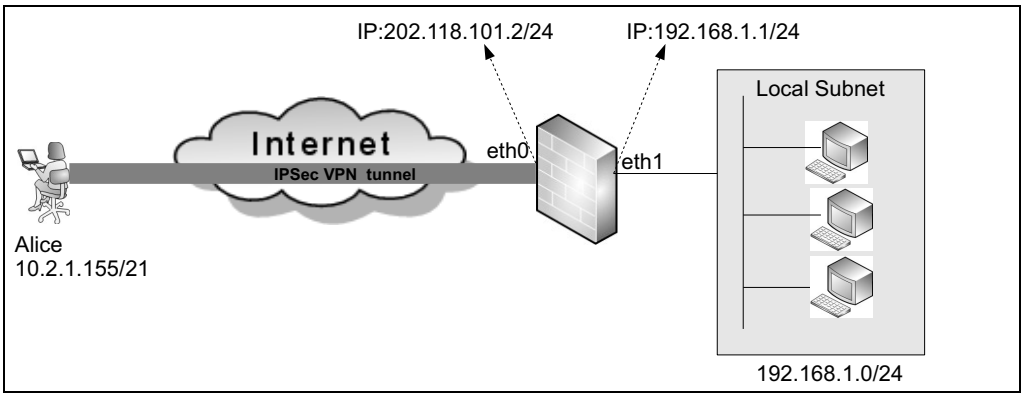
Basic Information	
Name	atob
Remote Peer Type	Static IP Address
Remote Peer Information	202.118.101.2
Dial-In IP Address	202.118.101.2
Outgoing Interface	eth1
Local IP Address	202.118.101.1
Authentication Method	Certificate

Basic Information	
Name	btoa
Remote Peer Type	Static IP Address
Remote Peer Information	202.118.101.1
Dial-In IP Address	202.118.101.1
Outgoing Interface	eth0
Local IP Address	202.118.101.2
Authentication Method	Certificate

Example 3. Site to Remote Peer IPSec Auto IKE

Scenario:

You want a remote user to use IPSec to create a VPN to the internal network.



Security Requirements:

- Dial-in peer L2TP IPSec.
- Auto SA negotiation.
- IKE negotiation of keys.
- Pre-shared key or certificates for peer authentication.

Configuration Steps:

- 3.1. Configure I/F IP Addresses, Default Policy
- 3.2. Configure Remote PC client
- 3.3. Create IPSec VPN User
- 3.4. Create Auto IKE Tunnel
- 3.5. Dialin
- 3.6. Monitor Tunnel

3.1. Configure I/F IP Addresses, Default Policy

3.1.1. Configure I/F IP Addresses

1. Choose **Network** > **Interfaces** and configure eth0 and eth1 interfaces:
   - eth0: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 202.118.101.2/24.
   - eth1: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 192.168.1.1/24
2. Click OK.

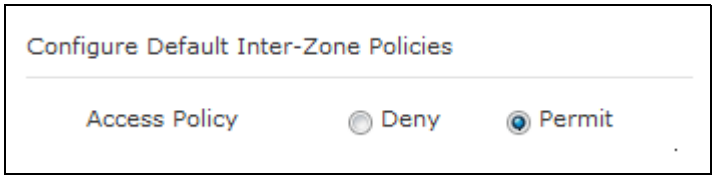
CLI

```
FGX@root> configure mode override
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] working-type layer3-interface
FGX@root-system-if-eth0] ip address 202.118.101.2 255.255.255.0
FGX@root-system-if-eth0] exit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] working-type layer3-interface
FGX@root-system-if-eth1] ip address 192.168.1.1 255.255.255.0
FGX@root-system-if-eth1] exit
FGX@root> save config
```

3.1.2. Default Policy

1. Choose **Firewall** > **Default Policy Settings** and configure：

   Default Inter Zone Policies / **Access Policy** = **Permit**.



2. Click **OK**.

CLI

```
FGX@root-system] policy default inter-zone access permit
FGX@root-system] exit
FGX@root> save config
```

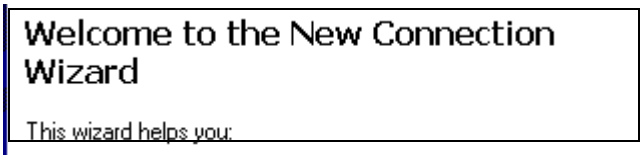
3.2. Configure Remote PC client

Remote IPSec VPN users can configure Windows built-in client or install VPN client software to access the VPN server.

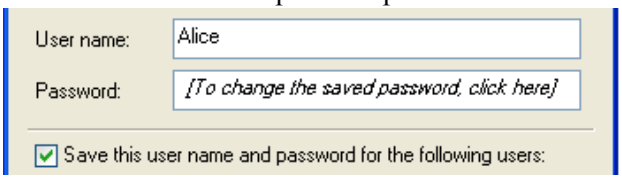
- 3.2.1. Configure Windows Built-In Client
- 3.2.2 Configure Neusoft NetEye VPN Client
- 3.2.3 Configure TheGreenBow VPN Client

3.2.1. Configure Windows Built-In Client

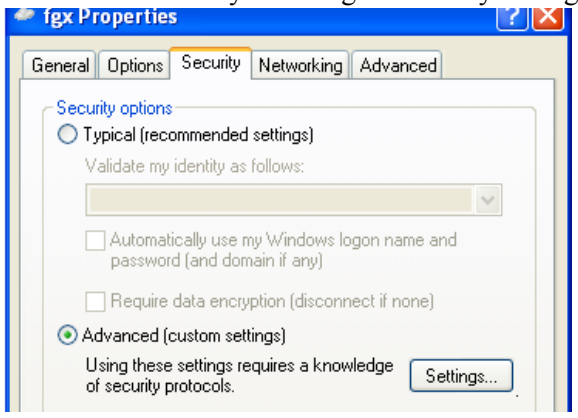
1. Choose Start > All Programs > Accessories > Communications > Network Connections.
2. Choose “Create a new connection” in Network Tasks, and the following window appears:



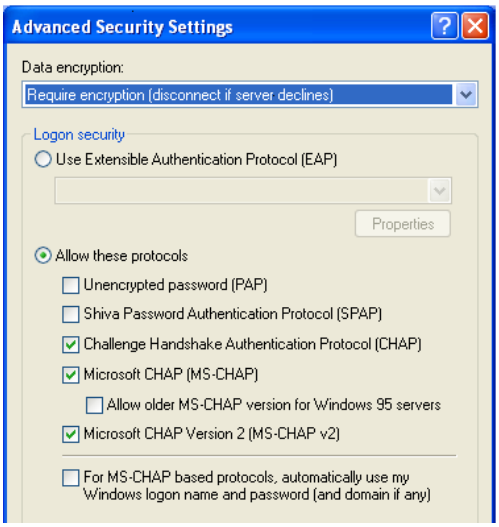
3. Click Next.
4. Select “Connect to the network at my workplace” and click Next.
5. Select “Virtual Private Network connection” and click Next.
6. Enter the company name and click Next.
7. Select “Do not dial the initial connection” and click Next.
8. Enter the outgoing interface address of the tunnel (202.118.101.2) and click Next.
9. Click Finish to complete the process.



10. Click Properties in the pop-up window.
11. Choose Security to configure security settings.



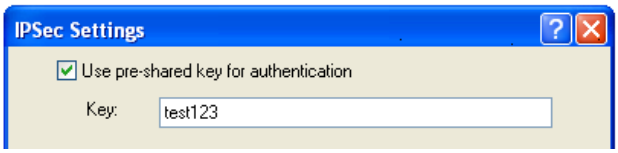
12. Choose Advanced (custom settings) and click Settings.



13. Check Challenge Handshake Authentication Protocol (CHAP) and click OK.

14. Configure pre-shared key authentication and certificate authentication.

- Configure pre-shared key authentication. Click IPSec Settings..., check "Use pre-shared key for authentication," set the preshared key as test123, and click OK.

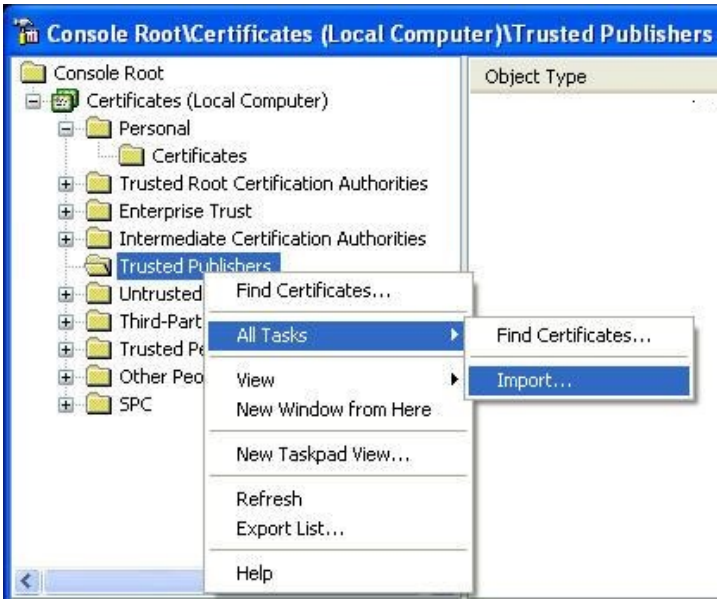


Note: When certificate authentication is used, uncheck "Use pre-shared key for authentication".

- Configure certificate authentication (import certificates).
  - **a.** Click **Start** > **Run** and enter the **mmc** command.
  - **b.** Click **File** > **Add/Remove Snap-in...**to add certificates.

  - **c.** Choose **Computer account** > **Local computer** (**the computer this console is running on**).
  - **d.** Expand the **Certificates** node under Console Root and import personal and CA certificates.
    - Import personal certificate:

- Import CA certificate:



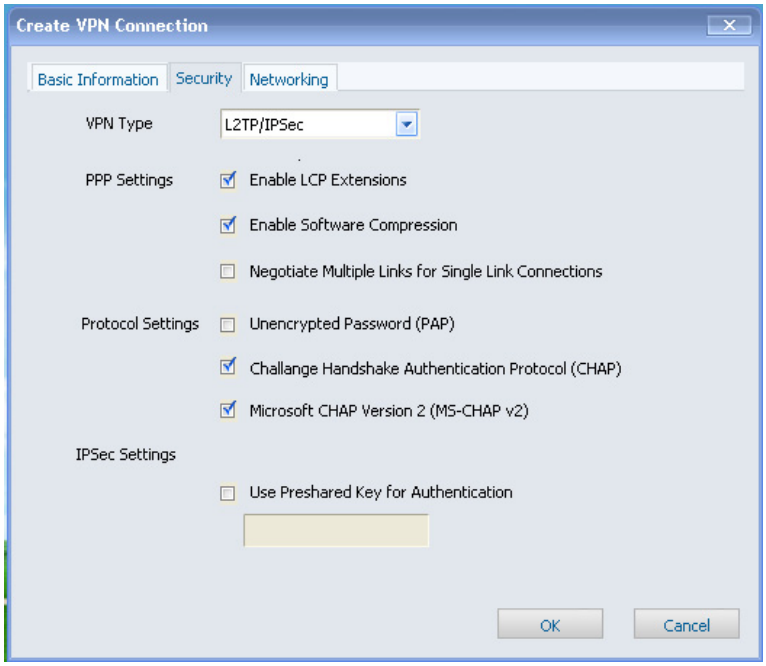
15. Choose Networking and select L2TP IPSec VPN from the Type of VPN drop-down list. Click OK to return to the connection window.

3.2.2 Configure Neusoft NetEye VPN Client

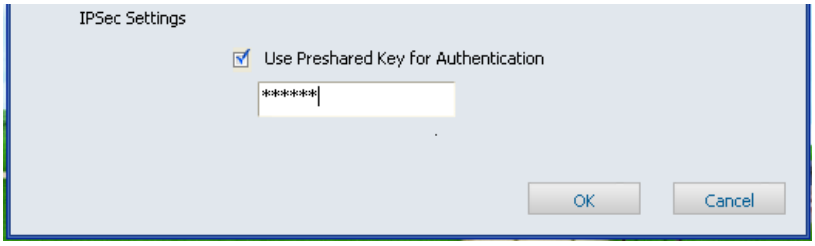
1. Install IPSec VPN client software on Windows operating system.

2. Click **Create** and configure basic information on **Create VPN Connection** page.

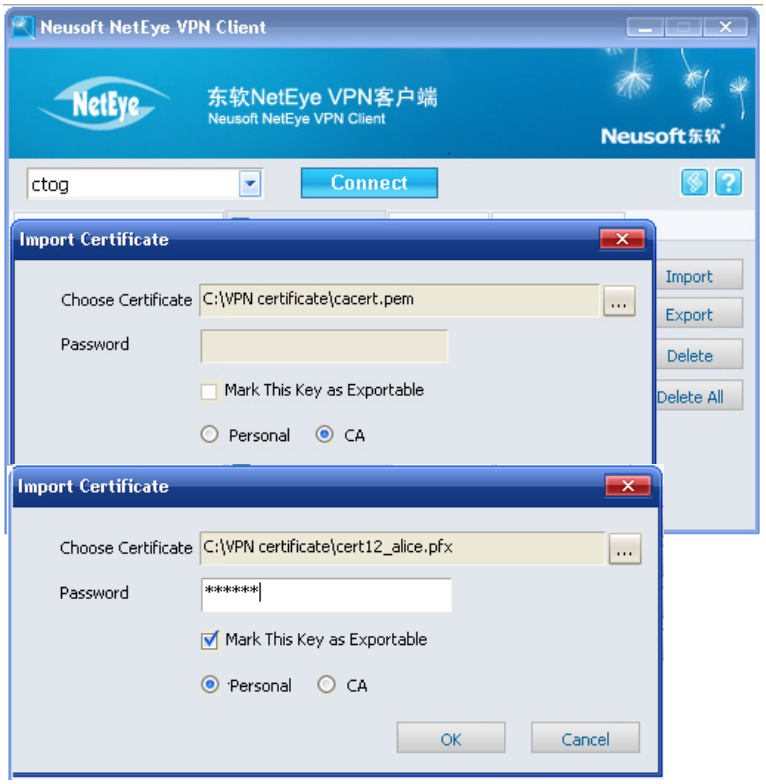
3. Click the Security tab and configure the related information.



- If pre-shared key is used for authentication, check the **Use preshared Key for Authentication** check box.



- If certificate is used for authentication, uncheck the **Use preshared Key for Authentication** check box. Import CA and persoanl certificates as follows:

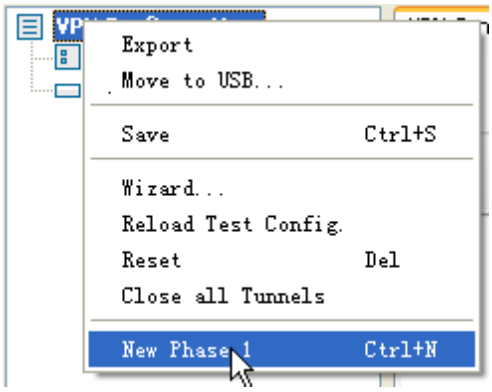


For detailed information about how to install and configure VPN client, see *CELESTIX FGX Integrated Security Software v4.2 VPN Client Users' Guide*.

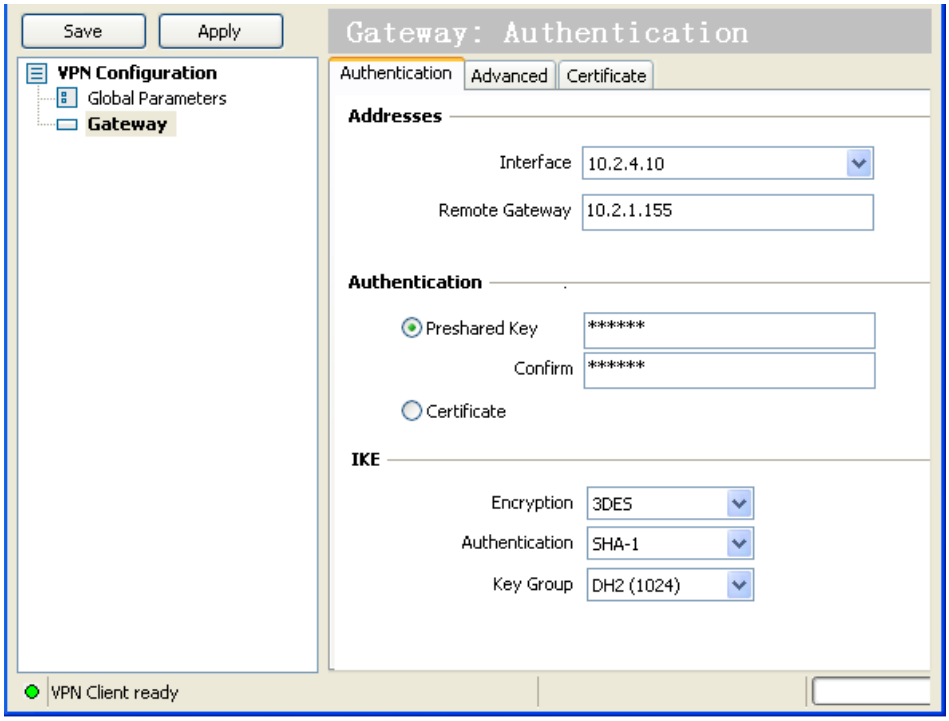
3.2.3 Configure TheGreenBow VPN Client

Xauth users can install and configure TheGreenBow IPSec VPN client software to connect to the IPSec VPN server. Configuration steps include:

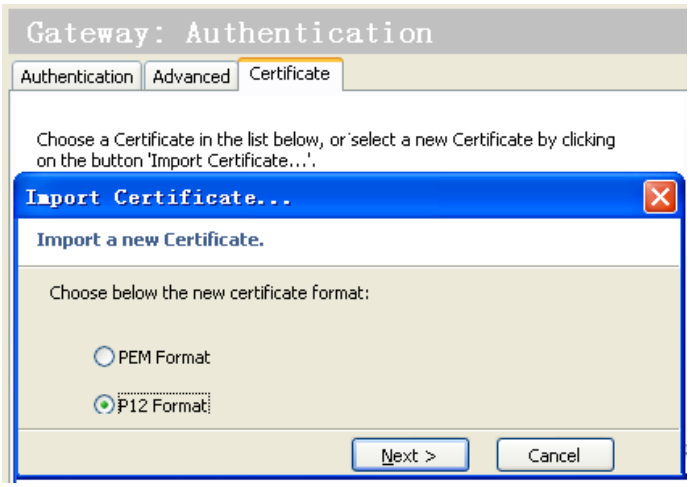
1. Go to **New Phase 1**.



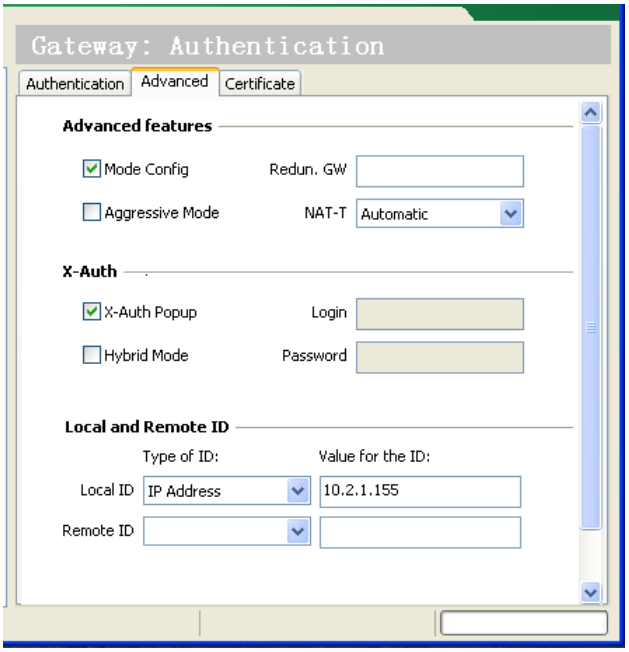
2. Click the **Authentication** tab and configure as follows:



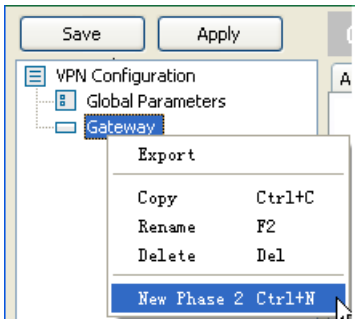
- Click the Certificate radio button to use certificate for authentication. Import CA and local certificates on Certificate page.(Click **P12 Format** to import the local certificate and click **PEM Format** to import CA certificate.)



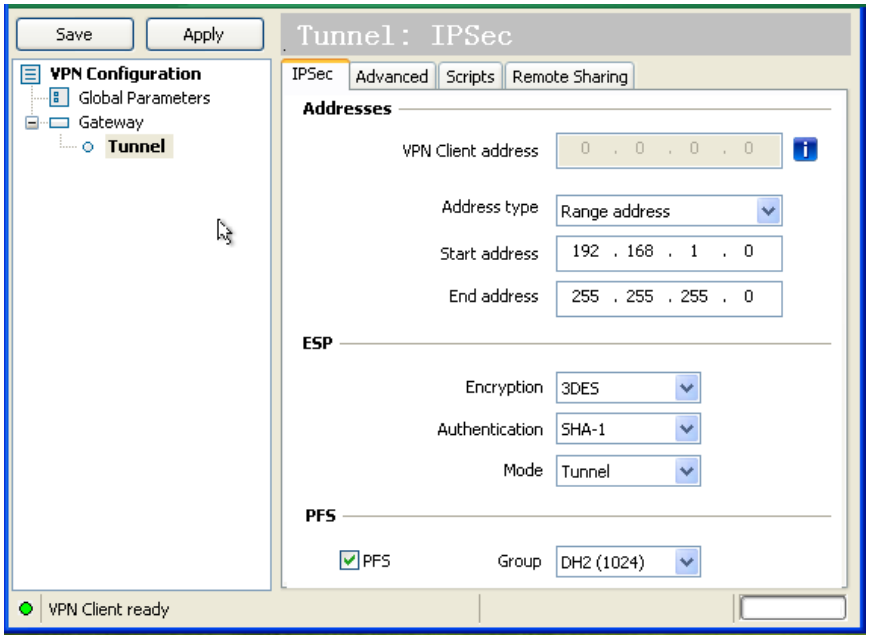
3. Click the **Advanced** tab and configure as follows:



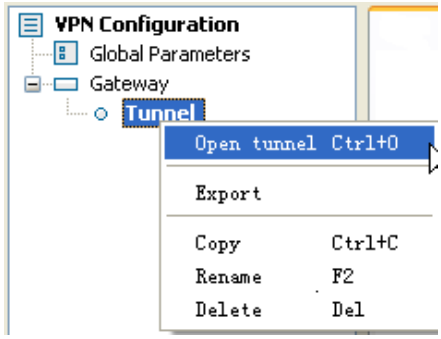
4. Go to **New Phase 2**.



5. Click the IPSec tab and configure as follows:



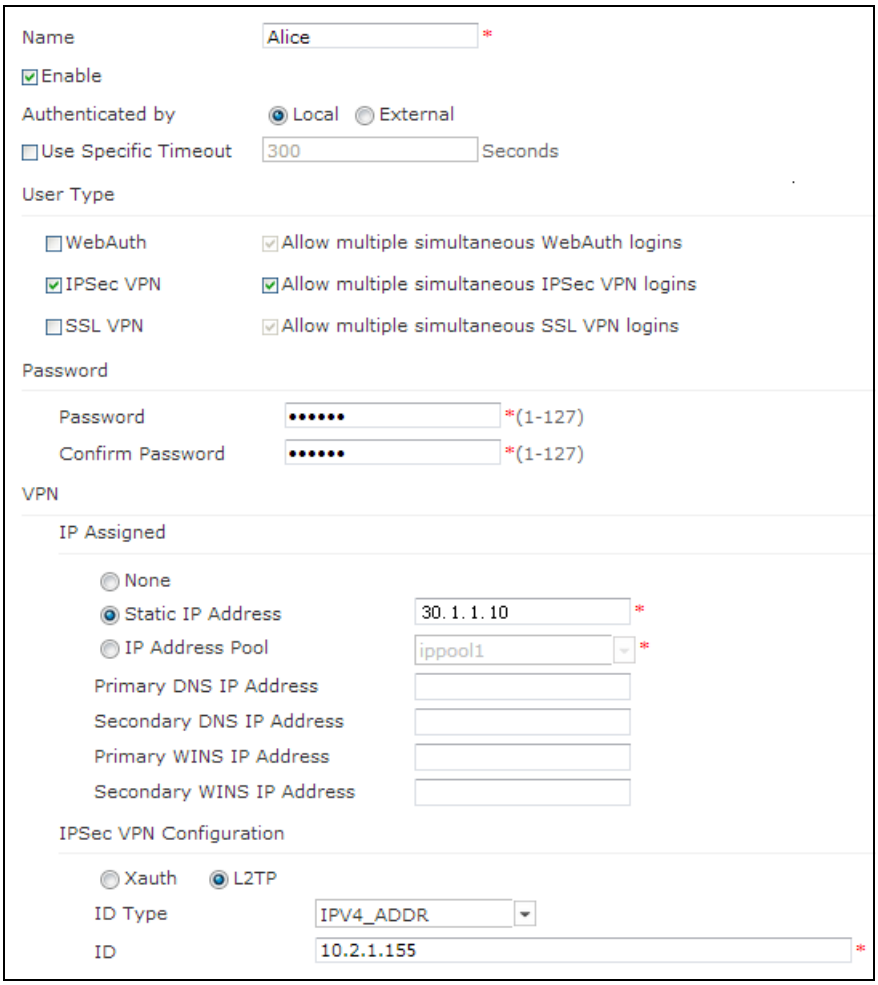
6. Open the tunnel and enter the user name and password on the login page.



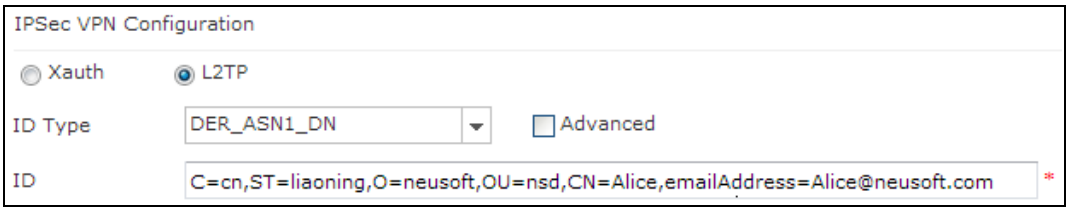
3.3. Create IPSec VPN User

Note: When you assign a static IP address or IP address pool to an IPSec user, you are not recommended to use the IP address of the subnet behind the VPN gateway.

1. Choose **System > Authentication > Users** to open the Users page.
2. Click **New** and configure as follows:



- If certificate authentication is used, the user ID type must be set.



CLI

- Pre-shared key authentication:

```
FGX@root-system] user authuser Alice authtype local password
alice123 enable
FGX@root-system] user authuser Alice ipsecvpn ike-id ipv4-address
10.2.1.155 type l2tp
FGX@root-system] user authuser Alice assigned-ip 30.1.1.10
FGX@root-system] exit
FGX@root> save config
```

- Certificate authentication:

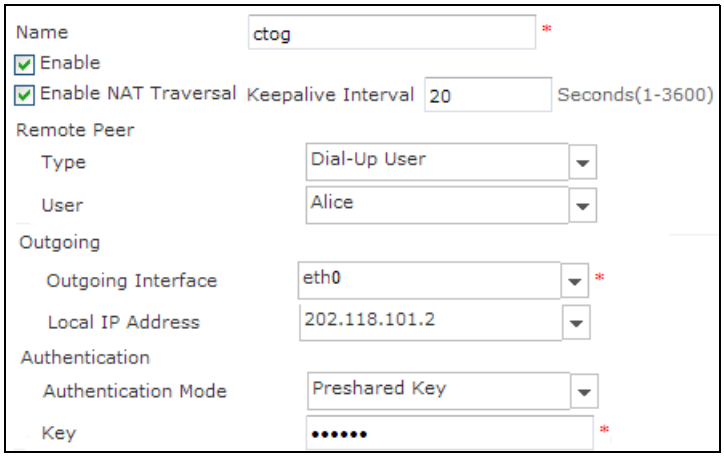
```
FGX@root-system] user authuser Bob ipsecvpn ike-id asn1-dn
C=cn,ST=liaoning,O=neusoft,OU=nsd,CN=Alice,emailAddress=Alice@neuso
ft.com type l2tp
```

3.4. Create Auto IKE Tunnel

- 3.4.1. Create Tunnel Using Pre-Shared Key for Authentication
- 3.4.2. Create Tunnel Using Certificate for Authentication

3.4.1. Create Tunnel Using Pre-Shared Key for Authentication

1. Choose **VPN** > **Auto IKE** to open the **Auto IKE** page.
2. Click **New** and configure as follows:

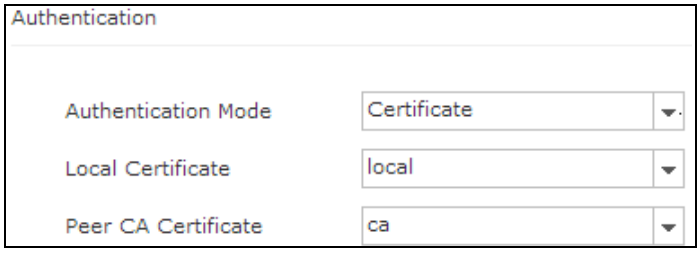


CLI

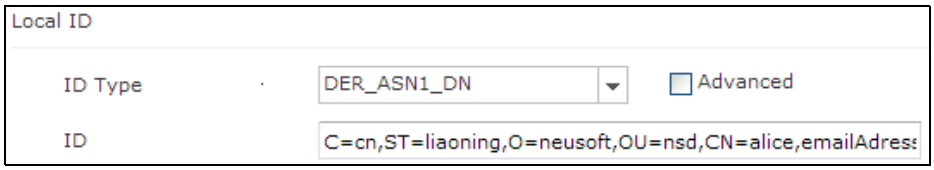
```
FGX@root-system] vpn
FGX@root-system-vpn] tunnel ctog dialup-user user Alice interface
eth0 202.118.101.2 preshared-key test123 enable
FGX@root-system-vpn] exit
FGX@root> save config
```

3.4.2. Create Tunnel Using Certificate for Authentication

1. Choose **VPN** >**IPSec VPN** > **Auto IKE** to go to the Auto IKE page to create a new tunnel. For more information, see 3.4.1. Create Tunnel Using Pre-Shared Key for Authentication. Set the Authentication Mode as Certificate.



2. Click Advanded Settings to set the local ID type.



CLI

```
FGX@root-system] vpn
FGX@root-system-vpn] tunnel ctog dialup-user user Alice interface
eth0 202.118.101.2 certificate local ca enable
FGX@root-system-vpn] tunnel ctog ike local-id asn1-dn
C=cn,ST=liaoning,O=neusoft,OU=nsd,CN=alice,emailAddress=Alice@neuso
ft.com
FGX@root-system-vpn] end
FGX@root> save config
```

3.5. Dialin

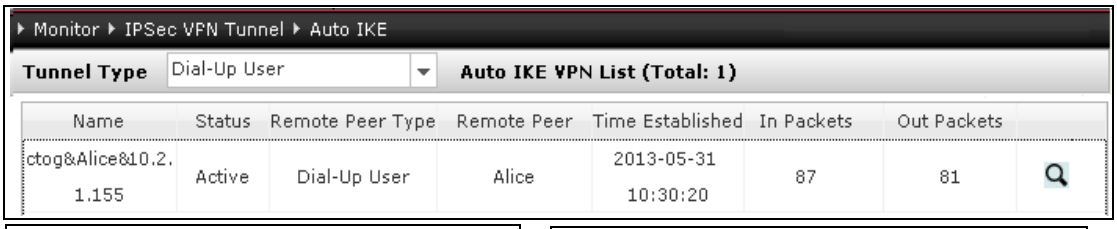
- Dialin on Windows Built-In Client. Enter user name and password, click **Connect** and dial-in.

- Dialin on Neusoft NetEye VPN client. Select the VPN connection and click **Connect**.

- Dialin on TheGreenBow VPN client.

3.6. Monitor Tunnel

Choose **Monitor** > **VPN Tunnel** > **Auto IKE** to view VPN tunnel information.



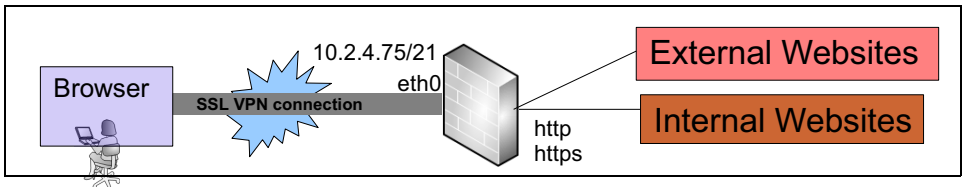
Basic Information	
Name	ctog&Alice&10.2.1.155
Remote Peer Type	Dial-Up User
Remote Peer Information	Alice
Dial-In IP Address	10.2.1.155
Private IP Address	30.1.1.10
Outgoing Interface	eth1
Local IP Address	202.118.101.2
Xauth/L2TP	L2TP
Authentication Method	Preshared Key

Basic Information	
Name	ctog&Alice&10.2.4.10
Remote Peer Type	Dial-Up User
Remote Peer Information	Alice
Dial-In IP Address	10.2.4.10
Private IP Address	30.1.1.2
Outgoing Interface	eth0
Local IP Address	10.2.4.9
Xauth/L2TP	Xauth
Authentication Method	Certificate

Example 4. SSL VPN Portal

Scenario

You want a remote user to use a browser to securely access company internal / external URL's. using SSL.



Configuration Steps:

- 4.1. Configure IP Addresses for Interfaces
- 4.2. Create an IP Address Pool, VPN User, Group
- 4.3. Create SSL VPN Applications, Template
- 4.4. Import CA/Local Certificates
- 4.5. Create SSL VPN Services
- 4.6. Access Applications with SSL VPN

4.1. Configure IP Addresses for Interfaces

1. Choose **Network** > **Interfaces** and configure eth0 and eth1 interfaces:
   - eth0: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 10.2.4.75/21.
   - eth1: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 202.118.101.1/24.
2. Click **OK**.

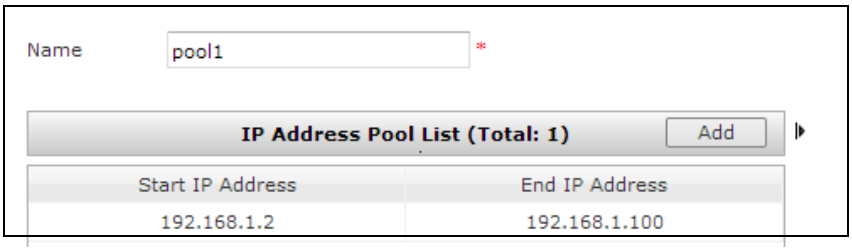
CLI

```
FGX@root> configure mode override
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] working-type layer3-interface
FGX@root-system-if-eth0] ip address 10.2.4.75 255.255.248.0
FGX@root-system-if-eth0] exit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] working-type layer3-interface
FGX@root-system-if-eth1] ip address 202.118.101.1 255.255.255.0
FGX@root-system-if-eth1] end
FGX@root> save config
```

4.2. Create an IP Address Pool, VPN User, Group

4.2.1. IP Address Pool

1. Choose **VPN** > **IP Address Pools** to create an IP address pool.

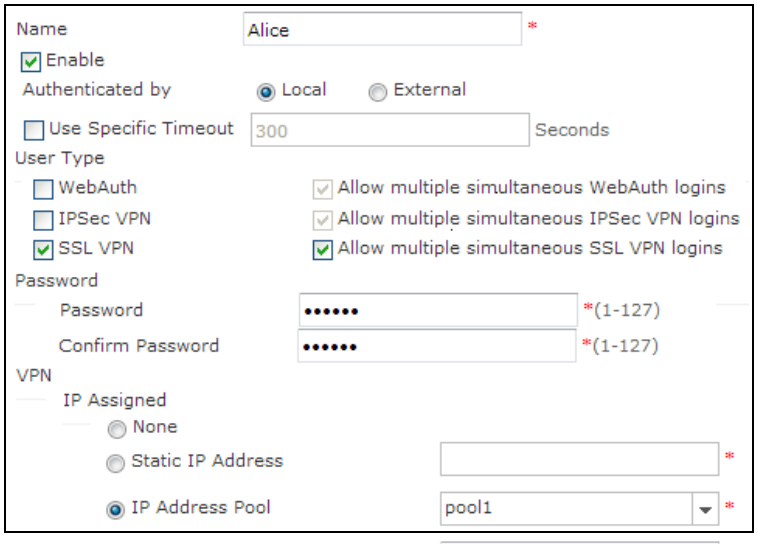


CLI

```
FGX@root-system] ippool pool1 192.168.1.2-192.168.1.100
FGX@root-system] exit
FGX@root> save config
```

4.2.2. SSL VPN User

2. Choose **System** > **Authentication** > **Users** to open the **Users** page.
3. Click **New** and configure as follows:

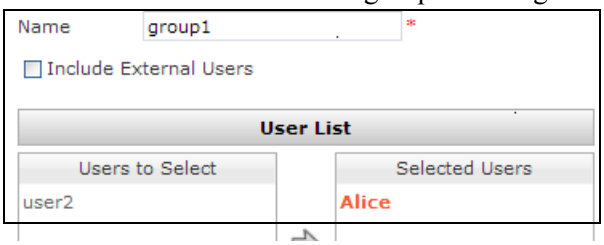


CLI

```
FGX@root-system] user authuser Alice authtype local password abcdef
enable
FGX@root-system] user authuser Alice sslvpn
FGX@root-system] user authuser Alice assigned-ip pool1
FGX@root-system] exit
FGX@root> save config
```

4.2.3. SSL VPN User Group

1. Choose **VPN** > **SSL VPN** > **User Groups** to open the **User Groups** page.
2. Click **New** to create a user group and assign a user:



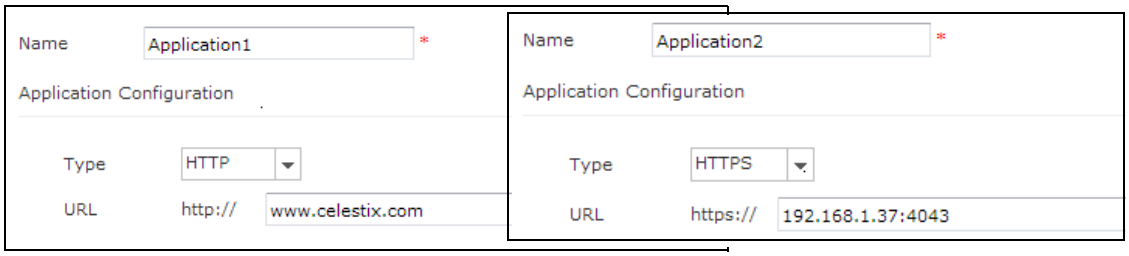
CLI

```
FGX@root-system] sslvpn
FGX@root-system-sslvpn] group group1 user Alice
FGX@root-system-sslvpn] group group1 external no
FGX@root-system-sslvpn] end
FGX@root> save config
```

4.3. Create SSL VPN Applications, Template

4.3.1. Create SSL VPN Applications

1. Choose **VPN** > **SSL VPN** > **SSL VPN Web Portal** > **Applications** to open the **Applications** page.
2. Click **New** and configure as follows:

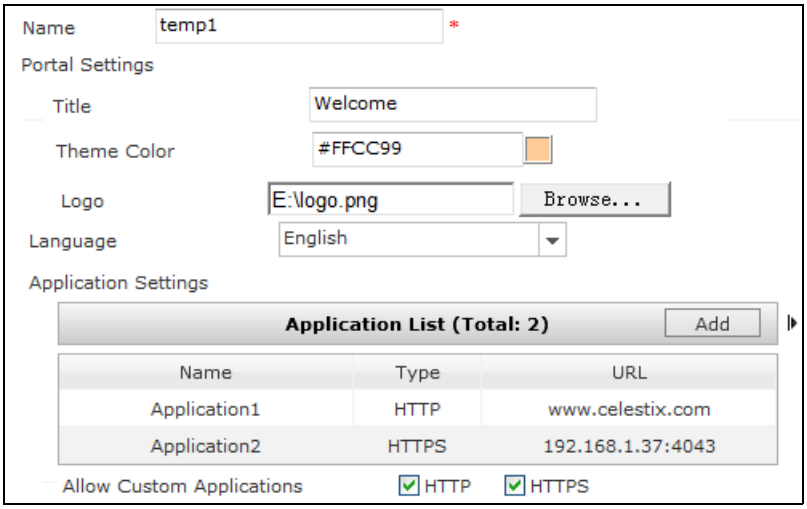


CLI

```
FGX@root-system] sslvpn
FGX@root-system-sslvpn] application Application1 type http url
www.test.com
FGX@root-system-sslvpn] application Application2 type https url
192.168.1.37:4043
FGX@root-system-sslvpn] end
FGX@root> save config
```

4.3.2. Create SSL VPN Portal Template

1. Choose **VPN** > **SSL VPN** > **SSL VPN Web Portal** > **Portal Templates** to open the **Portal Templates** page.
2. Click **New** and configure as follows:

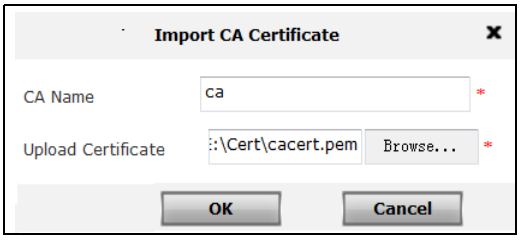


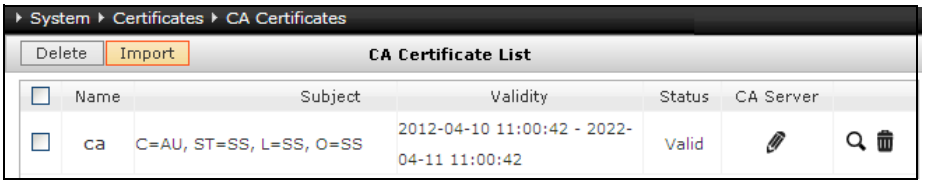
CLI

```
FGX@root-system] sslvpn
FGX@root-system-sslvpn] portal-template temp1
FGX@root-system-sslvpn] portal-template temp1 applist Application1
FGX@root-system-sslvpn] portal-template temp1 applist Application2
FGX@root-system-sslvpn] portal-template temp1 title Welcome
FGX@root-system-sslvpn] portal-template temp1 language English
FGX@root-system-sslvpn] portal-template temp1 themecolor #FFCC99
FGX@root-system-sslvpn] portal-template temp1 customapp HTTP enable
FGX@root-system-sslvpn] portal-template temp1 customapp HTTPS enable
FGX@root-system-sslvpn] end
FGX@root> save config
```

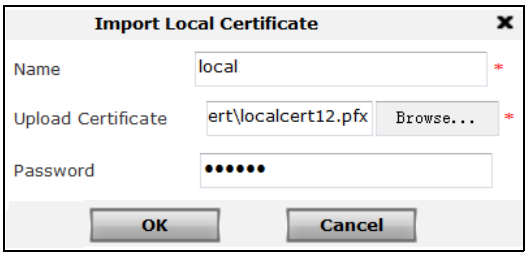
4.4. Import CA/Local Certificates

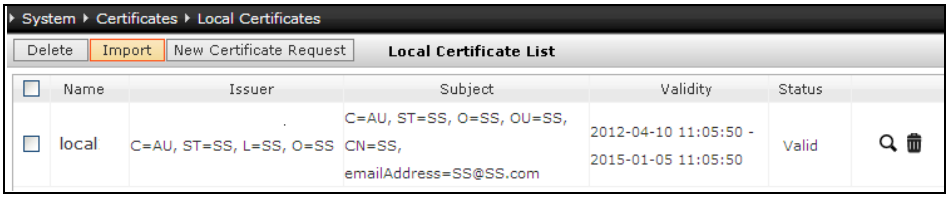
1. **System > Certificates > CA Certificates > Import.**





2. **System > Certificates > Local Certificates > Import.**



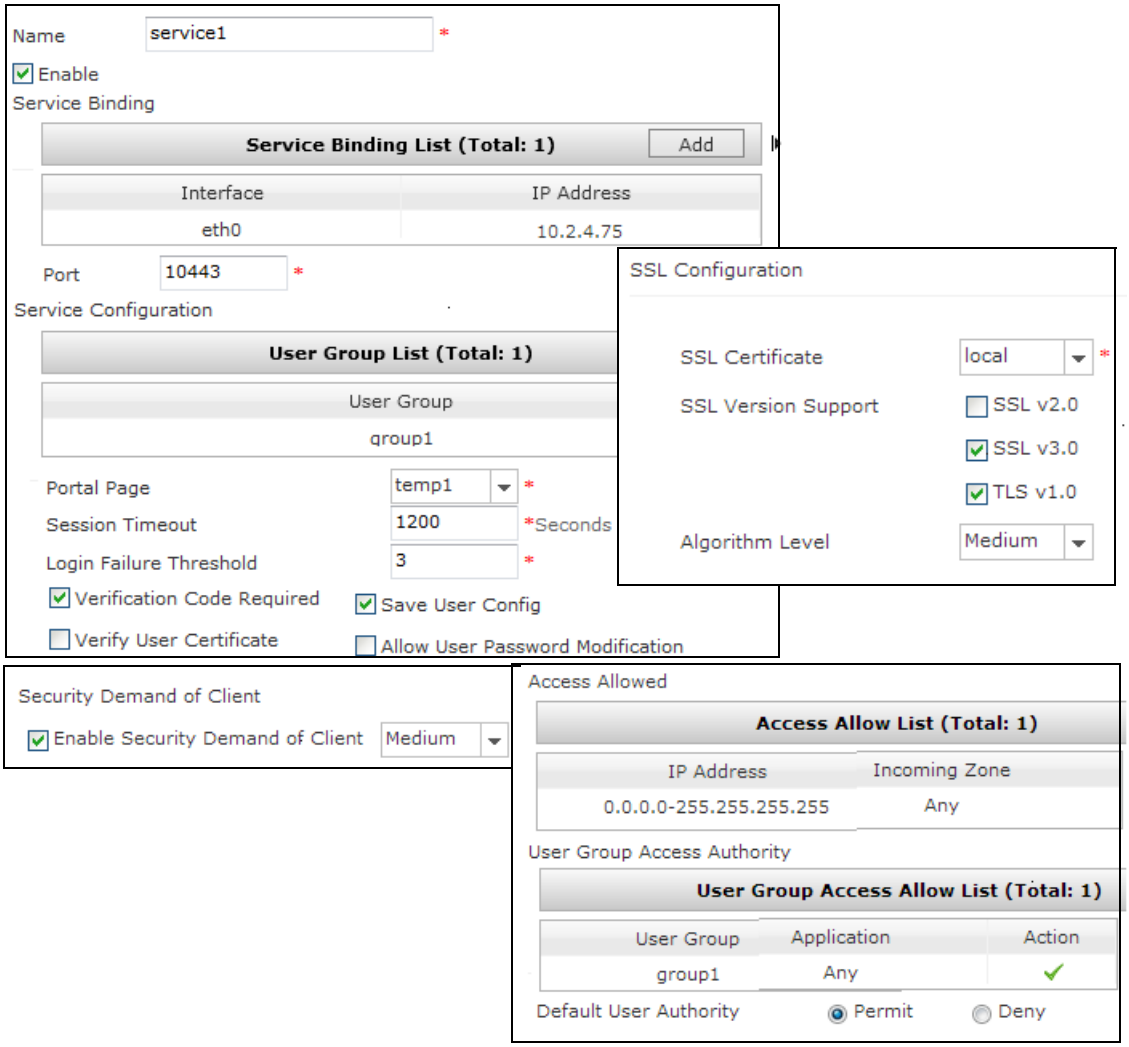


CLI

```
FGX@root-system] import vpn certificate ca from x/zmodem ca
FGX@root-system] import vpn certificate local from x/zmodem local
FGX@root-system] exit
FGX@root> save config
```

4.5. Create SSL VPN Services

1. Choose **VPN** > **SSL VPN** > **SSL VPN Web Portal** > **Portal Services** to open the **Portal Services** page.
2. Click **New** and configure as follows:

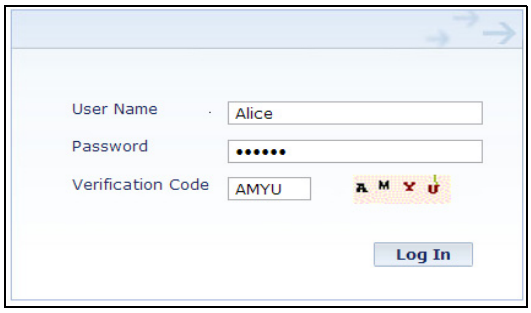


CLI

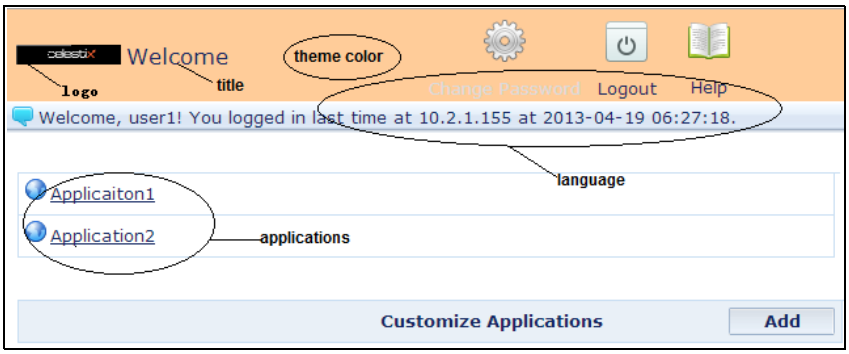
```
FGX@root-system] sslvpn
FGX@root-system-sslvpn] portal-service service1 10.2.4.75 port 10443
portal temp1 certificate local group1
FGX@root-system-sslvpn] portal-service service1 privilege group
group1 application Application1 permit
FGX@root-system-sslvpn] portal-service service1 privilege group
group1 application Application2 permit
FGX@root-system-sslvpn] portal-service service1 privilege default-
group-privilege permit
FGX@root-system-sslvpn] portal-service service1 enable
FGX@root-system-sslvpn] end
FGX@root> save config
```

4.6. Access Applications with SSL VPN

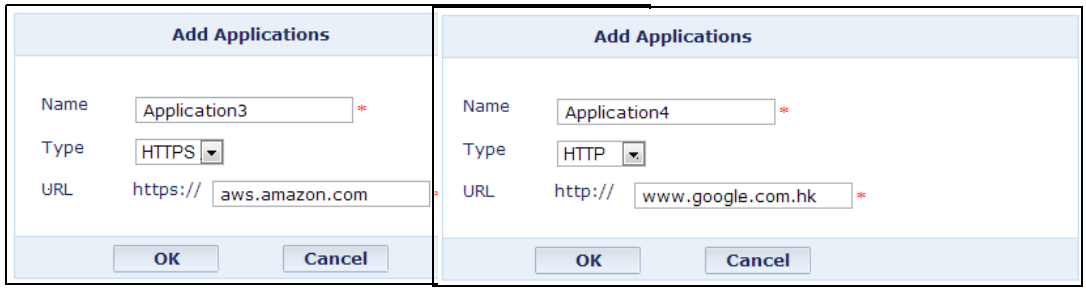
1. Open https://10.2.4.75:10443 with username = Alice, password = test12, and the verification code.



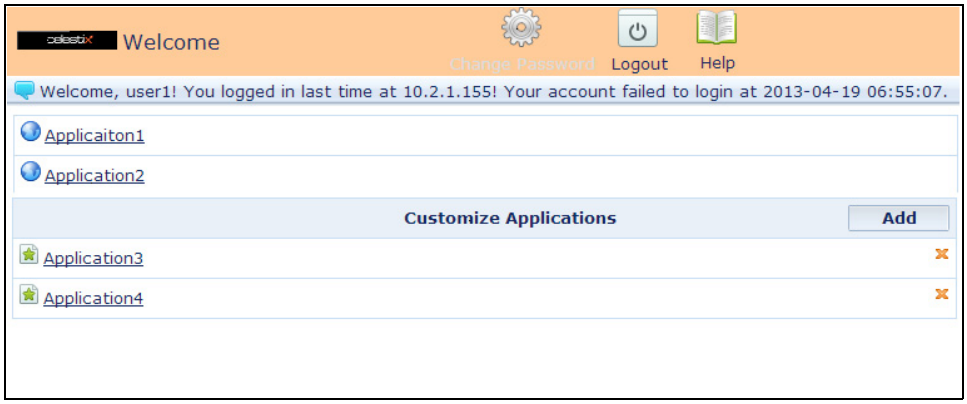
2. Click the application hyperlink to access the website you want.



3. Click **Add** to add a new application.



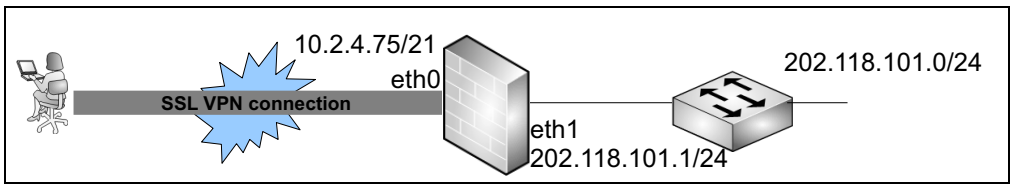
View the application list. You can delete the customized applications.



Example 5. SSL VPN Tunnel

Scenario

You want a remote user to use SSL to access the internal network.



Configuration Steps

- 5.1. Configure IP Addresses for Interfaces
- 5.2. Remote PC: Install Client Software / Add Client Connection
- 5.3. Create IP Address Pool, VPN User, Group
- 5.4. Create an SSL VPN Tunnel
- 5.5. Connect to SSL VPN Server
- 5.6. Monitor

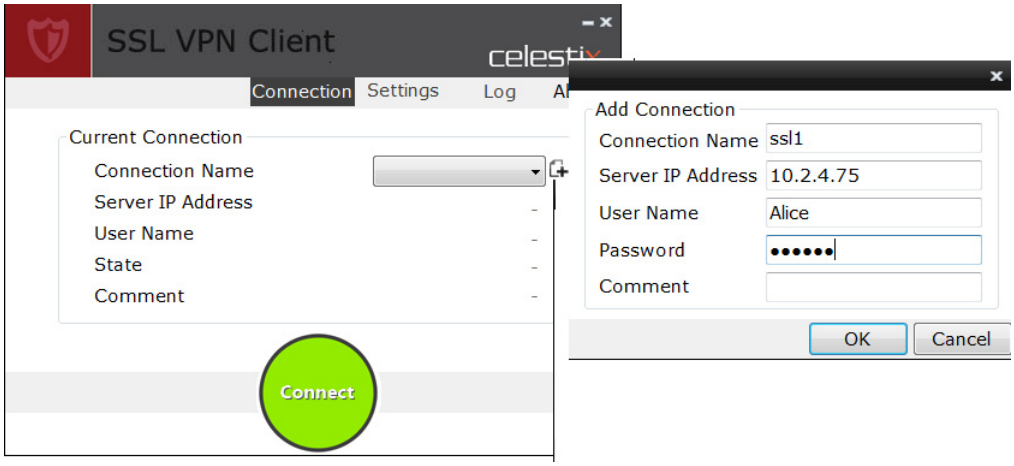
5.1. Configure IP Addresses for Interfaces

This step is the same as 4.1. Configure IP Addresses for Interfaces for SSL VPN Web portal example.

5.2. Remote PC: Install Client Software / Add Client Connection

Install the SSL VPN client on the client comptuer. For more information, see *CELESTIX FGX Integrated Security Software v4.2 SSL VPN Windows Client Users' Guide*.

Add a connection and configure as follows:

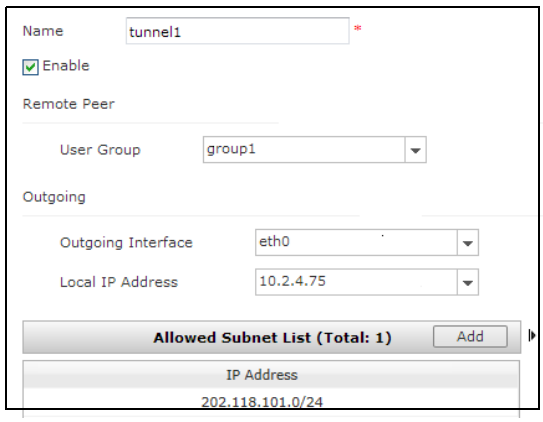


5.3. Create IP Address Pool, VPN User, Group

This step is the same as 4.2. Create an IP Address Pool, VPN User, Group.

5.4. Create an SSL VPN Tunnel

1. Choose **VPN** > **SSL VPN** > **SSL VPN Tunnels** > **Tunnels**. Click **New** and configure as follows:

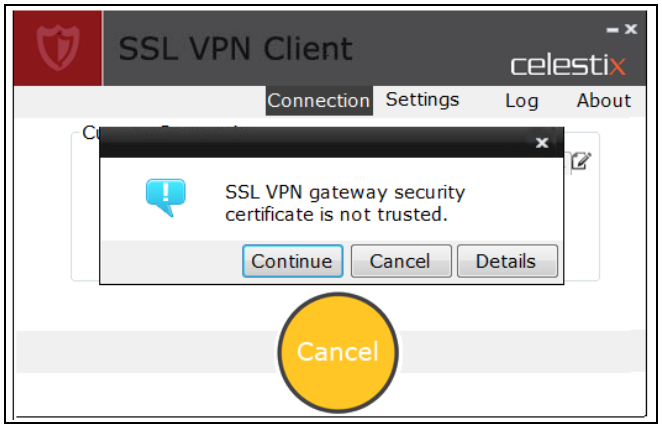


CLI

```
FGX@root-system] sslvpn
FGX@root-system-sslvpn] tunnel tunnel1 interface eth0 10.2.4.75 group
group1 allowed-subnet 202.118.101.0 255.255.255.0 enable
FGX@root-system-sslvpn] end
FGX@root> save config
```

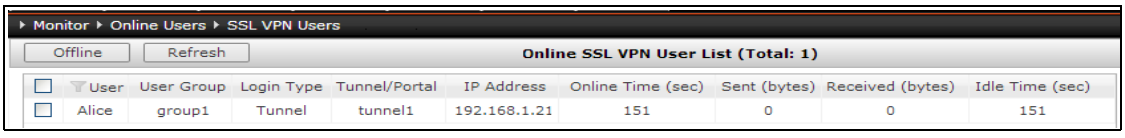
5.5. Connect to SSL VPN Server

Click Connect and Continue, and Alice will connect to the SSL VPN server successfully. .



5.6. Monitor

Choose **Monitor** > **Online Users** > **SSL VPN Users** to view online SSL VPN users.



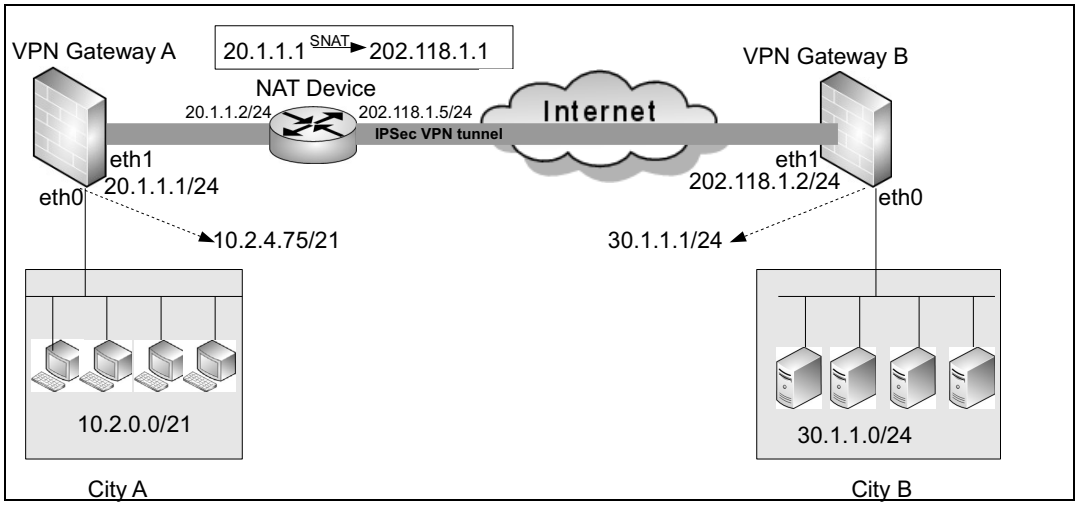
Example 6. SNAT Traversal (IPSec VPN)

Scenario

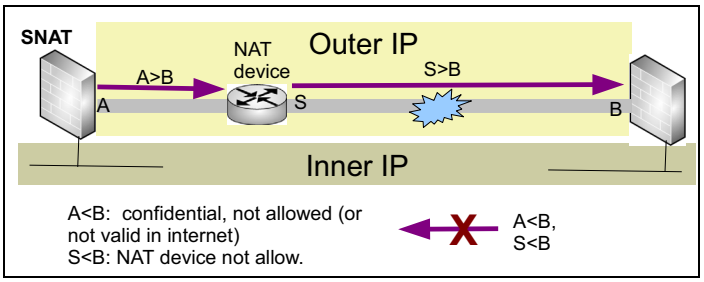
You want to allow VPN connections to be intiated from A, but the gateway A IP address must remain private.

Solution

Install a NAT device between A and the internet. Configure FGX for NAT (SNAT) traversal.



The following diagram shows how SNAT allows the tunnel to be initated from A while keeping A's IP address private.



Configuration Steps

- 6.1. Configure IP Addresses for Interfaces/Default Route
- 6.2. Establish Auto IKE Tunnel (static peer, pre-shared key)
- 6.3. Create Access Policy
- 6.4. Operation

Note: Follow the same steps to configure VPN gateways when DNAT or MIP rules are configured on the NAT device.

6.1. Configure IP Addresses for Interfaces/Default Route

6.1.1. Configure IP Addresses for Interfaces

VPN Gateway A:

1. Choose **Network** > **Interfaces** and configure eth0 and eth1 interfaces:
   - eth0: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 10.2.4.75/21.
   - eth1: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 20.1.1.1/24
2. Click OK.

VPN Gateway B:

1. Choose **Network** > **Interfaces** and configure eth0 and eth1 interfaces:
   - eth0: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List, Primary = 30.1.1.1/24.
   - eth1: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List, Primary = 202.118.1.2/24.
2. Click **OK**.

CLI

VPN Gateway A:

```
FGX@root> configure mode override
FGX@root-system] interface ethernet 0
FGX@root-system-if-eth0] working-type layer3-interface
FGX@root-system-if-eth0] ip address 10.2.4.75 255.255.248.0
FGX@root-system-if-eth0] exit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] working-type layer3-interface
FGX@root-system-if-eth1] ip address 20.1.1.1 255.255.255.0
FGX@root-system-if-eth1] end
FGX@root> save config
```

VPN Gateway B:

Same as VPN Gateway A with the following changes:

```
FGX@root-system-if-eth0] ip address 30.1.1.1 255.255.255.0
FGX@root-system-if-eth1] ip address 202.118.1.2 255.255.255.0
```

6.1.2. Configure Default Route

VPN Gateway A:

1. Choose **Network** > **Routing** > **Default Routing** and create a default route with

   Type = IPv4 Address, Destination IPv4 Address = 0.0.0.0, Mask Length = 0, Metric = 1, Outgoing Interface/ Gateway = Normal, Interface = eth1, Gateway =20.1.1.2.
2. Click **OK**.

VPN Gateway B:

Configure VPN Gateway B in the same way.

Type = IPv4 Address, Destination IPv4 Address = 0.0.0.0, Mask Length = 0, Metric = 1, Outgoing Interface/ Gateway = Normal, Interface = eth1, Gateway =202.118.1.5.

CLI

VPN Gateway A:

```
FGX@root-system] route 0.0.0.0 0.0.0.0 interface eth1 gateway
20.1.1.2
FGX@root-system] exit
FGX@root> save config
```

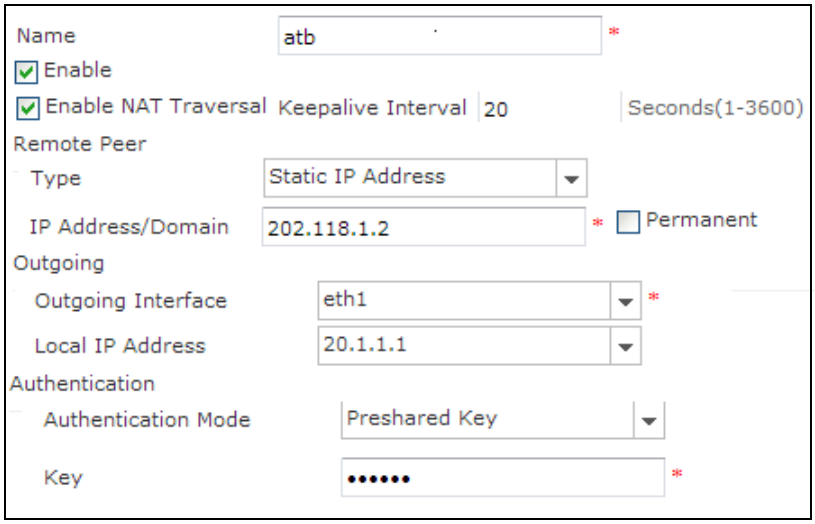
VPN Gateway B:

```
FGX@root-system] route 0.0.0.0 0.0.0.0 interface eth1 gateway
202.118.1.5
FGX@root-system] exit
FGX@root> save config
```

6.2. Establish Auto IKE Tunnel (static peer, pre-shared key)

VPN Gateway A:

1. Choose **VPN** > **IPSec VPN** > **Auto IKE**. Click **New** to create a tunnel.



2. Configure local and remote subnet. Local Subnet=10.2.0.0/21, Remote Subnet=30.1.1.0/24.
3. Click **Advanced Settings** and configure local and peer ID types as follows:

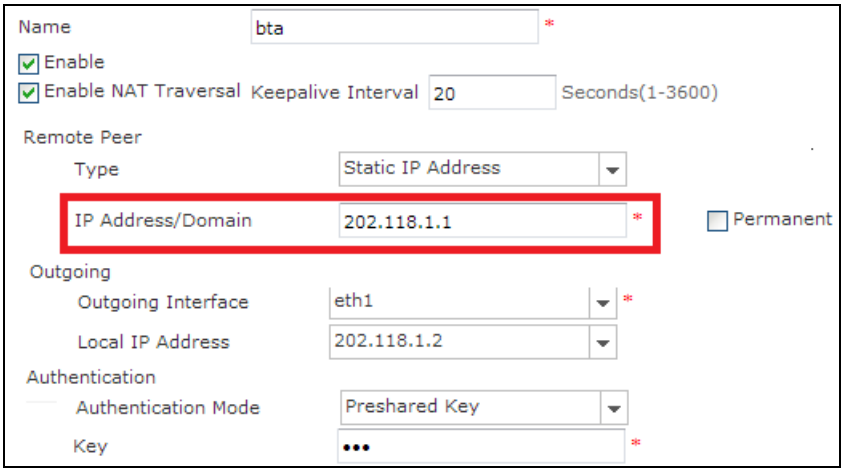
Note: When you set IPV4_ADDR as the ID type, you have to set the SNAT translated IP address as the local key ID. In this example, the key ID is 202.118.1.1.

CLI

```
FGX@root-system] vpn
FGX@root-system-vpn] tunnel atb gateway 202.118.1.2 interface eth1
202.118.1.1 preshared-key 123 local-subnet 10.2.0.0 255.255.248.0
remote-subnet 30.1.1.0 255.255.255.0 enable
FGX@root-system-vpn] tunnel atb ike local-id key-id test
FGX@root-system-vpn] tunnel atb ike peer-id key-id test
FGX@root-system-vpn] end
FGX@root> save config
```

- **Option A**: Set the remote peer type as **Static IP Address** and the IP is the SNAT translated IP address.

1. Choose **VPN** > **IPSec VPN** > **Auto IKE** to create an Auto IKE tunnel.



2. Configure local and remote subnet. Local Subnet=30.1.1.0/24, Remote Subnet=10.2.0.0/21.
3. **Advanced Settings**:
   Local ID type=IKE_ID=test,
   Peer ID type=IKE_ID=test.

CLI

```
FGX@root-system] vpn
FGX@root-system-vpn] tunnel bta gateway 202.118.1.1 interface eth1
202.118.1.2 preshared-key 123 local-subnet 30.1.1.0 255.255.255.0
remote-subnet 10.2.0.0 255.255.248.0 enable
FGX@root-system-vpn] tunnel bta ike local-id key-id test
FGX@root-system-vpn] tunnel bta ike peer-id key-id test
FGX@root-system-vpn] end
FGX@root> save config
```

- **Option B**: Set the remote peer type as **Dynamic**.

Name=bta, Enable=check, Enable NAT Traversal Keepalive Interval=20 Seconds, Remote Peer IP Address/Domain=Dynamic, Outgoing Interface=eth1, Local IP Address=202.118.1.2, Authentication Mode=Preshared Key, Key=test12, Local Subnet=30.1.1.0/24, Remote Subnet=10.2.0.0/21.

CLI

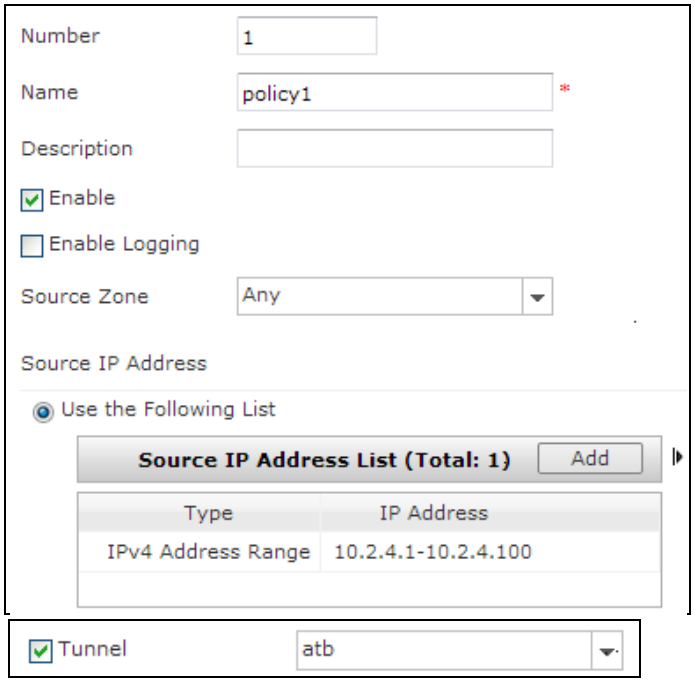
```
FGX@root-system] vpn
FGX@root-system-vpn] tunnel bta gateway any interface eth1 202.118.1.2
preshared-key test12 local-subnet 30.1.1.0 255.255.255.0 remote-
subnet 10.2.0.0 255.255.248.0 enable
FGX@root-system-vpn] end
FGX@root> save config
```

Note: In the case when Dynamic IP address is set, you don't have to set the local and peer IDs for VPN gateway A and B.

6.3. Create Access Policy

VPN Gateway A:

1. Choose **Firewall** > **Access Policies** and create a new access policy as follows:



2. Use the default configurations of other parameters and click **OK**.
3. Click  .

VPN Gateway B:

Choose **Firewall** > **Default Policy Settings** and configure the action of default inter-zone policies as **Permit**.

CLI

VPN Gateway A:

```
FGX@root-system] policy access policy1 any 10.2.4.1-10.2.4.100 any
any any any permit enable 1
FGX@root-system] policy access policy1 tunnel atb
FGX@root-system] exit
FGX@root> save config
```

VPN Gateway B:

```
FGX@root-system] policy default inter-zone access permit
FGX@root-system] exit
FGX@root> save config
```

Note: You can also use a route to direct packets to the VPN tunnel. For more information about using routes in IPSec VPN, see 1.3. Route Tunnel.

6.4. Operation

Choose **Monitor** > **IPSec VPN Tunnel** > **Auto IKE** to monitor the VPN tunnel information.

VPN Gateway A / B:

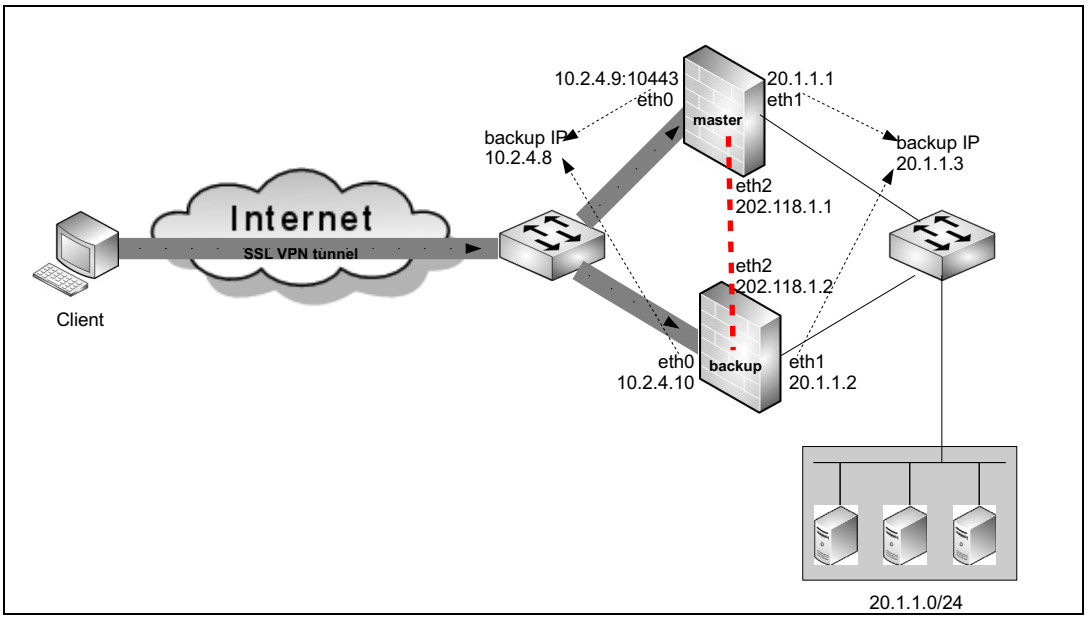
Basic Information	
Name	atb
Remote Peer Type	Static IP Address
Remote Peer Information	202.118.1.2
Dial-In IP Address	202.118.1.2
Outgoing Interface	eth1
Local IP Address	20.1.1.1
Authentication Method	Preshared Key

Basic Information	
Name	bta
Remote Peer Type	Dynamic IP Address
Remote Peer Information	any
Dial-In IP Address	202.118.1.1
Outgoing Interface	eth1
Local IP Address	202.118.1.2
Authentication Method	Preshared Key

Example 7. HA Synchronization（SSL VPN client)

Scenario

You want to have a VPN over a virtual router IP. The following example shows an SSL VPN client VPN over VR's.



Solution

Simply specify the VR backup IP as the FGX VPN server IP.

This example involves the following configurations:

- Configure both master and backup firewalls :
  - 7.1. Configure IP Addresses for Interfaces
  - 7.2. Configure Virtual Router Detection Group
  - 7.3. Configure Virtual Routers
  - 7.4. Configure Cluster
- Configure the master firewall:
  - 7.5. Create IP Address Pool
  - 7.6. Create SSL VPN User
  - 7.7. Create SSL VPN User Group
  - 7.8. Create SSL VPN Tunnel

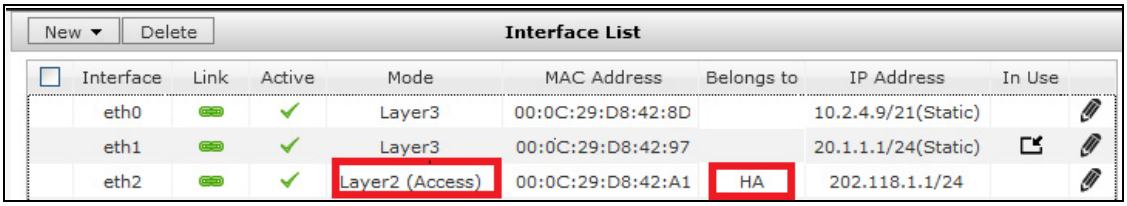
  This configuration information will be synchronized to the backup firewall automatically.
- Configure the client side:
  - 7.9. Install SSL VPN Client
  - 7.10. Create Client Connection
  - 7.11. Connect to SSL VPN Server

7.1. Configure IP Addresses for Interfaces

Master:

1. Choose **Network** > **Interfaces** and edit eth0, eth1, and eth2 interfaces:

- eth0: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 10.2.4.9/21.
- eth1: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 20.1.1.1/24.
- eth2: Active = On, Mode = Layer 2.



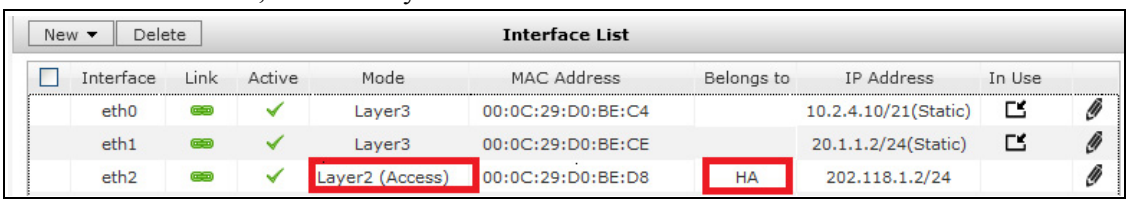
2. Click OK.

Note: The IP address of the Layer 2 interface eth2 can only be set in a cluster. See 7.4. Configure Cluster for more information.

Backup:

1. Choose **Network** > **Interfaces** and edit eth0, eth1, and eth2 interfaces:

- eth0: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 10.2.4.10/21.
- eth1: Active = On, Mode = Layer 3, MTU = 1500, Obtain IP Address = Static IP, IP Address List Primary = 20.1.1.2/24.
- eth2: Active = On, Mode = Layer 2.



2. Click **OK**.

CLI

Master:

```
FGX@root-system] interface ethernet eth0
FGX@root-system-if-eth0] ip address 10.2.4.9 255.255.248.0
FGX@root-system-if-eth0] exit
FGX@root-system] interface ethernet eth1
FGX@root-system-if-eth1] working-type layer3-interface
FGX@root-system-if-eth1] ip address 20.1.1.1 255.255.255.0
FGX@root-system-if-eth1] exit
FGX@root-system] interface ethernet eth2
FGX@root-system-if-eth2] working-type layer2-interface
FGX@root-system-if-eth2] end
FGX@root> save config
```

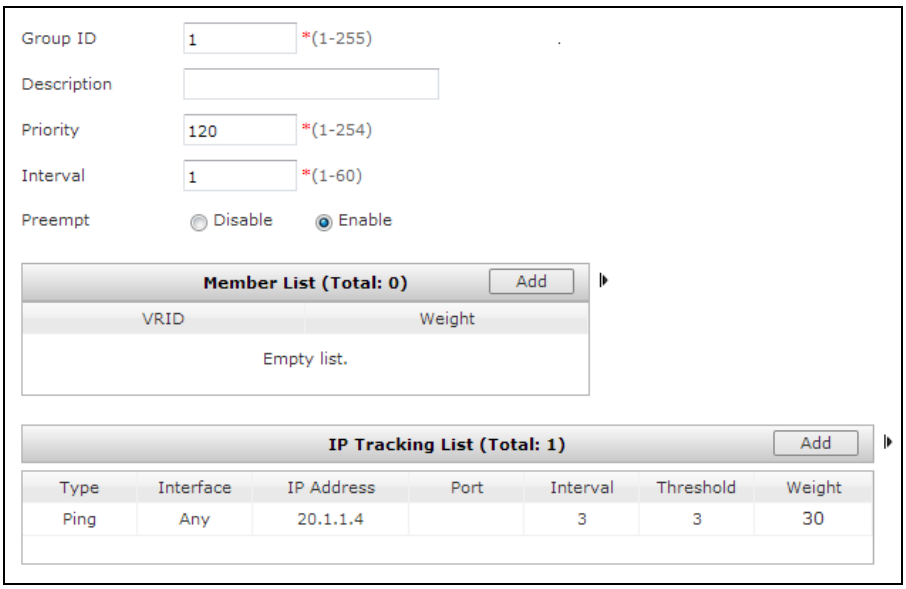
Backup:

```
FGX@root-system] interface ethernet eth0
FGX@root-system-if-eth0] ip address 10.2.4.10 255.255.248.0
FGX@root-system-if-eth0] exit
FGX@root-system] interface ethernet eth1
FGX@root-system-if-eth1] working-type layer3-interface
FGX@root-system-if-eth1] ip address 20.1.1.2 255.255.255.0
FGX@root-system-if-eth1] exit
FGX@root-system] interface ethernet eth2
FGX@root-system-if-eth2] working-type layer2-interface
FGX@root-system-if-eth2] end
FGX@root> save config
```

7.2. Configure Virtual Router Detection Group

Master:

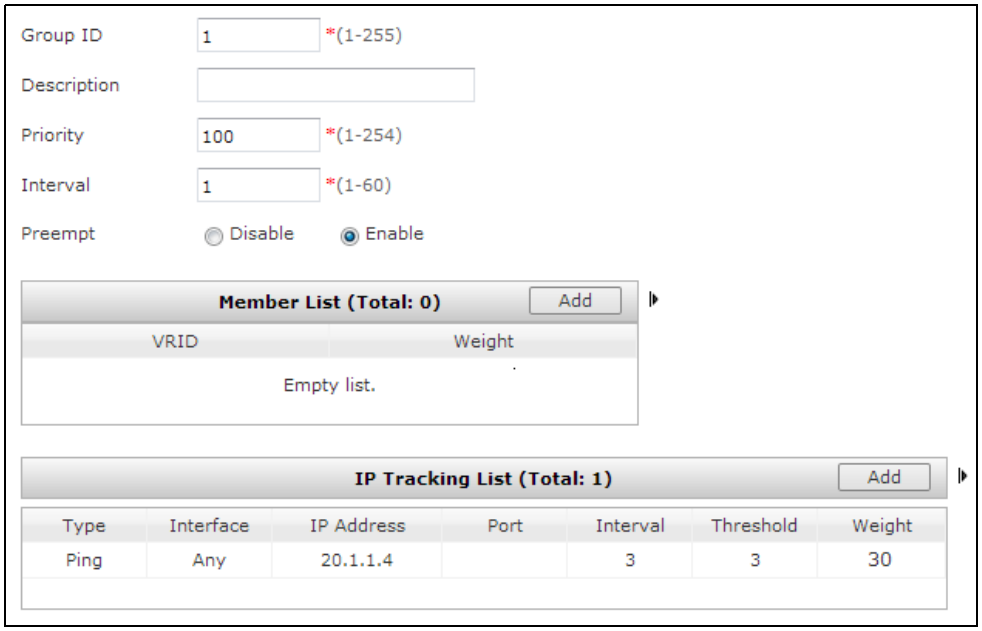
1. Choose **System** > **High Availability** > **Virtual Router Detection Groups** to create new virtual routers.
2. Click **New** and configure as follows:



3. Click **OK**.

Backup:

Configure a virtual router detection group for the backup firewall the same way as the master firewall.



CLI

Master:

```
FGX@root-system] detection group 1
FGX@root-system-dg1] priority 120
FGX@root-system-dg1] interval 1
FGX@root-system-dg1] ip-track type ping interface any ip 20.1.1.4
interval 3 threshold 3 weight 30
FGX@root-system-dg1] end
FGX@root> save config
```

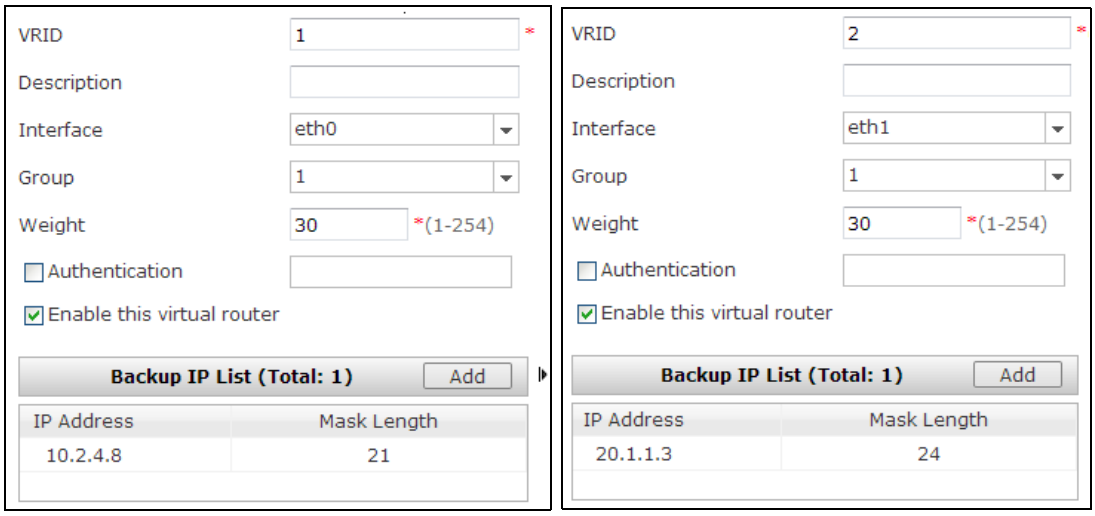
Backup:

```
FGX@root-system] detection group 1
FGX@root-system-dg1] priority 100
FGX@root-system-dg1] interval 1
FGX@root-system-dg1] ip-track type ping interface any ip 20.1.1.4
interval 3 threshold 3 weight 30
FGX@root-system-dg1] end
FGX@root> save config
```

7.3. Configure Virtual Routers

Master:

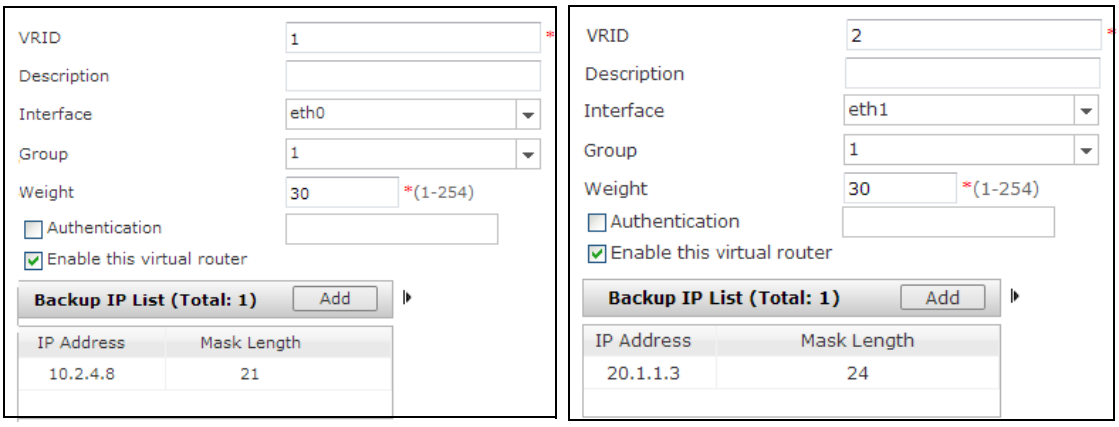
1. Choose **System** > **High Availability** > **Virtual Routers** to create new virtual routers and assign them to the virtual router detection group created in 7.2. Configure Virtual Router Detection Group.
2. Click **New** and configure as follows:



3. Click **OK**.

Backup:

1. Choose **System** > **High Availability** > **Virtual Routers** to create new virtual routers and assign them to the virtual router detection group created in 7.2. Configure Virtual Router Detection Group.
2. Click **New** and configure as follows:



3. Click **OK**.

CLI

Master:

```
FGX@root-system] virtual router 1
FGX@root-system-vr1] election interface eth0
FGX@root-system-vr1] backup ip address 10.2.4.8 mask 255.255.248.0
FGX@root-system-vr1] virtual-router enable
FGX@root-system-vr1] exit
FGX@root-system] virtual router 2
FGX@root-system-vr2] election interface eth1
FGX@root-system-vr2] backup ip address 20.1.1.3 mask 255.255.255.0
FGX@root-system-vr2] virtual-router enable
FGX@root-system-vr2] exit
FGX@root-system] detection group 1
FGX@root-system-dg1] hold virtual-router 1 weight 30
FGX@root-system-dg1] hold virtual-router 2 weight 30
FGX@root-system-dg1] end
FGX@root> save config
```

Backup:

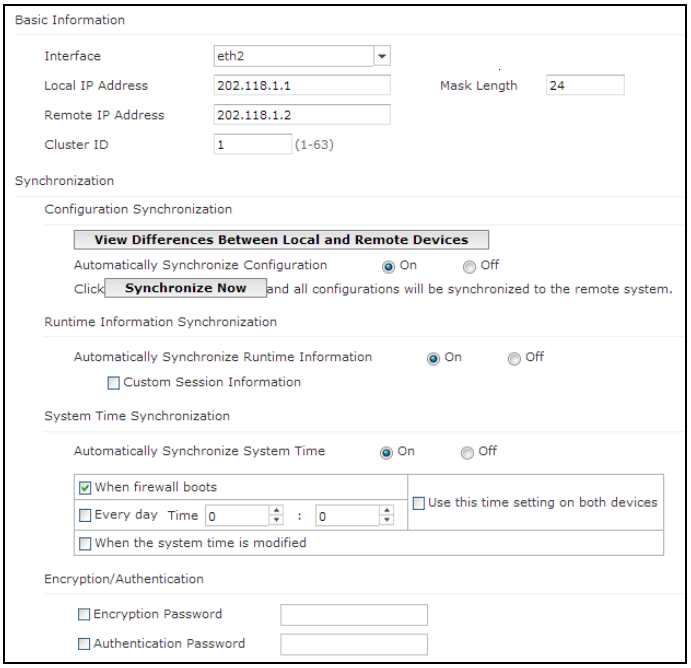
Configure the backup firewall in the same way as the master firewall.

7.4. Configure Cluster

After a cluster with auto synchronization enabled is configured on both firewalls, their configuration information and runtime information will be synchronized to each other automatically.

Choose **System** > **High Availability** > **Clusters** to create a cluster.

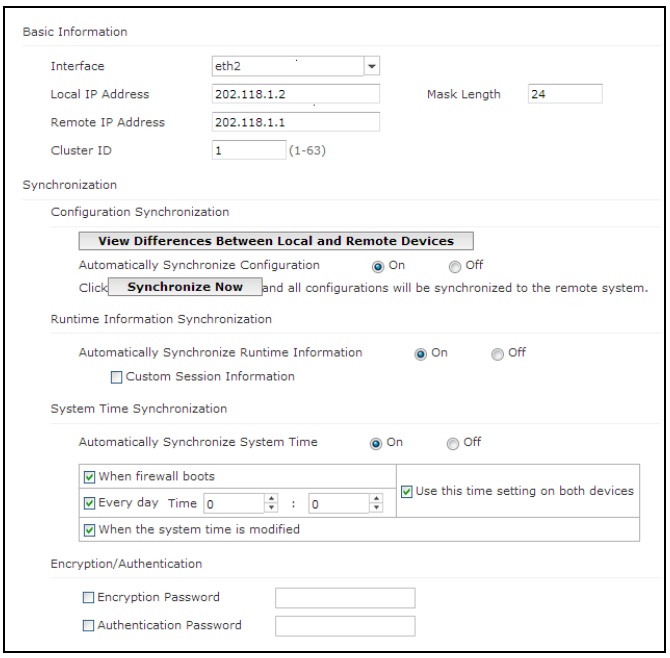
Master:



CLI

```
FGX@root-system] cluster
FGX@root-system-cluster] clusterid 1
FGX@root-system-cluster] local interface eth2
FGX@root-system-cluster] local ip address 202.118.1.1 mask
255.255.255.0
FGX@root-system-cluster] peer ip address 202.118.101.2
FGX@root-system-cluster] rti sync enable
FGX@root-system-cluster] time syn enable
FGX@root-system-cluster] time boot on
FGX@root-system-cluster] config sync auto enable
FGX@root-system-cluster] end
FGX@root> save config
```

Backup:

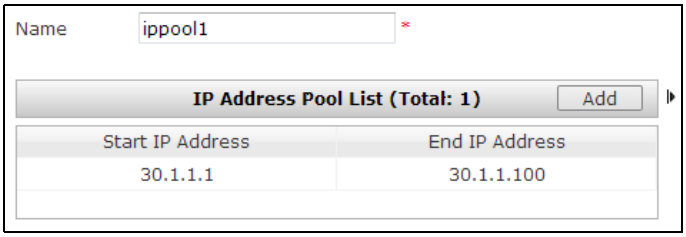


CLI

```
FGX@root-system] cluster
FGX@root-system-cluster] clusterid 1
FGX@root-system-cluster] local interface eth2
FGX@root-system-cluster] local ip address 202.118.1.2 mask
255.255.255.0
FGX@root-system-cluster] peer ip address 202.118.101.1
FGX@root-system-cluster] rti sync enable
FGX@root-system-cluster] time syn enable
FGX@root-system-cluster] time boot on
FGX@root-system-cluster] config sync auto enable
FGX@root-system] exit
FGX@root> save config
```

7.5. Create IP Address Pool

1. Choose **VPN** > **IP Address Pools** to create an IP address pool.



2. Click **OK**.

CLI

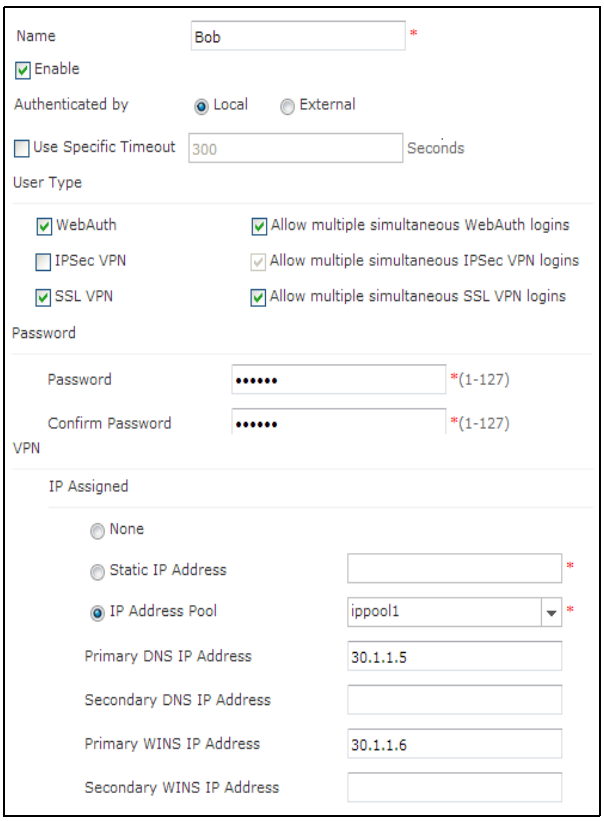
```
FGX@root-system] ippool ippool1 30.1.1.1-30.1.1.100
FGX@root-system] exit
FGX@root> save config
```

Note: When auto synchronization is enabled, IP address pool configurations will be synchronized to the backup firewall automatically.

7.6. Create SSL VPN User

Master:

1. Choose **System** > **Authentication** > **Users** to create an SSL VPN user.
2. Click **New** and configure as follows:



3. Click **OK**.

CLI

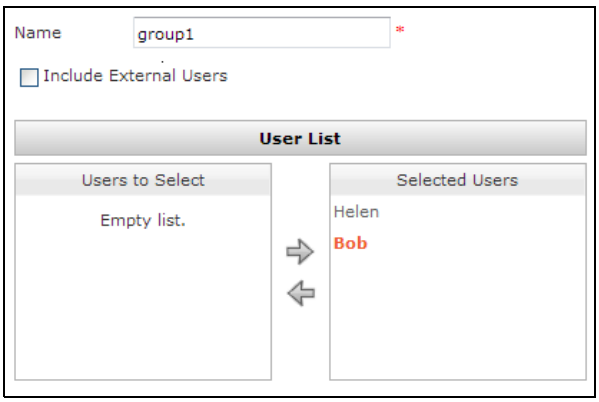
```
FGX@root-system] user authuser Bob authtype local password 123456
enable
FGX@root-system] user authuser Bob sslvpn multipoint enable
FGX@root-system] user authuser Bob assigned-ip ippool1 dns1 30.1.1.5
wins1 30.1.1.6
FGX@root-system] exit
FGX@root> save config
```

Note: When auto synchronization is enabled, SSL VPN user configurations will be synchronized to the backup firewall automatically.

7.7. Create SSL VPN User Group

Master:

1. Choose **VPN** > **SSL VPN** > **User Groups** to create an SSL VPN user group.
2. Click **New** and configure as follows:



3. Click **OK**.

CLI

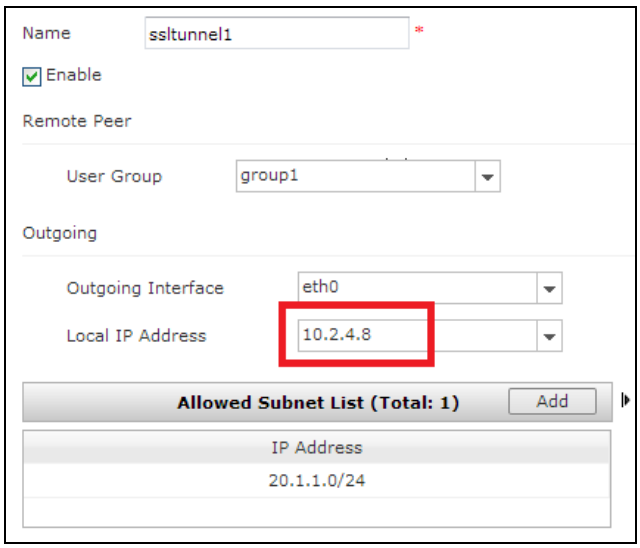
```
FGX@root-system] ssl vpn
FGX@root-system-sslvpn] group group1
FGX@root-system-sslvpn] group group1 user Bob
FGX@root-system-sslvpn] end
FGX@root> save config
```

Note: When auto synchronization is enabled, SSL VPN user group configurations will be synchronized to the backup firewall automatically.

7.8. Create SSL VPN Tunnel

Master:

1. Choose **VPN** > **SSL VPN** > **SSL VPN Tunnels** > **Tunnels** to create an SSL VPN tunnel.
2. Click **New** and configure as follows:



3. Click **OK**.
4. Click .

Note: 1.You can set the local IP Address as **Any**. If the packet belongs to an existing session, the VPN nogotiation IP will be selected according to the session. If not, the VR backup IP will be used to negotiate VPN tunnel.
2. When auto synchronization is enabled, SSL VPN tunnel configurations will be synchronized to the backup firewall automatically.

CLI

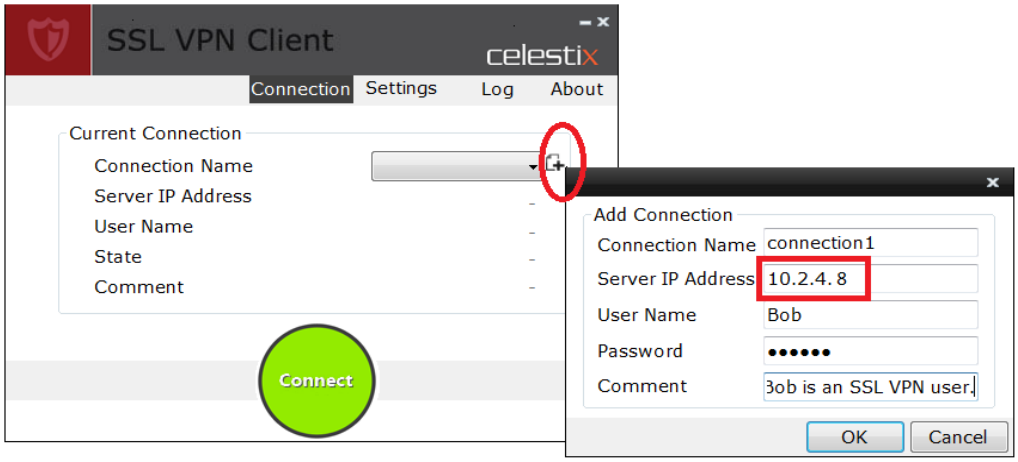
```
FGX@root-system] sslvpn
FGX@root-system-sslvpn] tunnel ssltunnel1 interface eth0 10.2.4.8
enable
FGX@root-system-sslvpn] tunnel ssltunnel1 group group1
FGX@root-system-sslvpn] tunnel ssltunnel1 allowed-subnet 20.1.1.0
FGX@root-system-sslvpn] tunnel ssltunnel1 allowed-subnet 20.1.1.0
255.255.255.0
FGX@root-system-sslvpn] end
FGX@root> save config
```

7.9. Install SSL VPN Client

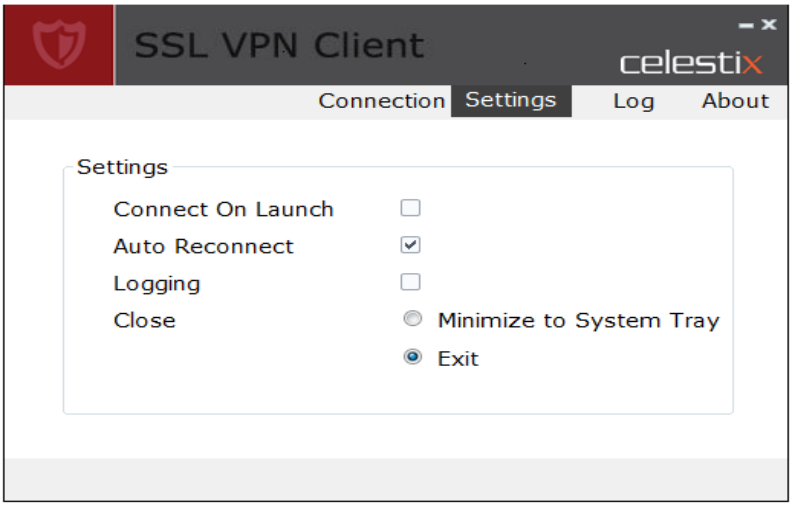
Install the SSL VPN client software on the client computer. For more information, see *CELESTIX FGX Integrated Security Software v4.2 SSL VPN Windows Client Users' Guide* or *CELESTIX FGX Integrated Security Software v4.2 SSL VPN Android Client Users' Guide*.

7.10. Create Client Connection

1. Add a connection and configure as follows:

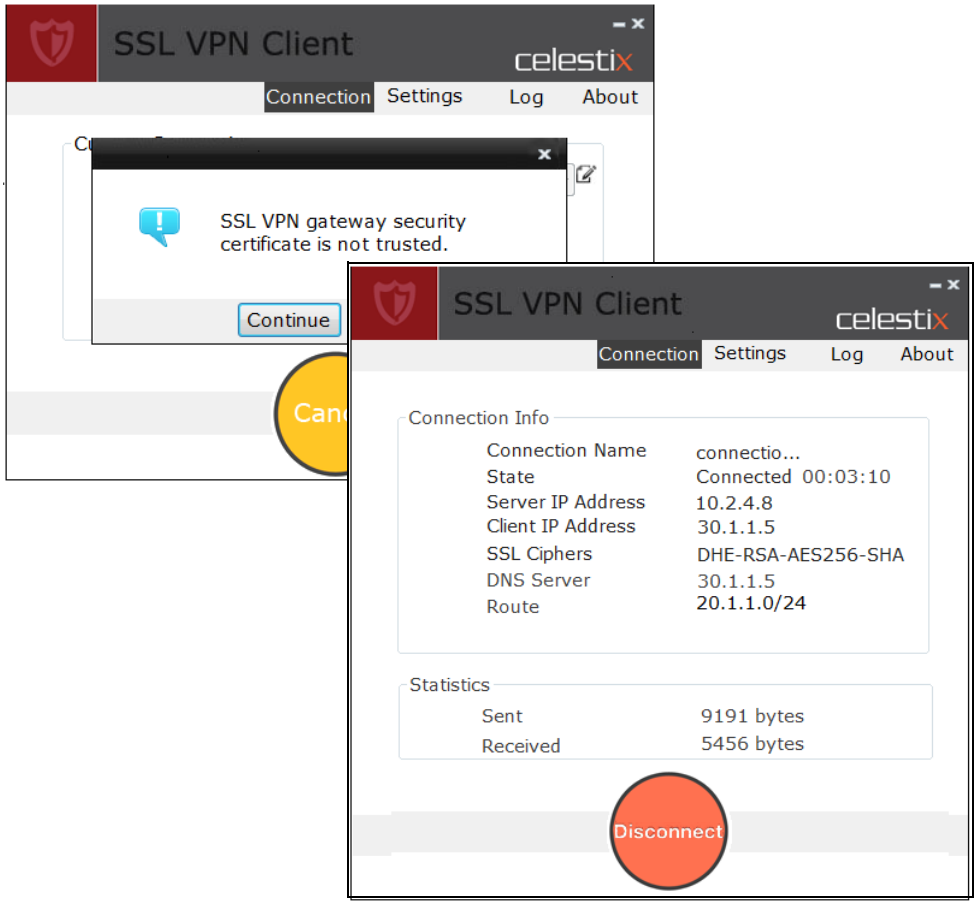


2. Click the **Settings** tab and check the **Auto Reconnect** check box to assure that the SSL VPN connection reconnects immediately when the switchover occurs.



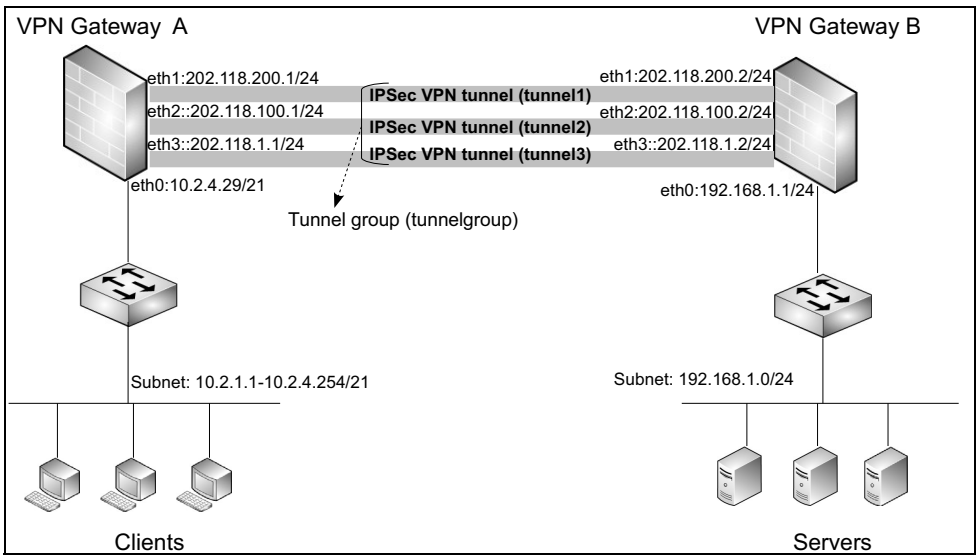
7.11. Connect to SSL VPN Server

Click **Connect** and **Continue**. Bob will connect to the SSL VPN server to access the protected server resources successfully.



Example 8. IPSec VPN Tunnel Group (for auto IKE tunnel only)

In this example, a tunnel group is created to ensure that the communication between VPN gateway A and B will not be interrupted when the working tunnel fails. When the tunnel fails, the available working tunnel with the highest priority will take over all its work.



Configuration steps include:

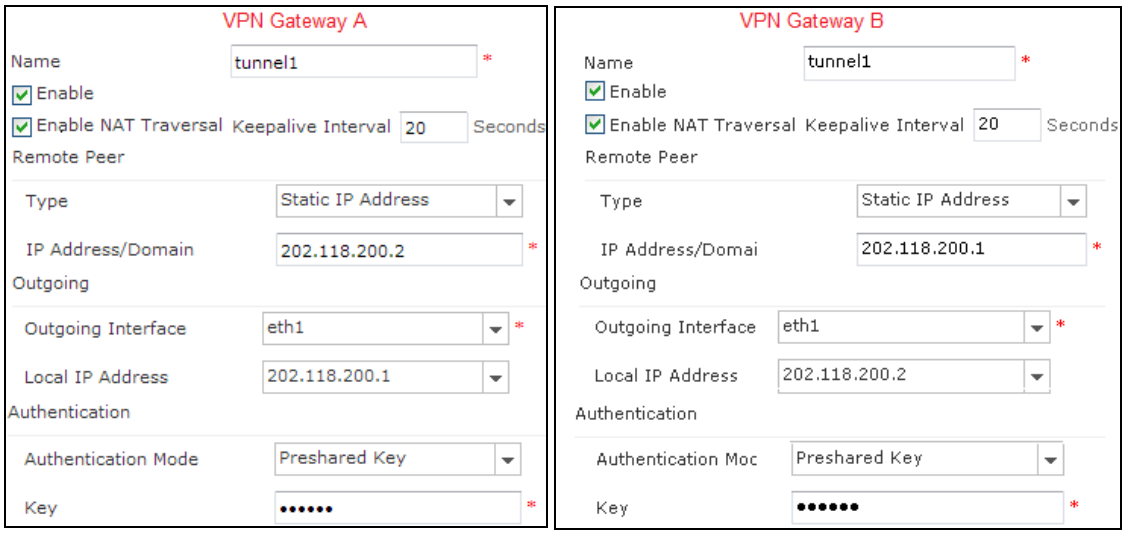
- 8.1. Configure Interface IP Addresses, Default Policy
- 8.2. Create Auto IKE Tunnels
- 8.3. Create Auto IKE Tunnel Group
- 8.4. Create Static Route
- 8.5. Monitor

8.1. Configure Interface IP Addresses, Default Policy

For information about how to configure interface IP addresses and default policy, see 2.1. Configure I/F IP Addresses, Default Route / Access Policy in Example 2.

8.2. Create Auto IKE Tunnels

1. Choose **VPN** > **IPSec VPN** > **Auto IKE** to create a new tunnel.



2. Create tunnel2 and tunnel 3 on both gateways in the same way. The Auto IKE tunnel lists are shown as follows:

VPN Gateway A:

New | Delete | Enable | Disable — **Auto IKE Tunnel List (Total: 3)**

Name	VPN Type	Remote Peer Type	Remote Peer	Outgoing Interface	Local IP Address	Authentication Mode	In Use	Enable
tunnel1	Site to Site	Static IP Address	202.118.200.2	eth1	202.118.200.1	Preshared Key		✓
tunnel2	Site to Site	Static IP Address	202.118.100.2	eth2	202.118.100.1	Preshared Key		✓
tunnel3	Site to Site	Static IP Address	202.118.1.2	eth3	202.118.1.1	Preshared Key		✓

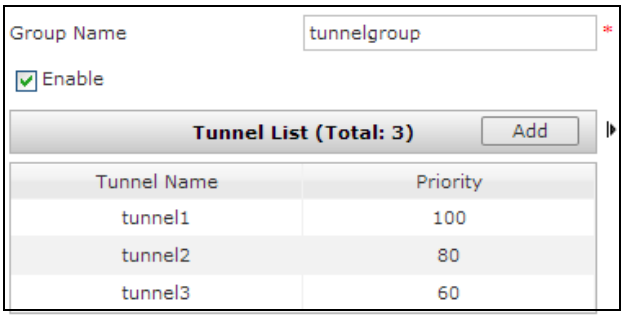
VPN Gateway B:

New | Delete | Enable | Disable — **Auto IKE Tunnel List (Total: 3)**

Name	VPN Type	Remote Peer Type	Remote Peer	Outgoing Interface	Local IP Address	Authentication Mode	In Use	Enable
tunnel1	Site to Site	Static IP Address	202.118.200.1	eth1	202.118.200.2	Preshared Key		✓
tunnel2	Site to Site	Static IP Address	202.118.100.1	eth2	202.118.100.2	Preshared Key		✓
tunnel3	Site to Site	Static IP Address	202.118.1.1	eth3	202.118.1.2	Preshared Key		✓

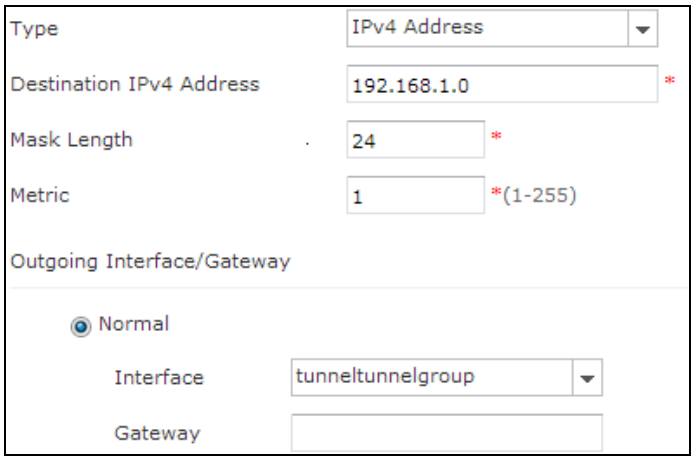
8.3. Create Auto IKE Tunnel Group

Choose **VPN** > **IPSec VPN** > **Tunnel Groups** to create an IPSec tunnel group on each gateway and add VPN tunnel tunnel1, tunnel2, and tunnel3 to the tunnel group.



8.4. Create Static Route

Choose **Network** > **Routing** > **Default Routing** to create a static route using the tunnel group interface as the outgoing interface.



Note: The tunnel group interface is created automatically when the tunnel group is created.

8.5. Monitor

- Choose **Monitor** > **IPSec VPN Tunnel** > **Auto IKE** to view the tunnel information.

VPN Gateway A:

Tunnel Type All — **Auto IKE VPN List (Total: 3)**

Name	Status	Remote Peer Type	Remote Peer	Time Established	In Packets	Out Packets	
tunnel1	Active	Static IP Address	202.118.200.2	2014-02-10 11:14:36	8603	3288	
tunnel2	Active	Static IP Address	202.118.100.2	2014-02-10 11:14:36	0	0	
tunnel3	Active	Static IP Address	202.118.1.2	2014-02-10 11:14:37	0	0	

VPN Gateway B:

Tunnel Type All — **Auto IKE VPN List (Total: 3)**

Name	Status	Remote Peer Type	Remote Peer	Time Established	In Packets	Out Packets	
tunnel1	Active	Static IP Address	202.118.200.1	2014-02-10 00:58:20	3282	8590	
tunnel2	Active	Static IP Address	202.118.100.1	2014-02-10 00:58:21	0	0	
tunnel3	Active	Static IP Address	202.118.1.1	2014-02-10 00:58:22	0	0	

- When tunnel1 fails, FGX will choose tunnel2 to take over all the work according to the priority.

VPN Gateway A:

Tunnel Type All — **Auto IKE VPN List (Total: 2)**

Name	Status	Remote Peer Type	Remote Peer	Time Established	In Packets	Out Packets	
tunnel2	Active	Static IP Address	202.118.100.2	2014-02-10 11:14:36	53	53	
tunnel3	Active	Static IP Address	202.118.1.2	2014-02-10 11:14:37	0	0	

VPN Gateway B:

Tunnel Type All — **Auto IKE VPN List (Total: 2)**

Name	Status	Remote Peer Type	Remote Peer	Time Established	In Packets	Out Packets	
tunnel2	Active	Static IP Address	202.118.100.1	2014-02-10 00:58:21	77	98	
tunnel3	Active	Static IP Address	202.118.1.1	2014-02-10 00:58:22	0	0	

11.4. Parameter Reference

This section explains in detail the parameters involved in IPSec VPN and SSL VPN configurations. It includes:

- 11.4.1. IPSec VPN Parameters
- 11.4.2. SSL VPN Parameters
- 11.4.3. IP Address Pool Parameters

11.4.1. IPSec VPN Parameters

You may use the following parameters in IPSec VPN configurations.

- 11.4.1.1. Parameters of IPSec VPN User Groups
- 11.4.1.2. Parameters of Auto IKE tunnels
- 11.4.1.3. Parameters of Manual Tunnels
- 11.4.1.4. Parameters of IPSec VPN Tunnel Groups
- 11.4.1.5. General Settings

11.4.1.1. Parameters of IPSec VPN User Groups

Table 241 Parameters of IPSec VPN User Groups

Parameter	Description
Group Name	IPSec VPN user group name. 1-63 UTF-8 characters. It cannot contain ? , " ' \ < > & # or spaces.
Included Users	Users that are allocated to a user group on FGX.
Used by Tunnel	A tunnel that uses this user group as the remote peer.
Include External Users	Indicates whether external Xauth user or L2TP users are included in this group. Xauth is short for Extended Authentication, and L2TP is short for Layer 2 Tunneling Protocol.

11.4.1.2. Parameters of Auto IKE tunnels

Table 242 Auto IKE Parameters

Parameters	Description
Name	IPSec VPN tunnel name. 1-63 UTF-8 characters. It cannot contain ? , " ' \ < > & # or spaces. It cannot be the same as any existing manual IPSec VPN tunnel, tunnel group, or SSL VPN tunnel.
Enable	Used to enable or disable a VPN tunnel.
Enable NAT Traversal	If Enable NAT Traversal is selected, the interval of sending NAT keepalive messages should be set. The range is from 1 through 3,600 seconds and the default interval is 20 seconds. It is enabled by default.
Remote Peer Type	The type of remote peer, including • Static IP Address—the IP address or domain name of the remote peer • Dynamic IP Address—the remote peer uses a dynamically assigned IP address for negotiation • Dial-Up User—the remote user name • Dial-Up User Group—the IPSec VPN user group name
Permanent	When Remote Peer Type is Static IP Address, you can set the tunnel to be permanent or not. A permanent tunnel will initiate a negotiation immediately when it is enabled and continues until the negotiation succeeds. On the other hand, a non-permanent tunnel will initiate a negotiation only when there is traffic passing through the tunnel.
Outgoing Interface	The interface of a VPN tunnel, used to negotiate the tunnel.
Local IP Address	The IP address of outgoing interface. Any indicates all IP addresses on the outgoing interface.
Authentication Mode	The authentication mode used for authenticating the remote peer identity in IKE negotiation, including Preshared Key and Certificate.
Key	When the authentication mode is set as Preshared Key, a key is required for authenticating the identity of the two peers of a tunnel. 1-127 UTF-8 characters. It cannot contain ? or spaces.
Local Certificate and CA Certificate	When the authentication mode is set as Certificate, the local certificate and CA certificate of the local peer are sent to the remote peer to check the validity of the local peer. Any in CA Certificate indicates that all CA certificates on FGX device are included.
Local Subnet	The local subnet behind the VPN gateway. It cannot be any of the multicast addresses 224.0.0.0-255.255.255.255, and cannot begin with 0. A maximum of 32 local subnets are supported.
Remote Subnet	The remote subnet behind the VPN gateway. It cannot be any of the multicast addresses 224.0.0.0-255.255.255.255, and cannot begin with 0. A maximum of 32 remote subnets are supported.
Advanced Settings:	
In Phase 1, two peers establish an IKE tunnel.	
Custom Proposals	The proposals include: • g1-3des-md5, g1-3des-sha1, g1-aes128-md5, g1-aes128-sha1 • g2-3des-sha1, g2-3des-md5, g2-aes128-sha1, g2-aes128-md5, g2-aes192-md5, g2-aes192-sha1, g2-aes256-md5, g2-aes256-sha1 • g5-3des-md5, g5-3des-sha1, g5-aes256-md5, g5-aes256-sha1. You can select one to four proposals. The default proposals of phase 1 negotiation are g2-3des-sha1, g2-3des-md5, g2-aes128-sha1, and g2-aes128-md5. Each proposal includes algorithms used during Phase 1. For example, in proposal g1-3des-md5, • g1—indicates DH group 1 is used in key exchange • 3des—indicates the encryption algorithm used • md5—indiciates the Hash function used
Mode	Includes Main and Aggressive. The default is Main mode.
Lifetime	The lifetime of the IPSec SA negotiated in phase1. If the interval exceeds the lifetime, a new IKE SA will be generated. The lifetime ranges from 180 through 2,147,483,647. It is 86,400 seconds by default.
In phase 2, the two peers negotiate IPSec SAs.	

Table 242 Auto IKE Parameters (*continued*)

Parameters	Description
Custom Proposals	The proposals include: • nopfs-esp-3des-md5, nopfs-esp-3des-sha1, nopfs-esp-aes128-md5, nopfs-esp-aes128-sha1 • g1-esp-3des-sha1, g1-esp-aes128-md5 • g5-esp-3des-md5, g5-esp-3des-sha1, g5-esp-aes128-md5, g5-esp-aes128-sha1 • g2-ah-md5, g2-ah-sha1 • g2-esp-aes128-md5, g2-esp-aes128-sha1, g2-esp-3des-md5, g2-esp-3des-sha1, g2-esp-aes192-md5, g2-esp-aes192-sha1, g2-esp-aes256-md5, g2-esp-aes256-sha1 • g2-ah-md5-esp-3des, g2-ah-md5-esp-3des, g2-ah-sha1-esp-3des, g2-ah-md5-esp-aes128, g2-ah-sha1-esp-aes128 The default proposals of phase 2 negotiation are g2-esp-aes128-md5, g2-esp-aes128-sha1, g2-esp-3des-md5, and g2-esp-3des-sha1, indicating that PFS is enabled by default and DH group 2 is used. The four custom proposals must be the same type. If the first custom proposal starts with g2, the other three must start with g2. If the first one starts with nopfs, the other three must start with nopfs. Each proposal indicates algorithms used during Phase 2. For example, in nopfs-esp-3des-md5, • nopfs—perfect forward secrecy is not enabled • esp—indicates the encapsulation protocol used • 3des—indicates the encryption algorithm used • md5—indiciates the Hash function used
Replay Protection	It is enabled by default.
Mode	Indicates tunnel mode used in VPN tunnel, including Transport and Tunnel. The default is Tunnel mode.
Lifetime	The lifetime of the IPSec SA negotiated in phase2. If the interval exceeds the lifetime, a new IKE SA will be generated. The lifetime ranges from 180 through 2,147,483,647 It is 28,800 seconds by default.
DPD	Dead Peer Detection (DPD) is used to detect the state of the remote gateway by sending keepalive messages. • The interval of DPD is from 1 through 3,600 seconds. • The range of Failure Threshold is from 2 through 32,767.
Local ID	The display type for a VPN user, including IPV4_ADDR, FQDN, USER_FQDN, DER_ASN1_DN, and KEY_ID. Different display types require different content in ID or IKE ID test box. • IPV4_ADDR—corresponds to the IP address of the local peer. • FQDN—corresponds to a fully qualified domain name of the local peer. • USER_FQDN—corresponds to an e-mail address of the local peer. • DER_ASN1_DN—unchecked Advanced to fill content in a certain format to indicate the basic information, such as C=country,ST=state,L=city,O=company,OU=department,CN=user, emailAddress=mail. Or check Advanced and fill some more detailed information in the corresponding country name, State or Province Name, Locality (Town) Name, Organization Name, Organizational Unit Name, Common Name, E-mail Address text boxes. The country name is a two-letter code. State or Province Name, Locality (Town) Name, Organization Name, Organizational Unit Name, Common Name should be 1-127 UTF-8 characters. It cannot contain ? , " ' \ < > & or spaces. • KEY_ID—a string corresponds to a key. 1-1023 UTF-8 characters. It cannot contain ? , " ' \ < > & or spaces. DER_ASN1_DN must be selected when using certificate authentication.
Peer ID	The same as the requirements of Local ID
VPN Type	Indicates the remote peer type, including Site to Site and Dialup.
In Use	Indicates that this VPN tunnel is used by a policy.
Enable/Disable	Used to enable or disable existing VPN tunnels.

11.4.1.3. Parameters of Manual Tunnels

Table 243 Parameters of Manual Tunnels

Parameter	Description
Name	IPSec VPN tunnel name. 1-63 UTF-8 characters. It cannot contain ? , " ' \ < > & # or spaces. It cannot be the same as any existing auto IKE tunnel, tunnel group, or SSL VPN tunnel.
Enable	The state of an IPSec VPN tunnel.
Mode	The mode of an IPSec VPN tunnel, including Tunnel and Transport It is Tunnel by default.
Local IP Address	The IP address of the interface used by the local FGX device when establishing an IPSec VPN tunnel. IP address 192.168.255.254, IP address range 127.0.0.0/8, and multicast addresses 224.0.0.0-255.255.255.255 are not supported.
Remote IP Address	The IP address of the interface used by the remote FGX device when establishing an IPSec VPN tunnel. IP address 192.168.255.254, IP address range 127.0.0.0/8, and multicast addresses 224.0.0.0-255.255.255.255 are not supported.
ESP	
Encryption Algorithm	The encryption algorithm used for encrypt IP packet transported in IPSec VPN tunnels, including AES-128, AES-192, AES-256, 3DES, and none. The number indicates the length of the key. The longer the key is, the safer the packets are. Longer key requires more time to be resoluted.
Encryption Key	The key for ESP encryption. Different encryption algorithm requires different length of encryption key. • If the encryption algorithm is AES-128, the key should be a 32-digit hexadecimal number. • If the encryption algorithm is AES-192, the key should be a 48-digit hexadecimal number. • If the encryption algorithm is AES-256, the key should be a 64-digit hexadecimal number. • If the encryption algorithm is 3DES, the key should be a 48-digit hexadecimal number.
Authentication Algorithm	The authentication algorithm used in IPSec VPN tunnels, including HMAC-MD5, HMAC-SHA1, and none.
Authentication Key	The key for ESP authentication. Different encryption algorithm requires different length of authentication key. • If the authentication algorithm is HMAC-MD5, the key should be a 32-digit hexadecimal number. • If the authentication algorithm is HMAC-SHA1, the key should be a 40-digit hexadecimal number.
Local SPI	The SPI of the local peer used to identify SA established. It is required and must be an 8-digit hexadecimal number, ranging from 00000100-2FFFFFFF.
Remote SPI	The SPI of the remote peer. It is required and must be an 8-digit hexadecimal number, ranging from 00000100-2FFFFFFF.
AH	

Table 243 Parameters of Manual Tunnels (*continued*)

Parameter	Description
Authentication Algorithm	The authentication algorithm used for authenticate IP packet transported in IPSec VPN tunnels, including HMAC-MD5 and HMAC-SHA1.
Authentication Key	The key for AH authentication. Different encryption algorithm requires different length of authentication key. • If the authentication algorithm is HMAC-MD5, the key should be a 32-digit hexadecimal number. • If the authentication algorithm is HMAC-SHA1, the key should be a 40-digit hexadecimal number.
Local SPI	The SPI of the local peer used to identify SA established. It is required and must be an 8-digit hexadecimal number, ranging from 00000100-2FFFFFFF.
Remote SPI	The SPI of the remote peer. It is required and must be an 8-digit hexadecimal number, ranging from 00000100-2FFFFFFF.

Note: You must choose either ESP or AH protocols. If ESP is chosen, the encryption algorithm and authentication algorithm for ESP cannot be none simultaneously.

11.4.1.4. Parameters of IPSec VPN Tunnel Groups

Table 244 Parameters of Tunnel Groups

Parameter	Description
Group Name	Tunnel group name. 1-63 UTF-8 characters. It cannot contain ? , " ' \ < > & # or spaces.
Tunnel Name	Site-to-site auto IKE tunnels included in a tunnel group. A maximum of 16 tunnels can be added to a tunnel group.
Priority	The priority of a tunnel in a tunnel group The priority range is 0-255. The greater the value, the higher the priority.
Tunnel State	The state of a tunnel in a tunnel group, including usable and unusable.
In Use	Indicates whether the current tunnel group is being used by other modules as a VPN tunnel, for example, used by an access policy.
Enable	Used to enable or disable a tunnel group.

11.4.1.5. General Settings

You can enable or disable the VPN accelerator card by clicking the Yes and No radio buttons.

11.4.2. SSL VPN Parameters

You may use the following parameters in SSL VPN configuration.

- 11.4.2.1. SSL VPN User Group Parameters

SSL VPN web portal includes the configurations of applications, portal templates, and portal services.

- 11.4.2.2. SSL VPN Web Portal Application Parameters
- 11.4.2.3. SSL VPN Web Portal Template Parameters
- 11.4.2.4. SSL VPN Web Portal Services Parameters.

SSL VPN tunnel configurations include:

- 11.4.2.5. Parameters of SSL VPN Tunnels

11.4.2.1. SSL VPN User Group Parameters

Table 245 Parameters of SSL VPN User Groups

Parameter	Description
Name	SSL VPN user group name. 1-63 UTF-8 characters. It cannot contain ? , " ' \ < > & # or spaces.
Included Users	SSL VPN users included in an SSL VPN user group. An SSL VPN user can only be included by one SSL VPN user group. All SSL VPN users can be assigned to an SSL VPN group. No user is included by default.
Used by Service	SSL VPN services using an SSL VPN user group.
Include External Users	Indicates whether an SSL VPN user group includes external SSL VPN users. External SSL VPN users include users created on FGX whose passwords are saved on an external server and those created on an external server whose user name and password are both saved on the external server. External users are not included by default.

11.4.2.2. SSL VPN Web Portal Application Parameters

Table 246 Parameters of SSL VPN Applications

Parameter	Description
Name	SSL VPN application name. 1-63 UTF-8 characters. Cannot contain ? , " ' \ < > & # or spaces.
Type	SSL VPN application type, including HTTP and HTTPS.
URL	URL address of an SSL VPN application.

Note: SSL VPN applications being used by page templates cannot be deleted.

11.4.2.3. SSL VPN Web Portal Template Parameters

Table 247 Parameters of SSL VPN Portal Templates

Parameter	Description
Name	SSL VPN portal template name. 1-63 UTF-8 characters. Cannot contain ? , " ' \ < > & # or spaces.
Portal Settings	• Title—the title of the Web portal page, displaying on the upper left of the portal page. 1-90 UTF-8 characters and it can be set as blank. • Theme Color—the theme color of the Web portal page, including the login page frame, background, line, etc. Click on the color block to select a color, or enter a color code in the text box to specify a color. The color code ranges from #000000-#FFFFFF. • Logo—the logo image displays in upper left corner of the portal page and above the login text box. The logo file must be a .jpg, .png, .gif, or .bmp file, its dimensions must be 15x80, and its size must be no greater than 150 KB. After a logo is imported, you can view it in the preview area below. A logo file with a length 0 is accepted in which case the logo appears as blank. • Language—the displaying language of the Web portal page, including Simplified Chinese and English.
Application Settings	• Type—the applications type that users can add to the portal page, including HTTP and HTTPS. • Application—the application added to the portal template. • Split Line—a line used to divide two applications on the portal page. A maximum of 32 applications or split lines can be added to an SSL VPN portal template. Applications and dividing lines will be displayed on a portal page according to the order they are shown in the application list box on the portal template. To move an application or dividing line, select the corresponding entry in the list box and click ⬆ or ⬇ to the right of the list box. A maximum of 32 applications or dividing lines can be added to an SSL VPN portal template.
Allow Custom Applications	To set whether to allow users to customize applications.

Note: SSL VPN portal templates being used by SSL VPN services can be edited but cannot be deleted.

11.4.2.4. SSL VPN Web Portal Services Parameters.

Table 248 Parameters of SSL VPN Services

Parameter	Description
Name	SSL VPN application name. 1-63 UTF-8 characters. Cannot contain ? , " ' \ < > & # or spaces.
User Group	The user group that can use this SSL VPN service. All users included in this user group can access the SSL VPN service.
Service Address	The IP address(es) and port(s) through which FGX provides SSL VPN service.
Enable	To enable an SSL VPN service
Service Binding	To set on which IP address and port the SSL VPN service is provided. A Vsys can support up to four SSL VPN services and an SSL VPN service can include four IP address and port pairs at most. • Interface—indicates all Layer 3 interfaces except loopback, tunnel, and virtual interfaces. • IP Address—the IP address of the selected Layer 3 interface. **Any** indicates all IP addresses of the Layer 3 interface. • Port—indicates the port number bound to the Layer 3 interface.
Service Configuration	• User Group List—the user in the group can access this SSL VPN service. • Portal Page—the portal page displayed when you log through SSL VPN. • Session Timeout—If no operation is performed within this timeout, the session will be terminated automatically and the user will log off. The timeout range is 1-60,000. It is 1,200 by default. A timeout of 0 indicates the user will never log off until he closes the browser. • Login Failure Threshold—the maximum number of consecutive failure allowed. After the threshold is reached, the current IP address will be blocked, first for 5 minutes, then for 1 hour, and the third time when the threshold is reached, the IP address will be blocked for 24 hours, after 24 hours the previous login failure statistics will be cleared. The threshold range is 0-10. • Verification Code Required—whether a verification code is required on the portal page when user log through SSL VPN. • Verify User Certificate—During Uni-directional authentication, the certificate from the server will be verified at the client side. During Bi-directional authentication, certificates from both sides will be verified. If the authentication fails, the connection between server and client will be disconnected. Check Verify User Certificate to perform bi-direction authentication which requires the consistency between issuer of the certificate from the client and that of the server. Uncheck to perform uni-directional authentication. • Save User Config—save the user-customized application settings to FGX. This option will be invalid if the current template doesn't support customizing. If you switch Save Users Config from checked to unchecked, all settings saved will be cleared. • Allow User Password Modification—allow users to modify login passwords after logging in on the portal page. If an SSL VPN user is also a WebAuth or VPN user, the password for WebAuth or VPN will be changed. New password should be entered when the user is being authenticated. There will be no effect on the users who have already passed authentication.

Table 248 Parameters of SSL VPN Services (*continued*)

Parameter	Description
SSL Configuration	• SSL Certificate—local certificate saved on the server side. • SSL Version Support—SSL VPN version supported. Different kinds of browsers have different requirements on SSL versions. Connection cannot be established if nothing is selected and users cannot access the SSL VPN servers. • Algorithm Level—SSL encryption algorithm level, including High, Medium, and Low. The higher the level, the more secure it is. **High—**ADH-AES256-SHA, DHE-RSA-AES256-SHA, DHE-DSS-AES256-SHA, AES256-SHA, ADH-AES128-SHA, DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA, AES128-SHA, ADH-DES-CBC3-SHA,EDH-RSA-DES-CBC3-SHA,EDH-DSS-DES-CBC3-SHA,DES-CBC3-SHA, and DES-CBC3-MD5 **Medium—**ADH-RC4-MD5, IDEA-CBC-SHA, RC4-SHA, RC4-MD5, IDEA-CBC-MD5, RC2-CBC-MD5, and RC4-MD5 **Low—**ADH-DES-CBC-SHA, EDH-RSA-DES-CBC-SHA, EDH-DSS-DES-CBC-SHA, DES-CBC-SHA, and DES-CBC-MD5
Security Demand of Client	When you check the Enable Security Demand of Client, you can select a security level or select custom and make detailed configurations: • Browser Version—only browsers of IE7+/Firefox10+/Chrome22+ can display the web portal page. • The Lowest Version of OS—the OS version must be Windows XP/Linux 3.0+. • Anti-Virus Software Installed—anti-virus software is required on the client. This can be specified when the OS on the client is Windows XP. • Windows Firewall Enabled—Windows firewall is required to be enabled on the client. This can be specified when the OS on the client is Windows XP. • Clear Browser Cache when Logout—clear the cache file generated when accessing the current service when the user logs out. • Clear Browser Cookie when Logout—clear the cookie generated when accessing the current service when the user logs out. • Clear Browser History Record when Logout—clear the browser history generated when accessing the current service when the user logs out. • Clear Browser Auto-Form Record when Logout—clear auto-form date saved when accessing the current service when the user logs out. • Clear OS Temporary File when Logout—clear temporary files generated when accessing the current service when the user logs out.
Access Allowed	Define the IP address range that can access this SSL VPN service. A complete IP address range entry is composed of a start IP address (required), end IP address, and an incoming zone. Zone “any” indicates that access from any zone of the specified IP address range is accepted. A maximum of 32 access allow entries can be added in an access allow list.
User Group Access Authority	• User Group—the user group that is set to allow or not allow to access specified applications. • Application—an application included in the SSL VPN portal template which the current SSL VPN service belongs to. • Action—whether this user group is allowed or not allowed to access this application. • Default User Authority—the action to be taken when the combination of user group and application is not in the above User Group Access Authority list. A maximum of 65,535 entries can be added in the User Group Access Authority list.

11.4.2.5. Parameters of SSL VPN Tunnels

Table 249 Parameters of SSL VPN Tunnel

Parameter	Description
Name	SSL VPN tunnel name. 1-63 UTF-8 characters. Cannot contain ? , " ' \ < > & # or spaces. SSL VPN tunnel name cannot be the same as any existing IPSec VPN tunnel or IPSec VPN tunnel group name.
User group	User group that is allowed to access with this SSL VPN tunnel.
Outgoing Interface	The interface of an SSL VPN tunnel
Local IP Address	The IP address of the outgoing interface. Any indicates all IP addresses on the outgoing interfaces are included.
Allowed Subnet	The subnet that can be assessed after an SSL VPN tunnel is established, including IPv4 addresses except multicast addresses 224.0.0.0-255.255.255.255 and IPv6 addresses except FF00/8-FFFF/8. The IPv4 mask length range is 0-32 and the IPv6 IP prefix range is 0-128.
Enable	Enables this tunnel.

11.4.3. IP Address Pool Parameters

An IP address pool is used for assigning IP addresses to VPN users.

Table 250 Parameters of IP Address Pools

Parameter	Description
Name	IP address pool name. 1-63 UTF-8 characters. It cannot contain ? , " ' \ < > & # or spaces.
IP Address Range	An IP address range or a single IP address. It cannot be 192.168.255.254.
In Use	Indicates that this IP address pool is used by IPSec VPN or SSL VPN users.

12 High Availability

FGX provides high availability (HA) using the Virtual Router Redundancy Protocol (VRRP) and the enhanced VRRP election protocol and clusters.

This chapter describes

- 12.1. Overview. Basic HA concepts and fundamentals.
- 12.2. Basic configuration steps. Describes basic configuration steps (WebUI dialogs and CLI commands).
- 12.3. Examples. Provides detailed step-by-step examples.
- 12.4. Parameter reference. Describes in detail all parameters.

12.1. Overview

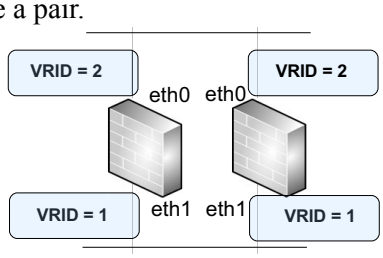
This section describes

- 12.1.1. Standard and enhanced VRRP. FGX supports standard VRRP VR's and provides enhanced VR functionality with VRDG and clusters.
- 12.1.2. Standard VRRP Configuration.
- 12.1.3. Enhanced VRRP (VRDG/Cluster) Configuration. Configuration of VRs, VRDGs, and clusters.
- 12.1.4. Standard VRRP operation
- 12.1.5. Enhanced (VRDG/cluster) operation. VR, VRDG and cluster activity during normal operation. (synchronization, IP tracking and elections).

12.1.1. Standard and enhanced VRRP

Standard

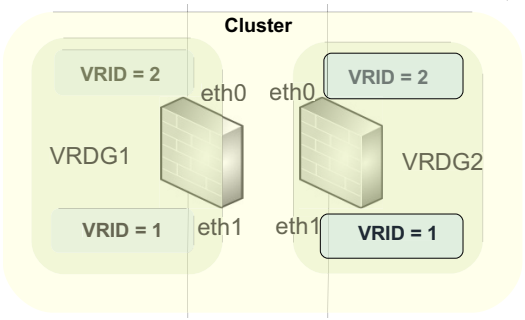
The standard VRRP has **virtual routers** (VR). FGX has virtual router pairs with one VR on each device on the same segment with the same VRID. In the example below the VR's with VRID = 2 are a pair.



Enhanced

The components involved in enhanced VRRP include

- **Virtual router** (VR) pairs.
- **VR detection group** (VRDG). A VRDG contains VRs on different segments on the same device. VRDGs can be created in pairs, one on each cluster device. VRDG's effectively enable switching a group of VR's to a backup while maintaining compatibility with the VRRP protocol.
- **Cluster**. A pair of devices that sync all required data (over a dedicated Ethernet or a channel interface) to ensure seamless VR failover (switch from device1 VR1 to device2 VR1 when device1 fails or device1 VR1 interface fails).



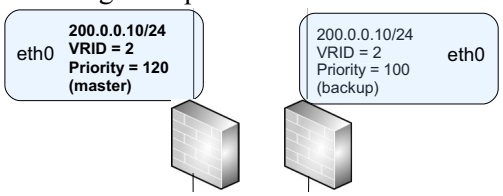
12.1.2. Standard VRRP Configuration

The following describes basic configuration for
- 12.1.2.1 VR
- 12.1.2.2 VR election
- 12.1.2.3 VR IP tracking

For parameter information, see 12.4.1. Virtual Routers.
For configuration steps, see 12.2.1. Basic VRRP.

12.1.2.1 VR

The following example shows virtual routers on a master and backup device.



VR configuration settings include
- **Interface**. Used for master/backup election and data communication. Layer 3 or shared Layer 3 Ethernet interface, Layer 3 or shared Layer 3 channel, or VLAN interface.
- **Backup IP address**. Used as a default gateway address (es). Should be an unused subnet IP address or a set of addresses from different subnets.

Note: If set to the IP address of the device interface (IP address owner), the VR will always have a priority of 255 and failover will not occur even if the interface fails. Do not use IP address owner's address as the backup IP address.

- **VRID**. The master/backup virtual routers on the same segment have the same VRID. The virtual MAC address used by the master virtual router for responding to ARP requests is 00-00-5E-00-01-[VRID].

12.1.2.2 VR election

Election settings include
- **Priority**. Determine the master/backup in VR election. A device with the higher priority becomes the master.
- **Interval**. The interval between advertisements sent by the master.
- **Preempt**. Enable the backup to preempt the master with a lower priority.

For VR election operation, see 12.1.4.2. Election.
For example, see Example 2: Master/backup election.

12.1.2.3 VR IP tracking

VR IP tracking detects how reachable a destination IP address is, making it possible to modify master and backup VR priorities to cause the election of a new master with a better performing interface. IP tracking settings include

1. Type: ARP, ICMP, or TCP.
2. Interface.
3. Tracked IP address.
4. Tracking port (TCP ping only).
5. Interval between tracking messages (secs).
6. Failure threshold (number of tracking messages sent since last response).
7. Weight to delete from VR priority on failure.

For example, see Example 4: IP tracking.

12.1.3. Enhanced VRRP (VRDG/Cluster) Configuration

The following describes basic configuration for

- 12.1.3.1 VR.
- 12.1.3.2 VRDG
- 12.1.3.3 VRDG election
- 12.1.3.4 VRDG IP tracking
- 12.1.3.5 Cluster

For parameter information, see 12.4.2. Virtual Router Detection Groups and 12.4.3. Clusters.
For basic configurations, see 12.2.2. Enhanced (VRDG/Cluster).
For examples, see

- Example 1: Basic enhanced (VRDG/cluster) configuration
- Example 2: Master/backup election
- Example 5: Cluster synchronization.

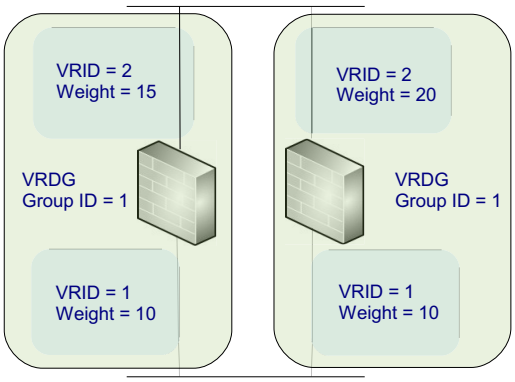
12.1.3.1 VR

Same as for standard configuration, except that VR IP tracking is overwritten by VRDG settings, so do not set.

12.1.3.2 VRDG

A device VRDG has

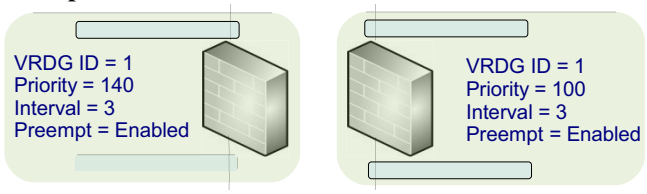
- **Group ID.** Identifies the same VRDG to which VRs belong to.
- **Member VR's** on different segments on the same device. The second VRDG on the other device should have the same VR members as the first one.
- **VR weights.** When a VR is added to a VRDG, the VR has a VR weight (see diagram below). This weight is used to degrade the VRDG priority when the VR fails.



12.1.3.3 VRDG election

It is actually the election of VRs within a VRDG. The following VRDG election settings override VR settings:

- **Priority**. VRDG adjustment of VR priority assures that the master VR's within a VRDG are all on one device.
- **Interval**. The interval at which a VRDG sends advertisements.
- **Preempt**.



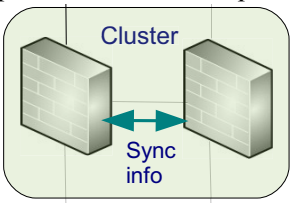
12.1.3.4 VRDG IP tracking

VRDG IP tracking is similar to basic (VR) tracking. This effectively lowers the priority of all VR's in a VRDG (all same value) if any of the IP tracking entries detects a problem.

Note: When a VR joins a VRDG, its IP tracking settings are cleared. VR failure also decreases the VRDG priority by the VR weight.

12.1.3.5 Cluster

A cluster comprises two FGX devices that host the VR's synchronizable system configuration and runtime information. After a VR switchover, the device hosting the new VR master has complete information required to seamlessly continue VR operation.



Recommended to configure two FGX devices in a cluster with the same hardware model and system version.

Cluster configuration includes:

1. **Link**. A dedicated Layer 2 link. Layer 2 Ethernet interface or Layer 2 channel used only for synchronization between two devices. Recommended:
   - Layer 2 Ethernet interfaces for synchronizing configurations
   - Layer 2 channels for synchronizing runtime information (requires extra bandwidth).
   - Directly connect the two HA interfaces (reliable and secure communication).
2. **Encryption**. Encrypt the synchronization packets using DES. Encryption is only recommended when the connection is through an intermediate device (such as a hub or switch). Clustered members should have the same encryption password.
3. **Authentication**. Authenticates packets from the other cluster device. Clustered members should have the same authentication password.

4. **Runtime info sync.** Enable and optionally specify “Custom session information”.
5. **System time sync.** You can specify synchronizing system time at
   1. Bootup
   2. Specified time every day
   3. When system time has been modified manually or through NTP synchronization.

   In (1) and (2), one device is set as the time reference point.
6. **View differences between remote and local devices.** Before performing configuration synchronization, click this button to compare the configuration difference between two clustered devices.
7. **Synchronize now.** Before enabling automatic configuration synchronization, you are recommended to manually synchronize to ensure that the configuration and topology of the two devices are consistent.
8. Perform **manual (complete) synchronization—**synchronizes all configuration data, overwriting existing configurations.
9. Enable **Automatic (modifications) synchronization—**automatically synchronizes device configurations when modifications are made. Original data is not deleted.

12.1.4. Standard VRRP operation

- 12.1.4.1. States
- 12.1.4.2. Election
- 12.1.4.3. IP tracking

12.1.4.1. States

On FGX, there are three states of the routers running VRRP:

- **Initialize**—FGX has not participated in an election
- **Master**—FGX is in the master state after an election and can forward packets
- **Backup**—FGX is in the backup state after an election and can only listen to the VRRP messages sent from the master but does not participate in data forwarding

12.1.4.2. Election

Trigger. An election is triggered when

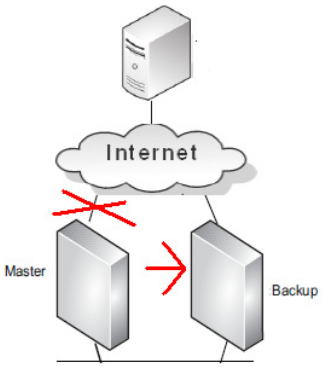
- Device starts.
- VR priority changes.
  - The device with a higher priority is elected as the master.
  - If two devices are of the same priority, the one whose election interface has the higher primary IP address will become the master.
- Failed master recovers from a failure only when 1) preemption is enabled; and 2) initially not of the same priority.

Result. The election result is determined by priority as well as:

- **Preempt mode**.
  - Enabled: If the backup receives a VRRP message from the master showing that the master has a lower priority, the backup will transition to the master after three advertisement intervals plus the skew time.
  - Not enabled: The backup will only transition to the master when the master fails.
- **Interval**. When the backup receives no VRRP messages from the master within three advertisement intervals in a row (or receives a message with a priority of zero), it will consider the master has failed and will transition to the master after a short skew-time delay.

12.1.4.3. IP tracking

The following is an example of IP tracking.



IP tracking monitors the route to the destination host. If the master is detected that its track failures have reached a specified threshold, the master will lower its priority by the track weight, possibly triggering a new election. New election trigger requires (1) preempt mode and (2) the weight should be bigger than the difference in priorities between the VRs.

Failure track continues on the original master, which restores the original priority and transitions back to the master upon recovering from failure, it.

For example, see Example 4: IP tracking.

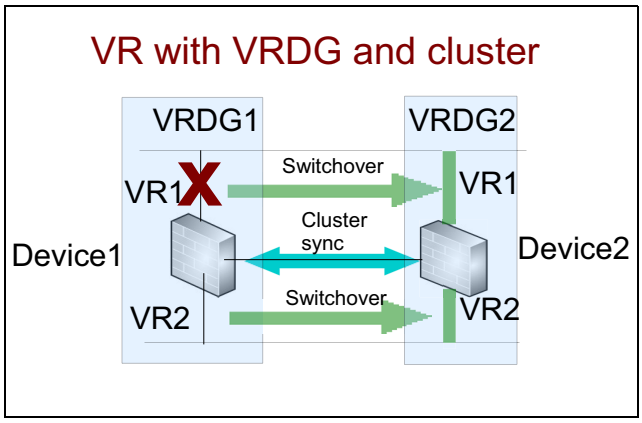
12.1.5. Enhanced (VRDG/cluster) operation

- 12.1.5.1. VRDG/cluster operation
- 12.1.5.2. Cluster sync info

12.1.5.1. VRDG/cluster operation

A FGX VRDG contains virtual routers of different segments on the same device, ensuring that master virtual routers all on one device. Complete device-level switchover can be achieved when failure occurs.

A cluster enables settings on the master to be synchronized in realtime to the backup to keep consistent information. Seamless transfer of information is achieved upon switchover. The following figure shows how a VRDG and cluster work.



12.1.5.2. Cluster sync info

Synchronized data includes:

- **System time**
- **System configuration**. You need to manually configure some configuration information that cannot be synchronized. Includes:
  - Host name
  - System language
  - Interface configurations (tunnel interface configurations can be synchronized)
  - Vsys configurations

Note: When there is a Vsys with the same name on both cluster FGX devices, you can synchronize configuration information and runtime information of the Vsys.

  - Virtual network configurations
  - STP configurations
  - Login, logout, and configuration lock of administrative users
  - Priority, IP tracking, election interface, and authentication of VRs
  - Priority and IP tracking of VRDGs
  - Cluster configurations
  - License operations

- Banner configurations
- Reboot, shutdown, and reset operations
- Technical support
- System backup and restore operations
- System upgrade configurations and operations
- Copying and deleting logs
- Storage media settings
- Display operations
- Export operations
- Search operations
- Manual NTP synchronization

- **Runtime**. During a failover, the backup takes over all responsibilities of the master, requiring the failed device's runtime information. The following default runtime information is synchronized:
  - UDP sessions (whose port is not 53)
  - TCP sessions (whose port is not 80 or 8080)
  - IPSec SAs
  - NAT resources
  - ARP table
  - DHCP address assignment information
  - WebAuth user authentication status
  - VPN user connection status
  - VPN IP address pool assignment.

12.2. Basic configuration steps

This section describes the basic configuration procedure for

- 12.2.1. Basic VRRP.
- 12.2.2. Enhanced (VRDG/Cluster).

12.2.1. Basic VRRP

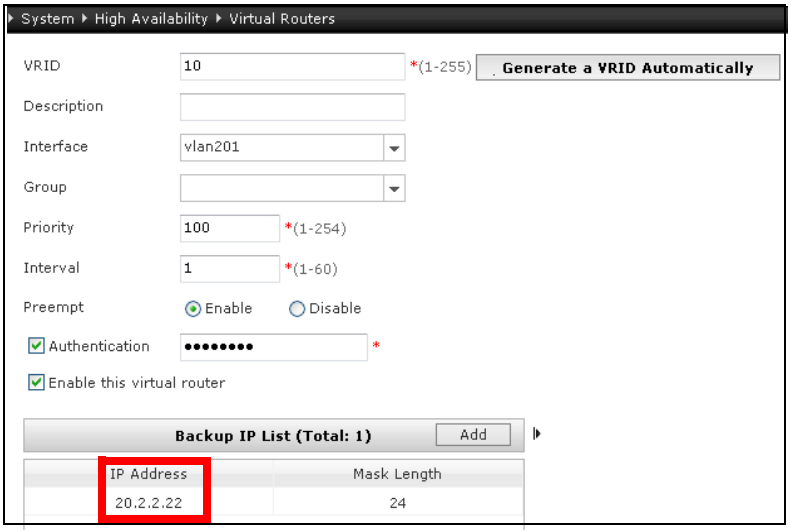
- 12.2.1.1. Device1: Configure VR.
- 12.2.1.2. Device2.

For parameters, see 12.4.1. Virtual Routers.

For example, see Example 2: Master/backup election and Example 4: IP tracking.

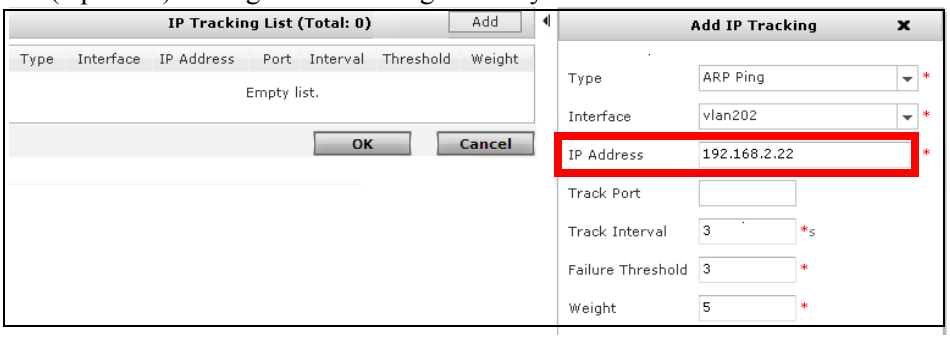
12.2.1.1. Device1: Configure VR

1. Choose **System > High Availability > Virtual Routers**.
2. Click **New**. Configure the election interface and other parameters as follows:



The backup IP address format is [1-223].[0-255].[0-255].[0-255]. It cannot be 127.0.0.0-127.255.255.255 or 192.168.255.254.

3. (Optional) Configure IP tracking on a Layer 3 interface to track link reachability:



- When two IP tracking items have the same interface and IP address, the recent one will overwrite the previous one.
- The tracked IPv4 address format is [1-223].[0-255].[0-255].[0-255]. It cannot be 127.0.0.0-127.255.255.255 or 192.168.255.254.
- You can add up to 64 IP tracking entries.

12.2.1.2. Device2

Do the above for Device2.

Table 251 Virtual router commands

virtual router *vr_id*	Create a virtual router or enter the configuration mode of this virtual router.
unset virtual router *vr_id*	Delete an existing specified virtual router.
election interface *interface_name*	Specify an election interface for a virtual router.
unset election interface *interface_name*	Delete a specified election interface.
priority *pri*	Set the priority of a VRRP router in a virtual router.
interval *interval_value*	Set the interval of sending advertisement messages from a master router to a backup.
preempt {**enable** | **disable**}	Enable or disable the preempt mode.
auth {**enable password** *auth_key* **| disable**}	Enable or disable the authentication of VRRP routers within a virtual router.
virtual-router {**enable** | **disable**}	Enable or disable a virtual router.
backup ip address *ipv4* **mask** *netmask*	Set a backup IP address for a virtual router.
unset backup ip address *ipv4*	Delete the backup IP address of a virtual router.
ip-track	Set IP tracking for a virtual router.
unset ip-track	Delete IP tracking settings of a virtual router.
show virtual-router {**all |** *vr_id*}	Display virtual router configuration information.

12.2.2. Enhanced (VRDG/Cluster)

- 12.2.2.1. Device1: Configure VR.
- 12.2.2.2. Device1: Configure VRDG.
- 12.2.2.3. Device1: Configure cluster.
- 12.2.2.4. Device2.

For parameters, see 12.4.2. Virtual Router Detection Groups and 12.4.3. Clusters.

For examples, see Example 1: Basic enhanced (VRDG/cluster) configuration, Example 3: Load sharing (master/master mode), and Example 5: Cluster synchronization.

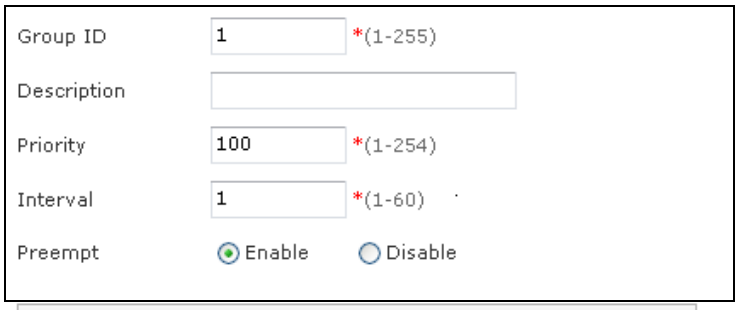
12.2.2.1. Device1: Configure VR

See 12.2.1.1. Device1: Configure VR.

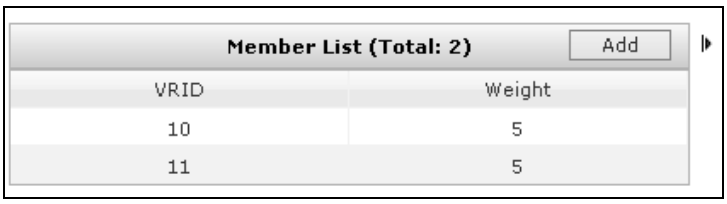
Note: Do not need to configure IP tracking on a VR because the tracking setting will be cleared once the VR joins a VRDG.

12.2.2.2. Device1: Configure VRDG

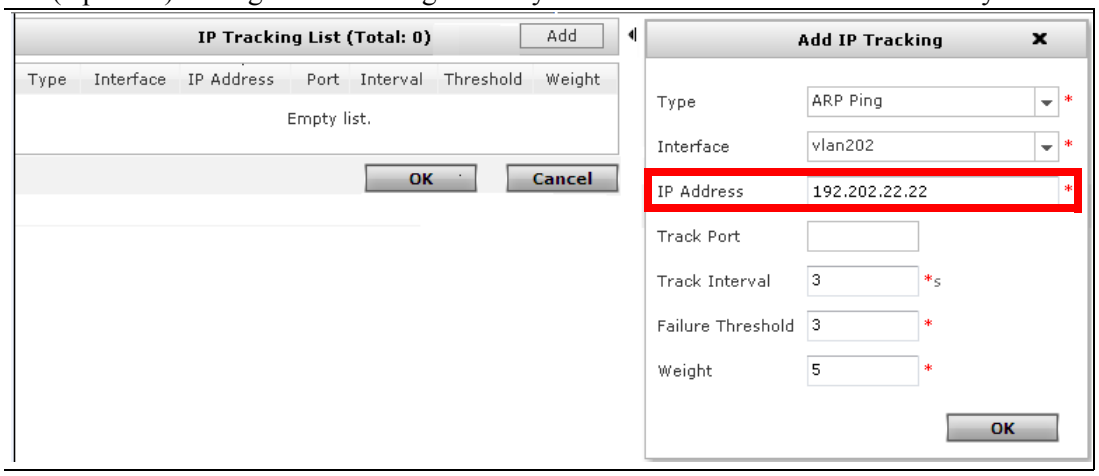
1. Choose **System > High Availability > Virtual Router Detection Groups**.
2. Click **New**. Configure group ID, priority, interval, and preempt:



3. Add the virtual routers and the weights.:



4. (Optional) Configure IP tracking on a Layer 3 interface to track link reachability:



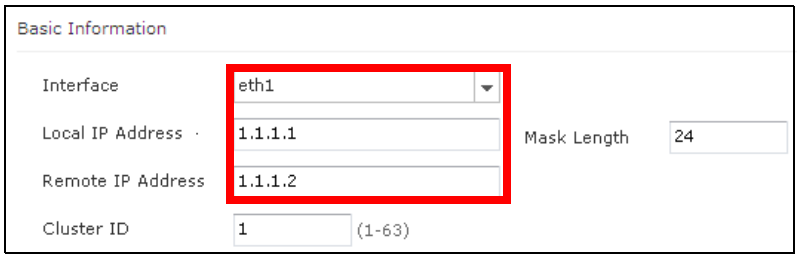
When two VRDGs have the same group ID, the recent one will take effect and its configurations will overwrite those of the previous one.

Table 252 Detection group commands

detection group *group_id*	Create a VRDG or enter the configuration mode of the VRDG.
unset detection group *group_id*	Delete a specified VRDG.
hold virtual-router weight	Assign a virtual router member to a VRDG.
unset hold virtual-router *vr_id*	Delete a specified virtual router from a VRDG.
priority *pri*	Set the priority of a VRDG.
interval *interval_value*	Set the interval of sending advertisement messages for a VRDG.
preempt {**enable** | **disable**}	Enable or disable preempt mode of a VRDG.
ip-track	Set IP tracking of a VRDG.
unset ip-track	Delete the IP tracking of the VRDG.
show detection-group {**all** | *group_id*}	Display the configuration information about VRDGs.

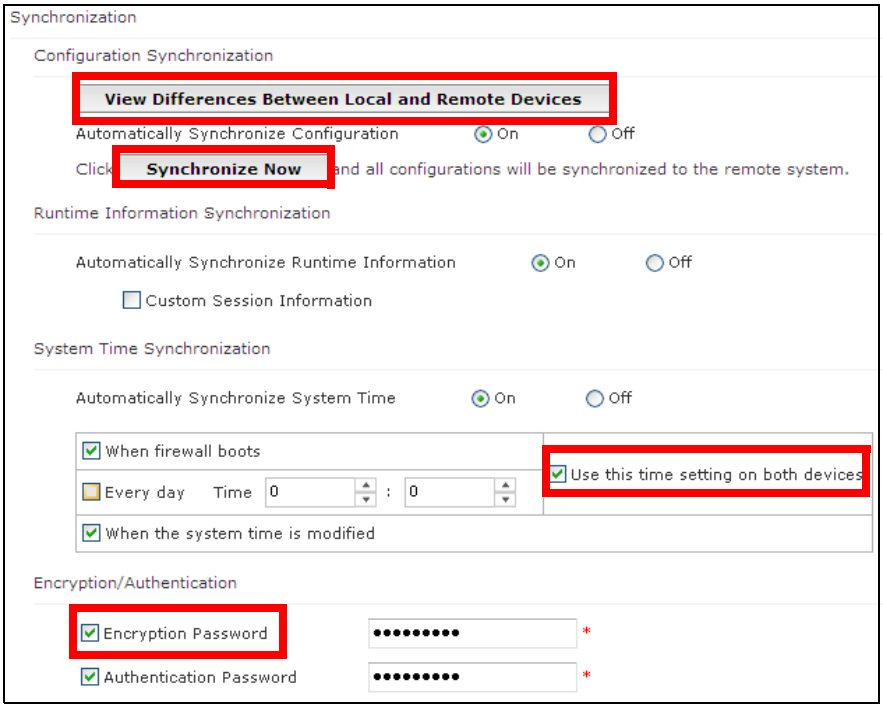
12.2.2.3. Device1: Configure cluster

1. Choose **System > High Availability > Clusters**.
2. Configure cluster ID, local and remote IP addresses, and a Layer 2 Ethernet or channel interface for synchronization,:



- You are recommended to use Layer 2 Ethernet interfaces for synchronizing configurations and Layer 2 channels for synchronizing runtime information.
- The local and remote IP address format is [1-223].[0-255].[0-255].[0-255]. It cannot be 127.0.0.0-127.255.255.255 or 192.168.255.254.

3. Configure synchronization, encryption, and authentication:



- **View Differences Between Local and Remote Devices**—before enabling automatic synchronization of configuration, you can check the configuration differences between local and remote devices.
- **Synchronize Now**—you are recommended to perform manual synchronization before automatic synchronization to keep configurations consistent for clustered devices.
- **Use this time setting on both devices**—only one device can be used as a reference point of time synchronization within a cluster.
- **Encryption**—If Device1 and Device2 are directly connected, disable encryption.

12.2.2.4. Device2

Do the above for Device2.

Table 253 Cluster commands

clusterid *cluster_id*	Add a FGX device to a specified cluster by specifying the cluster ID.
unset clusterid	Delete a FGX device from a cluster.
local interface *interface_name*	Set an interface for synchronization on the local cluster device.
unset local interface	Delete the interface for synchronization from the local cluster device.
local ip address *ipv4* **mask** *netmask*	Set the IP address of the synchronization interface on the local cluster device.
peer ip address *ipv4*	Set the IP address of the synchronization interface on the remote cluster device.
config check	Check whether the configuration information of cluster devices are the same.
config sync	Manually synchronize configuration information to the remote device.
config sync auto {**enable** | **disable**}	Enable or disable the function of automatically synchronizing configuration information.
rti sync {**enable** | **disable**}	Enable or disable the function of automatically synchronizing runtime information.
rti session default	Synchronize default sessions.
rti session {**tcp** | **udp** | **other**}	Add a custom session to be synchronized. Then the session will be synchronized to FGX.
unset rti session {**tcp** | **udp** | **other**}	Delete custom sessions to be synchronized.
time sync {**enable** | **disable**}	Enable or disable the function of automatically synchronizing system time.
time boot {**on** | **off**}	Set whether to synchronize the system time immediately when FGX is started.
time daily {*time_sync* | **off**}	Set the function of synchronizing the system time every day.
time benchmark {**on** | **off**}	Set the current FGX as the benchmark for system time synchronization.
time modified {**on** | **off**}	Set whether to synchronize the system time immediately when the FGX system time is modified.
encrypt {**enable password** *enc_key* | **disable**}	Enable or disable synchronization encryption between cluster devices.
auth {**enable** | **disable**}	Set authentication between two devices of a cluster.
show cluster	Display cluster configuration information.

12.3. Examples

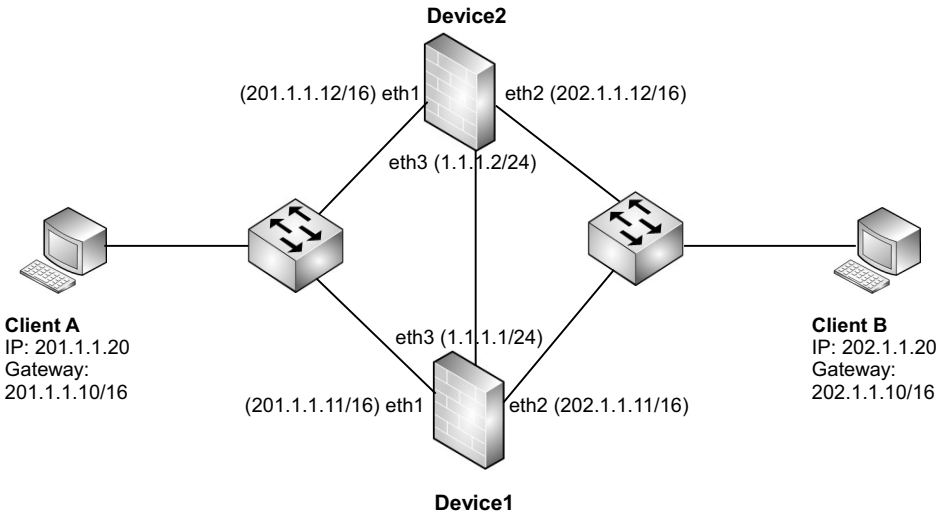
- Example 1: Basic enhanced (VRDG/cluster) configuration
- Example 2: Master/backup election
- Example 3: Load sharing (master/master mode)
- Example 4: IP tracking
- Example 5: Cluster synchronization

Example 1: Basic enhanced (VRDG/cluster) configuration

When the master device becomes unavailable, the backup device becomes the master.

This example shows how to connect two devices, Device1 and Device2, through two Layer 2 Ethernet interfaces. Enable synchronization of configurations, runtime information and system time.

Figure 48 Master/Backup Mode

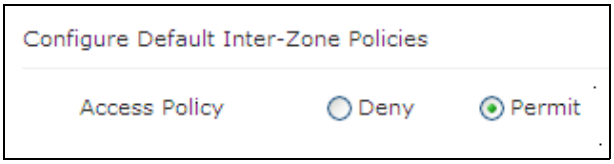


- 1.1 Configure default policy, interfaces
- 1.2 Configure VR
- 1.3 Configure VRDG
- 1.4 Configure cluster

1.1 Configure default policy, interfaces

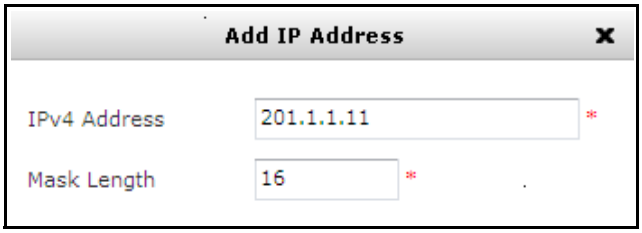
Device1

1. Choose **Firewall > Default Policy Settings**.

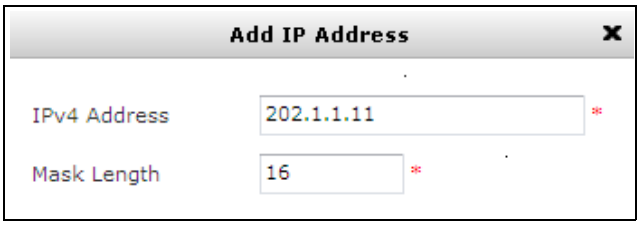


2. Click **OK**.
3. Choose **Network > Interfaces**.
4. Click corresponding to eth1 to open the Edit page. In **IP Address List**, click **Add**.

Note: If the interface is working in Layer 2 mode, you need to configure it as Layer 3 interface first and assign corresponding IP address(es).



5. Click corresponding to eth2 to open the Edit page. In **IP Address List**, click **Add**.



6. Click **OK**.

CLI

```
FGX@root> configure mode override
FGX@root-system] policy default inter-zone access permit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] ip address 201.1.1.11 255.255.0.0
FGX@root-system] exit
FGX@root-system] interface ethernet 2
FGX@root-system-if-eth2] ip address 202.1.1.11 255.255.0.0
FGX@root-system] exit
```

Device2

7. Access policy=Permit.
8. In **IP Address List**, add eth1 201.1.1.12/16 and eth2 202.1.1.12/16.

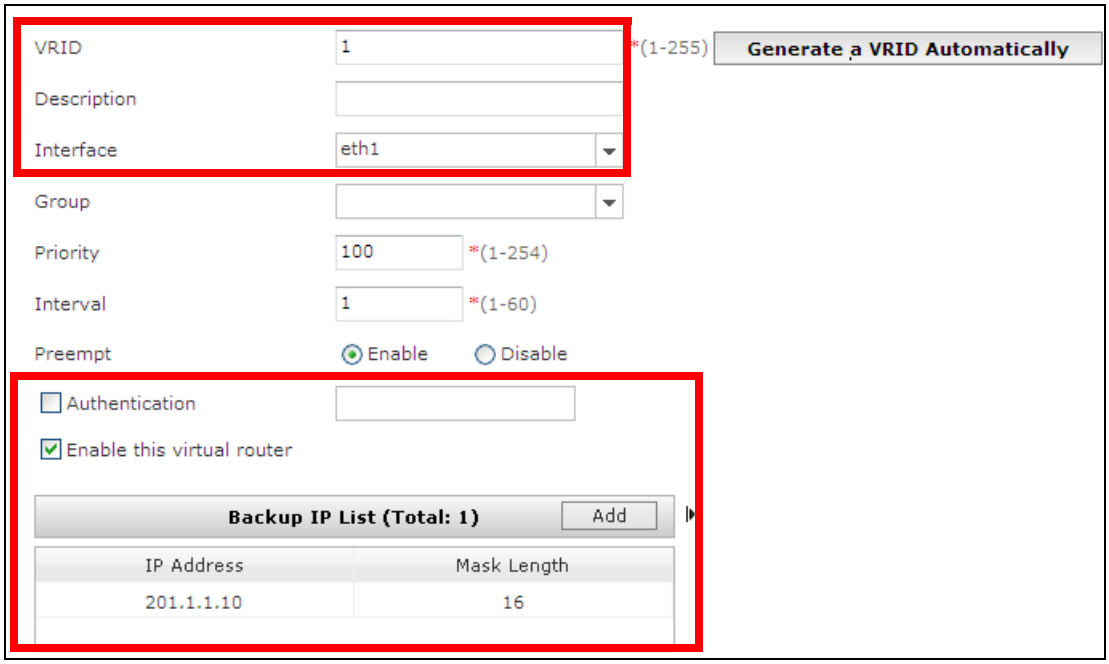
CLI

```
FGX@root> configure mode override
FGX@root-system] policy default inter-zone access permit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] ip address 201.1.1.12 255.255.0.0
FGX@root-system] exit
FGX@root-system] interface ethernet 2
FGX@root-system-if-eth2] ip address 202.1.1.12 255.255.0.0
FGX@root-system] exit
```

1.2 Configure VR

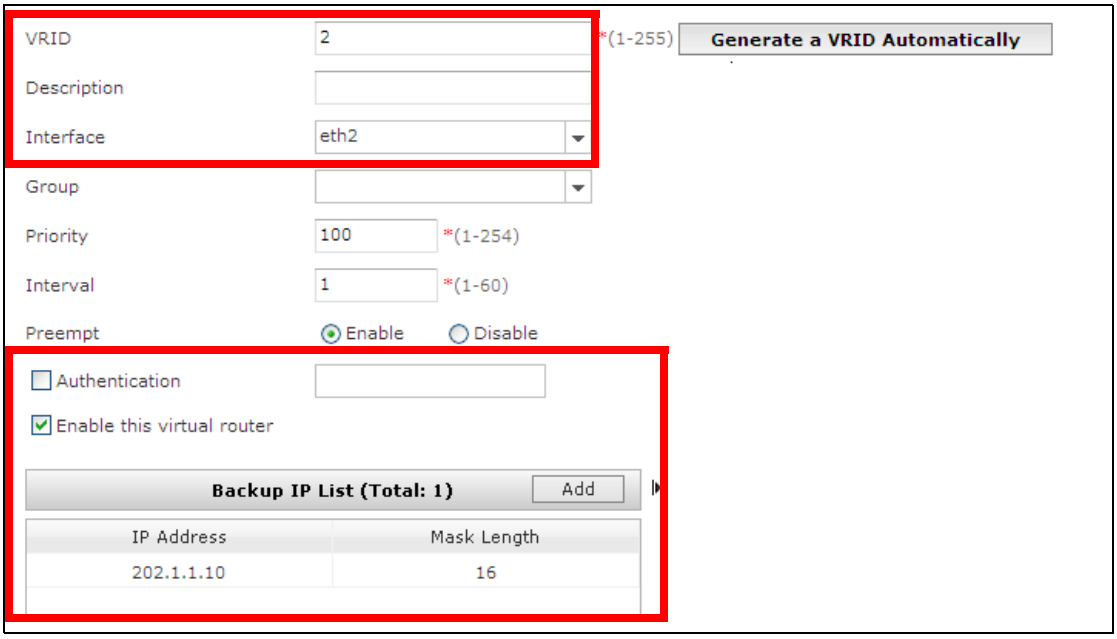
Device1

1. Choose **System > High Availability > Virtual Routers**.
2. Click **New** and set the following (the individual VR priority/interval/preempt will be overridden by VRDG settings).



3. Click **OK**.

4. Click **New** and set as follows:



5. Click **OK**.

CLI

```
FGX@root-system] virtual router 1
FGX@root-system-vr1] backup ip address 201.1.1.10 mask 255.255.0.0
FGX@root-system-vr1] election interface eth1
FGX@root-system-vr1] virtual-router enable
FGX@root-system-vr1] exit
FGX@root-system] virtual router 2
FGX@root-system-vr2] backup ip address 202.1.1.10 mask 255.255.0.0
FGX@root-system-vr2] election interface eth2
FGX@root-system-vr2] virtual-router enable
FGX@root-system-vr2] exit
```

Device2

6. New VR with VRID=1, eth1, priority=100, interval=1, preempt enabled, VR enabled, and backup IP address 201.1.1.10/16.
7. New VR with VRID=2, eth2, priority=100, interval=1, preempt enabled, VR enabled, and backup IP address 202.1.1.10/16.

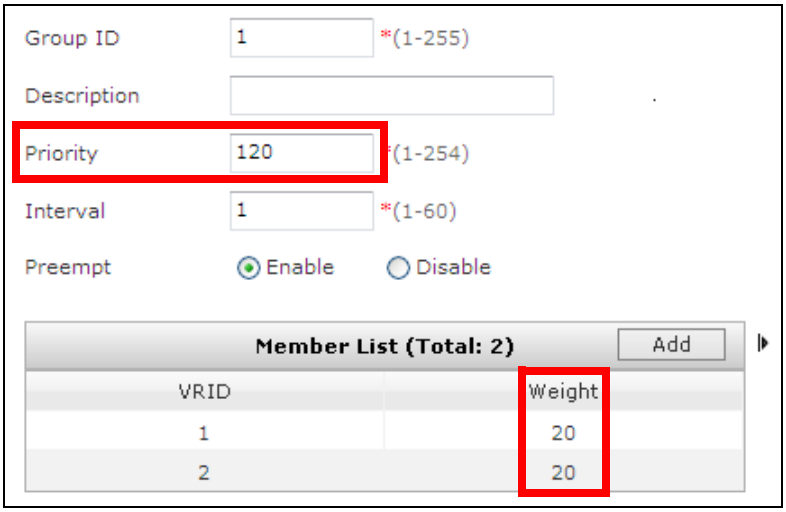
CLI

```
FGX@root-system] virtual router 1
FGX@root-system-vr1] backup ip address 201.1.1.10 mask 255.255.0.0
FGX@root-system-vr1] election interface eth1
FGX@root-system-vr1] virtual-router enable
FGX@root-system-vr1] exit
FGX@root-system] virtual router 2
FGX@root-system-vr2] backup ip address 202.1.1.10 mask 255.255.0.0
FGX@root-system-vr2] election interface eth2
FGX@root-system-vr2] virtual-router enable
FGX@root-system-vr2] exit
```

1.3 Configure VRDG

Device1

1. Choose **System > High Availability > Virtual Router Detection Groups**.
2. Click **New** and set as follows. Set the weight of both VRs as 20. If a VR fails on Device1, then the weight is subtracted from the group priority, 120-20=100. This is less than 110 (the priority for Device2 you set in step 4), and therefore the switchover will occur.



3. Click **OK**.

CLI

```
FGX@root-system] detection group 1
FGX@root-system-dg1] hold virtual-router 1 weight 20
FGX@root-system-dg1] hold virtual-router 2 weight 20
FGX@root-system-dg1] priority 120
FGX@root-system-dg1] exit
```

Device2

4. New VRDG with group ID=1, priority=110, interval=1, preempt enabled, members include VRID 1 and 2 with weight=20.

CLI

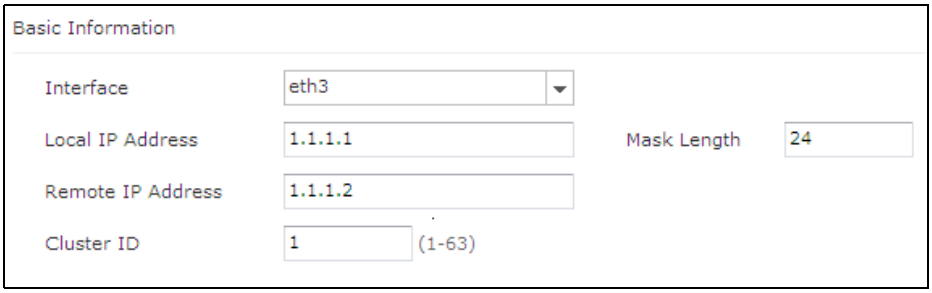
```
FGX@root-system] detection group 1
FGX@root-system-dg1] hold virtual-router 1 weight 20
FGX@root-system-dg1] hold virtual-router 2 weight 20
FGX@root-system-dg1] priority 110
FGX@root-system-dg1] exit
```

1.4 Configure cluster

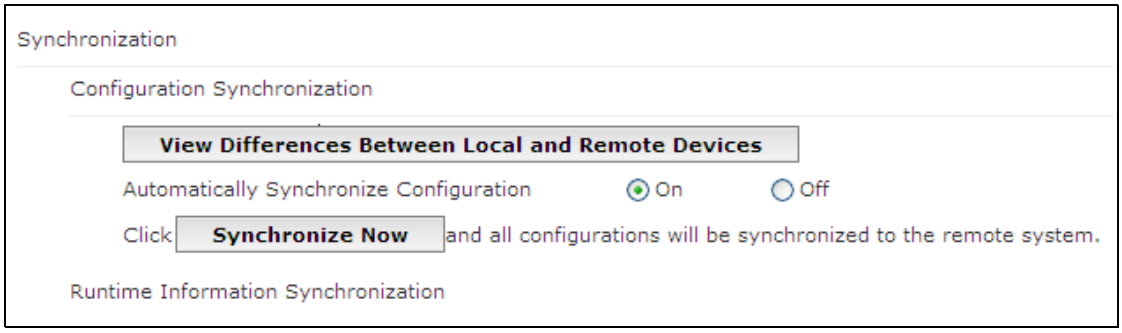
Device1

The HA interface for synchronization should be a Layer 2 Ethernet interface or channel interface. The settings here will cause data to synchronize from Device1 to Device2.

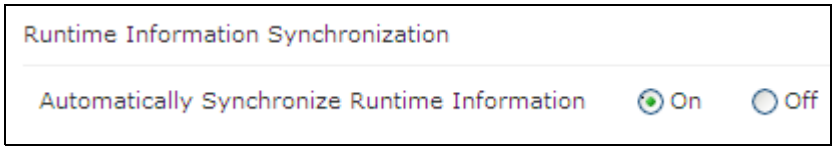
1. Choose **System > High Availability > Clusters** and set a cluster:



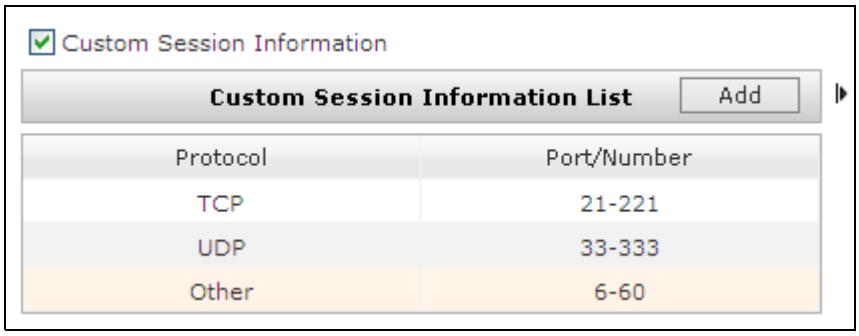
2. (Optional) Click **View Differences Between Local and Remote Devices**. This will check the other device, and see if there are any differences between configurations.
3. If any, click **Synchronize Now**. This will synchronize Device1 to Device2 to keep consistent configurations.
4. Click **Automatically Synchronize Configuration** to **On**. This setting causes any realtime configuration change on Device1 to be synchronized to Device2. After enabling this function on Device2, any changes on either device will be automatically synchronized to each other.



5. Click **Automatically Synchronize Runtime Information** to **On**. This setting causes default runtime information on Device1 to be synchronized to Device2. After enabling this function on Device2, default runtime information will be automatically synchronized to each other.

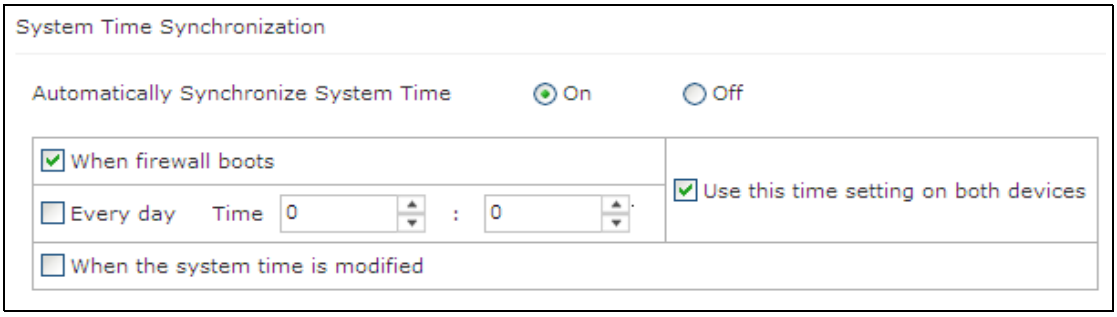


6. Check **Custom Session Information** to customize sessions to synchronize by specifying protocol types and port numbers. This setting will cause custom sessions on Device1 to be automatically synchronized to Device2.



7. Click **Automatically Synchronize System Time** to **On**.
8. Check "**When firewall boots.**" and optionally check "**Use this time setting on both devices.**" Whenever Device1 boots, its system time is automatically synchronized to Device2.

Note: Only one device can be used as a reference point of time synchronization within a cluster.



9. Click **OK**.
10. Click .

CLI

```
FGX@root-system] cluster
FGX@root-system-cluster] clusterid 1
FGX@root-system-cluster] local interface eth3
FGX@root-system-cluster] local ip address 1.1.1.1 mask 255.255.255.0
FGX@root-system-cluster] peer ip address 1.1.1.2
FGX@root-system-cluster] config check
FGX@root-system-cluster] config sync
FGX@root-system-cluster] config sync auto enable
FGX@root-system-cluster] rti sync enable
FGX@root-system-cluster] rti session default
FGX@root-system-cluster] rti session tcp 21-221
FGX@root-system-cluster] rti session udp 33-333
FGX@root-system-cluster] rti session other 6-60
FGX@root-system-cluster] time sync enable
FGX@root-system-cluster] time boot on
FGX@root-system-cluster] time benchmark on
FGX@root-system-cluster] end
FGX@root> save config
```

Device2

11. Create cluster with interface=eth3, local IP address=1.1.1.2/24, remote IP address=1.1.1.1, cluster ID=1.

12. **Automatically Synchronize Configuration/Runtime Information/System Time**=On. This will cause data changes on Device2 to be synchronized to Device1.

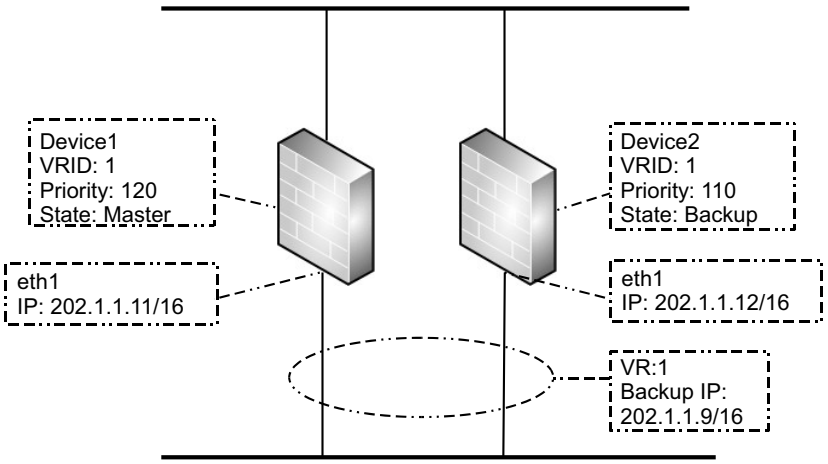
CLI

```
FGX@root-system] cluster
FGX@root-system-cluster] clusterid 1
FGX@root-system-cluster] local interface eth3
FGX@root-system-cluster] local ip address 1.1.1.2 mask 255.255.255.0
FGX@root-system-cluster] peer ip address 1.1.1.1
FGX@root-system-cluster] config sync auto enable
FGX@root-system-cluster] rti sync enable
FGX@root-system-cluster] time sync enable
FGX@root-system-cluster] end
FGX@root> save config
```

Example 2: Master/backup election

The following example simply shows how a virtual router election operates and the master/backup roles are determined.

Figure 49 Master/Backup Election

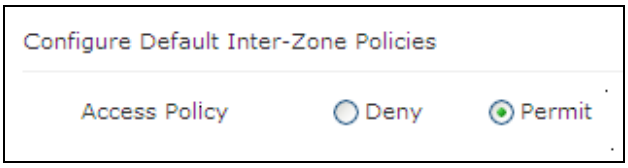


- 2.1 Configure default policy, interfaces
- 2.2 Configure VR
- 2.3 View election results
- 2.4 Failover
- 2.5 Failure restore

2.1 Configure default policy, interfaces

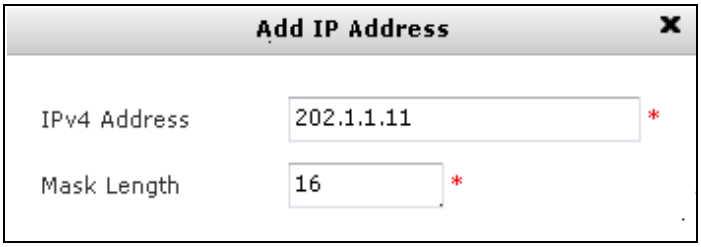
Device1

1. Choose **Firewall > Default Policy Settings**.



2. Click **OK**.
3. Choose **Network > Interfaces**.
4. Click corresponding to eth1 to open the Edit page. In **IP Address List**, click **Add**.

Note: If the interface is working in Layer 2 mode, you need to configure it as Layer 3 interface first and assign corresponding IP address (es).



5. Click **OK**.

CLI

```
FGX@root> configure mode override
FGX@root-system] policy default inter-zone access permit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] ip address 202.1.1.11 255.255.0.0
FGX@root-system] exit
```

Device2

6. Access policy = Permit.
7. In **IP Address List**, add eth1 202.1.1.12/16.

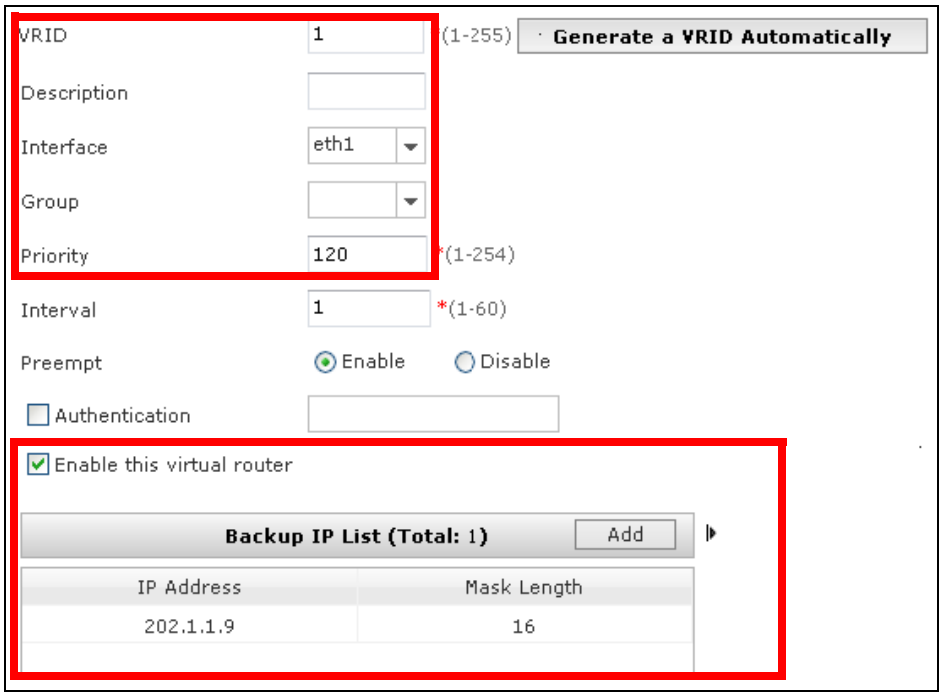
CLI

```
FGX@root> configure mode override
FGX@root-system] policy default inter-zone access permit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] ip address 202.1.1.12 255.255.0.0
FGX@root-system] exit
```

2.2 Configure VR

Device1

1. Choose **System > High Availability > Virtual Routers**.
2. Click **New** and set the following (use default value for interval and preempt).



3. Click **OK**.
4. Click .

CLI

```
FGX@root-system] virtual router 1
FGX@root-system-vr1] priority 120
FGX@root-system-vr1] backup ip address 202.1.1.9 mask 255.255.0.0
FGX@root-system-vr1] election interface eth1
FGX@root-system-vr1] virtual-router enable
FGX@root-system-vr1] end
FGX@root> save config
```

Device2

5. New VR with VRID=1, eth1, priority = 110, interval = 1, preempt enabled, VR enabled, and backup IP address 202.1.1.9/16.

CLI

```
FGX@root-system] virtual router 1
FGX@root-system-vr1] priority 110
FGX@root-system-vr1] backup ip address 202.1.1.9 mask 255.255.0.0
FGX@root-system-vr1] election interface eth1
FGX@root-system-vr1] virtual-router enable
FGX@root-system-vr1] end
```

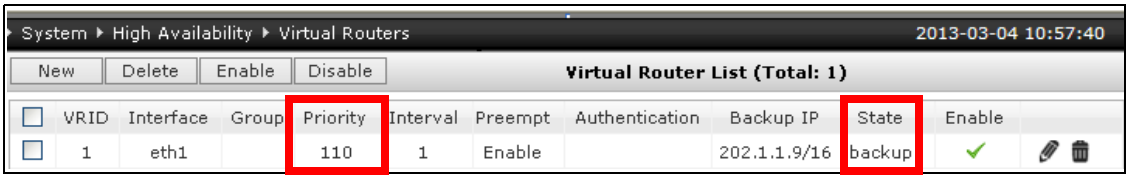
2.3 View election results

The election starts.

1. Choose **System > High Availability > Virtual Routers**.
2. View the state on Device1. Device1 is the master because it has a higher priority.


```
FGX@root> show virtual-router all
VRID:            1
Enable:          on
Interface:       eth1
Interval:        1
Preempt:         Enable
Authentication:  None
Backup ip:       202.1.1.9/16
State:           master
Detection Group:
Config Priority:         120
Election Priority:       120
Description:
```

3. View the state on Device2. It becomes the backup.



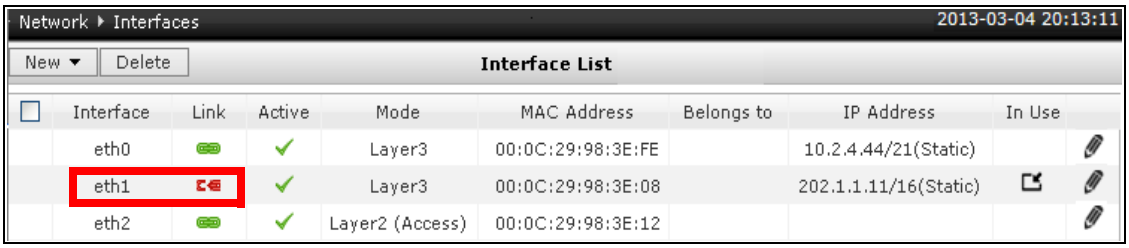

```
FGX@root> show virtual-router all
VRID:            1
Enable:          on
Interface:       eth1
Interval:        1
Preempt:         Enable
Authentication:  None
Backup ip:       202.1.1.9/16
State:           backup
Detection Group:
Config Priority:         110
Election Priority:       110
Description:
```

If they are of the same priority, Device2 will become the master because it has a higher primary IP address 202.1.1.12/16 than Device1 (202.1.1.11/16). For more information about primary IP address, see 12.1.2.2 VR election.

2.4 Failover

When eth1 on Device1 goes down, a new election is triggered.

1. Choose **Network > Interfaces**. The interface eth1 is shown as disconnected.



2. Choose **System > High Availability > Virtual Routers**.

   View the master/backup state in the WebUI and CLI. Device1 is the backup device.


```
FGX@root> show virtual-router all
VRID:           1
Enable:         on
Interface:      eth1
Interval:       1
Preempt:        Enable
Authentication: None
Backup ip:      202.1.1.9/16
State:          backup
Detection Group:
Config Priority:        120
Election Priority:      120
Description:
```

3. Device2 is the master device.

```
FGX@root> show virtual-router all
VRID:           1
Enable:         on
Interface:      eth1
Interval:       1
Preempt:        Enable
Authentication: None
Backup ip:      202.1.1.9/16
State:          master
Detection Group:
Config Priority:        110
Election Priority:      110
Description:
```

The priority initially configured (shown as Config Priority in the CLI) will not change. The device adjusts the master/backup state based on the dynamic priority (shown as Election Priority in the CLI).

2.5 Failure restore

When eth1 on Device1 goes up, a new election is triggered. View the master/backup state on both devices. Device1 restores the master state. WebUI and CLI display is the same as that in 2.3 View election results.

Note: Failure restore does not occur when the two devices are initially of the same priority.

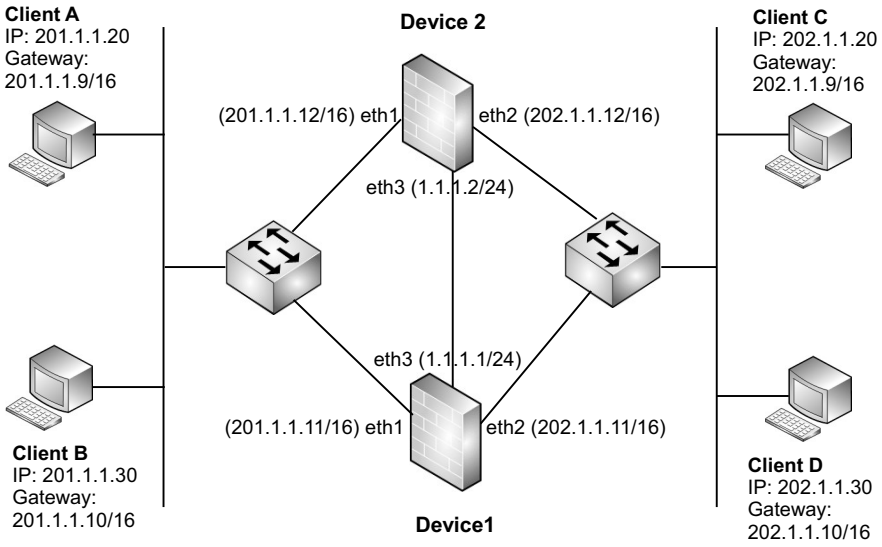
Example 3: Load sharing (master/master mode)

In master/master mode, both FGX devices in the master state can handle data simultaneously so that load sharing and redundancy can be achieved.

This example shows how to perform the following configurations:

- Directly connect two devices, Device1 and Device2, through two Layer 2 Ethernet interfaces.
- Enable synchronization of configurations, runtime information, and system time on both devices.
- Configure the two devices to synchronize system time whenever they restart, and Device1 is set as the reference point for time synchronization.
- Client A accesses Client C through Device1, and Client B accesses Client D through Device2.

Figure 50 Master/Master Mode



- 3.1 Configure default policy, interfaces
- 3.2 Configure VR
- 3.3 Configure VRDG
- 3.4 Configure cluster

3.1 Configure default policy, interfaces

Device1

1. Access policy=Permit.
2. In **IP Address List**, add eth1 201.1.1.11/16 and eth2 202.1.11/16.

CLI

```
FGX@root> configure mode override
FGX@root-system] policy default inter-zone access permit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] ip address 201.1.1.11 255.255.0.0
FGX@root-system] exit
FGX@root-system] interface ethernet 2
FGX@root-system-if-eth2] ip address 202.1.1.11 255.255.0.0
FGX@root-system] exit
```

Device2

3. Access policy = Permit.
4. In **IP Address List**, add eth1 201.1.1.12/16 and eth2 202.1.12/16.

CLI

```
FGX@root> configure mode override
FGX@root-system] policy default inter-zone access permit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] ip address 201.1.1.12 255.255.0.0
FGX@root-system] exit
FGX@root-system] interface ethernet 2
FGX@root-system-if-eth2] ip address 202.1.1.12 255.255.0.0
FGX@root-system] exit
```

3.2 Configure VR

Device1

1. New VR with VRID=1, eth1, priority =100, interval=1, preempt enabled, VR enabled, and backup IP address 201.1.1.9/16.
2. New VR with VRID=2, eth1, priority=100, interval=1, preempt enabled, VR enabled, and backup IP address 201.1.1.10/16.
3. New VR with VRID=3, eth2, priority=100, interval =1, preempt enabled, VR enabled, and backup IP address 202.1.1.9/16.
4. New VR with VRID=4, eth2, priority =100, interval=1, preempt enabled, VR enabled, and backup IP address 202.1.1.10/16.

CLI

```
FGX@root-system] virtual router 1
FGX@root-system-vr1] backup ip address 201.1.1.9 mask 255.255.0.0
FGX@root-system-vr1] election interface eth1
FGX@root-system-vr1] virtual-router enable
FGX@root-system-vr1] exit
FGX@root-system] virtual router 2
FGX@root-system-vr2] backup ip address 201.1.1.10 mask 255.255.0.0
FGX@root-system-vr2] election interface eth1
FGX@root-system-vr2] virtual-router enable
FGX@root-system-vr2] exit
FGX@root-system] virtual router 3
FGX@root-system-vr3] backup ip address 202.1.1.9 mask 255.255.0.0
FGX@root-system-vr3] election interface eth2
FGX@root-system-vr3] virtual-router enable
FGX@root-system-vr3] exit
FGX@root-system] virtual router 4
FGX@root-system-vr4] backup ip address 202.1.1.10 mask 255.255.0.0
FGX@root-system-vr4] election interface eth2
FGX@root-system-vr4] virtual-router enable
FGX@root-system-vr4] exit
```

Device2

Exactly the same as for Device1.

5. New VR with VRID=1, eth1, priority=100, interval=1, preempt enabled, VR enabled, and backup IP address 201.1.1.9/16.
6. New VR with VRID=2, eth1, priority=100, interval=1, preempt enabled, VR enabled, and backup IP address 201.1.1.10/16.
7. New VR with VRID=3, eth2, priority=100, interval=1, preempt enabled, VR enabled, and backup IP address 202.1.1.9/16.
8. New VR with VRID=4, eth2, priority=100, interval=1, preempt enabled, VR enabled, and backup IP address 202.1.1.10/16.

CLI

```
FGX@root-system] virtual router 1
FGX@root-system-vr1] backup ip address 201.1.1.9 mask 255.255.0.0
FGX@root-system-vr1] election interface eth1
FGX@root-system-vr1] virtual-router enable
FGX@root-system-vr1] exit
FGX@root-system] virtual router 2
FGX@root-system-vr2] backup ip address 201.1.1.10 mask 255.255.0.0
FGX@root-system-vr2] election interface eth1
FGX@root-system-vr2] virtual-router enable
FGX@root-system-vr2] exit
FGX@root-system] virtual router 3
FGX@root-system-vr3] backup ip address 202.1.1.9 mask 255.255.0.0
FGX@root-system-vr3] election interface eth2
FGX@root-system-vr3] virtual-router enable
FGX@root-system-vr3] exit
FGX@root-system] virtual router 4
FGX@root-system-vr4] backup ip address 202.1.1.10 mask 255.255.0.0
FGX@root-system-vr4] election interface eth2
FGX@root-system-vr4] virtual-router enable
FGX@root-system-vr4] exit
```

3.3 Configure VRDG

Device1

1. New VRDG with group ID=1, **priority=100**, interval=1, preempt enabled, members include VRID 1 and 3 with weight=10.
2. New VRDG with group ID=2, **priority=95**, interval=1, preempt enabled, members include VRID 2 and 4 with weight=10.

CLI

```
FGX@root-system] detection group 1
FGX@root-system-dg1] hold virtual-router 1 weight 10
FGX@root-system-dg1] hold virtual-router 3 weight 10
FGX@root-system-dg1] priority 100
FGX@root-system-dg1] exit
FGX@root-system] detection group 2
FGX@root-system-dg2] hold virtual-router 2 weight 10
FGX@root-system-dg2] hold virtual-router 4 weight 10
FGX@root-system-dg2] priority 95
FGX@root-system-dg2] exit
```

Device2

3. New VRDG with group ID=1, **priority=95**, interval=1, preempt enabled, members include VRID 1 and 3 with weight=10.
4. New VRDG with group ID=2, **priority=100**, interval=1, preempt enabled, members include VRID 2 and 4 with weight=10.

CLI

```
FGX@root-system] detection group 1
FGX@root-system-dg1] hold virtual-router 1 weight 10
FGX@root-system-dg1] hold virtual-router 3 weight 10
FGX@root-system-dg1] priority 95
FGX@root-system-dg1] exit
FGX@root-system] detection group 2
FGX@root-system-dg2] hold virtual-router 2 weight 10
FGX@root-system-dg2] hold virtual-router 4 weight 10
FGX@root-system-dg2] priority 100
FGX@root-system-dg2] exit
```

3.4 Configure cluster

Device1

1. Create cluster with interface=eth3, local IP address=1.1.1.1/24, remote IP address=1.1.1.2, cluster ID=1.
2. Configure synchronization.
   a. Click **Synchronize Now**.
   b. **Automatically Synchronize Configuration/Runtime Information=On**
   c. **Automatically Synchronize System Time=On**
      - Check "**When firewall boots**"
      - Check "**Use this time setting on both devices**"

CLI

```
FGX@root-system] cluster
FGX@root-system-cluster] clusterid 1
FGX@root-system-cluster] local interface eth3
FGX@root-system-cluster] local ip address 1.1.1.1 mask 255.255.255.0
FGX@root-system-cluster] peer ip address 1.1.1.2
FGX@root-system-cluster] config sync
FGX@root-system-cluster] config sync auto enable
FGX@root-system-cluster] rti sync enable
FGX@root-system-cluster] time sync enable
FGX@root-system-cluster] time boot on
FGX@root-system-cluster] time benchmark on
FGX@root-system-cluster] end
FGX@root> save config
```

Device2

3. Create cluster with interface=eth3, local IP address=1.1.1.2/24, remote IP address=1.1.1.1, cluster ID=1.
4. Configure synchronization.
   a. **Automatically Synchronize Configuration/Runtime Information/System Time=On**
   b. Check "**When firewall boots**"

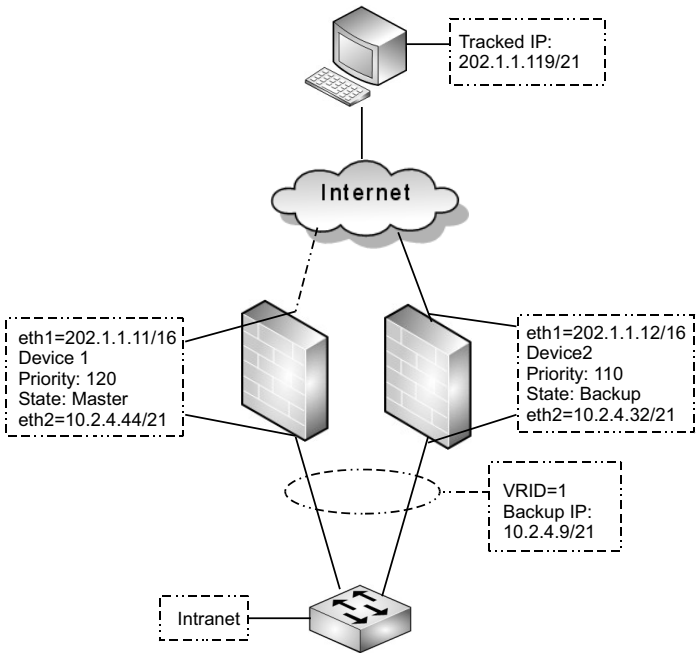
CLI

```
FGX@root-system] cluster
FGX@root-system-cluster] clusterid 1
FGX@root-system-cluster] local interface eth3
FGX@root-system-cluster] local ip address 1.1.1.2 mask 255.255.255.0
FGX@root-system-cluster] peer ip address 1.1.1.1
FGX@root-system-cluster] config sync auto enable
FGX@root-system-cluster] rti sync enable
FGX@root-system-cluster] time sync enable
FGX@root-system-cluster] time boot on
FGX@root-system-cluster] end
FGX@root> save config
```

Example 4: IP tracking

IP tracking is used for a virtual router to track link reachability. The tracking result affects virtual router priority and triggers a possible switchover. The following example shows how IP tracking is used on a VR to detect the connectivity of the external link.

Figure 51 IP Tracking



In the above scenario, a virtual router (VRID=1) is created on intranet interfaces (eth2). Device1 is the master router. When the link from Device1 to the destination host 202.1.1.119 is degraded, Internet traffic is sent to Device2, while internal traffic is still sent to Device1, resulting in traffic disruption.

This issue can be addressed by configuring IP tracking on both devices to dynamically monitor the links to 202.1.1.119 through eth1.

- On Device1, Ping packets are sent every 4 seconds. When IP tracking fails 5 times in a row, Device1 degrades its priority by 15 (track weight). Device2 will transition to master.
- When the degraded link on Device1 recovers, the priority will be restored to the original (120). Device1 will transition back to master.

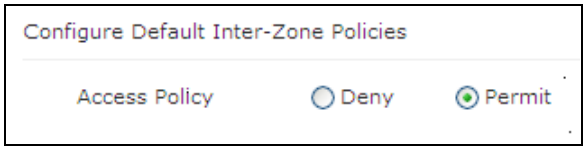
You need to:

- 4.1 Configure default policy, interfaces
- 4.2 Configure VR and IP tracking
- 4.3 View tracking status
- 4.4 Tracking failure on Device1
- 4.5 Failure restore

4.1 Configure default policy, interfaces

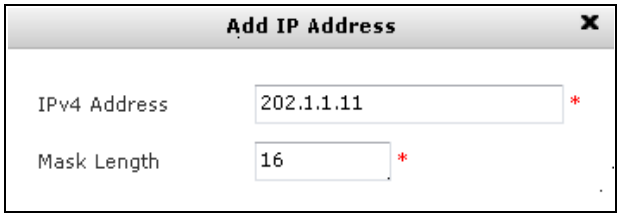
Device1

1. Choose **Firewall > Default Policy Settings**.

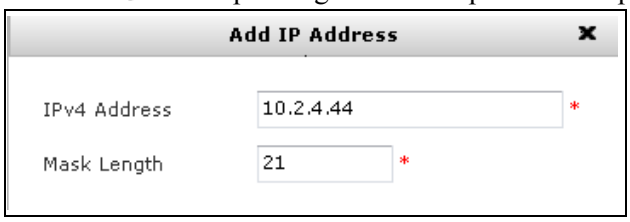


2. Click **OK**.
3. Choose **Network > Interfaces**.
4. Click corresponding to eth1 to open the Edit page. In **IP Address List**, click **Add**.

Note: If the interface is working in Layer 2 mode, you need to configure it as Layer 3 interface first and assign corresponding IP address (es).



5. Click corresponding to eth2 to open the Edit page. In **IP Address List**, click **Add**.



6. Click OK.

CLI

```
FGX@root> configure mode override
FGX@root-system] policy default inter-zone access permit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] ip address 202.1.1.11 255.255.0.0
FGX@root-system] exit
FGX@root-system] interface ethernet 2
FGX@root-system-if-eth2] ip address 10.2.4.44 255.255.248.0
FGX@root-system] exit
```

Device2

7. Access policy = Permit.
8. In **IP Address List**, add eth1 202.1.1.12/16 and eth2 10.2.4.32/21.

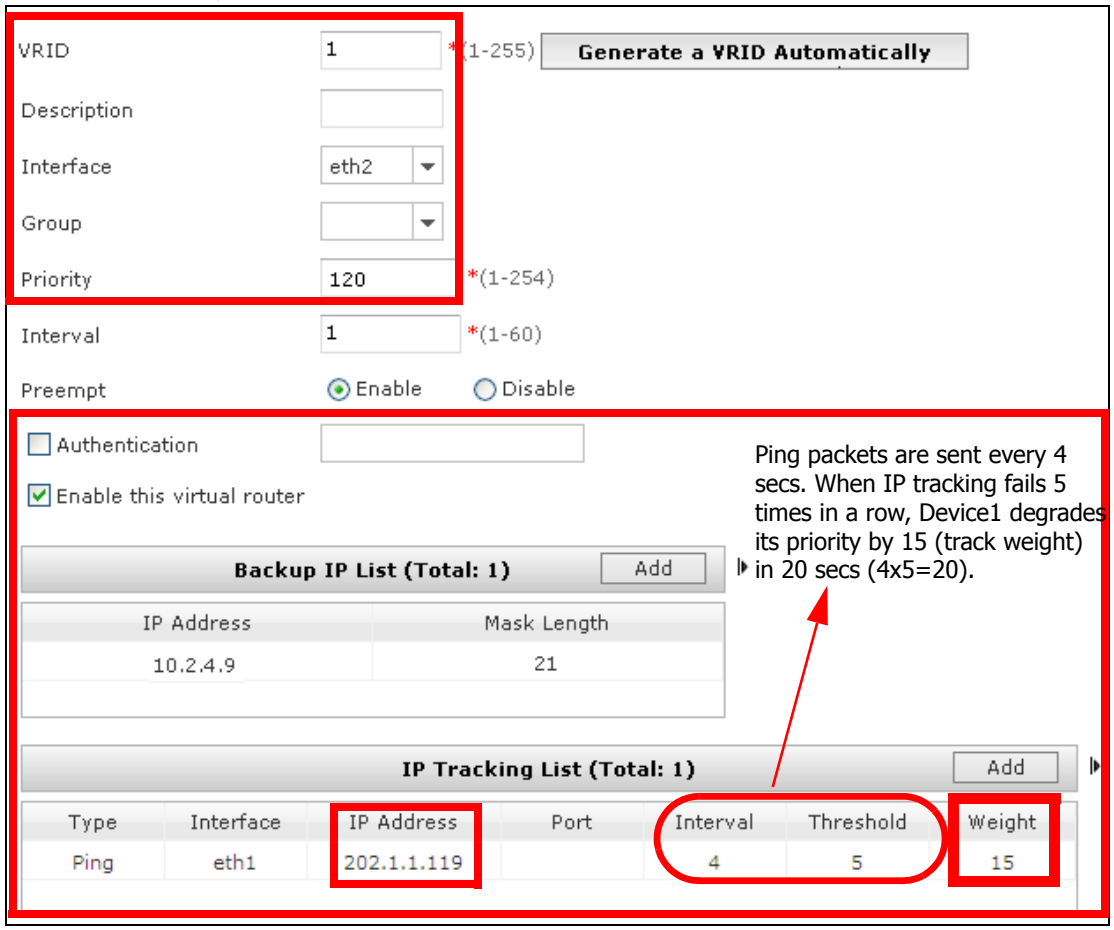
CLI

```
FGX@root> configure mode override
FGX@root-system] policy default inter-zone access permit
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] ip address 202.1.1.12 255.255.0.0
FGX@root-system] exit
FGX@root-system] interface ethernet 2
FGX@root-system-if-eth2] ip address 10.2.4.32 255.255.248.0
FGX@root-system] exit
```

4.2 Configure VR and IP tracking

Device1

1. Choose **System > High Availability > Virtual Routers**.
2. Click **New** and set the following (use default values for interval, preempt, and authentication).



- IP tracking to a specified destination for two master/backup devices should have the same IP address setting.
- To make sure failover occurs, you need to enable the preempt mode and configure the individual virtual router weight as greater than the difference between the virtual router priorities.

3. Click **OK**.
4. Click .

CLI

```
FGX@root-system] virtual router 1
FGX@root-system] priority 120
FGX@root-system-vr1] backup ip address 10.2.4.9 mask 255.255.248.0
FGX@root-system-vr1] election interface eth2
FGX@root-system-vr1] virtual-router enable
FGX@root-system-vr1] ip-track type ping interface eth1 ip 202.1.1.119
interval 4 threshold 5 weight 15
FGX@root-system-vr1] end
FGX@root> save config
```

Device2

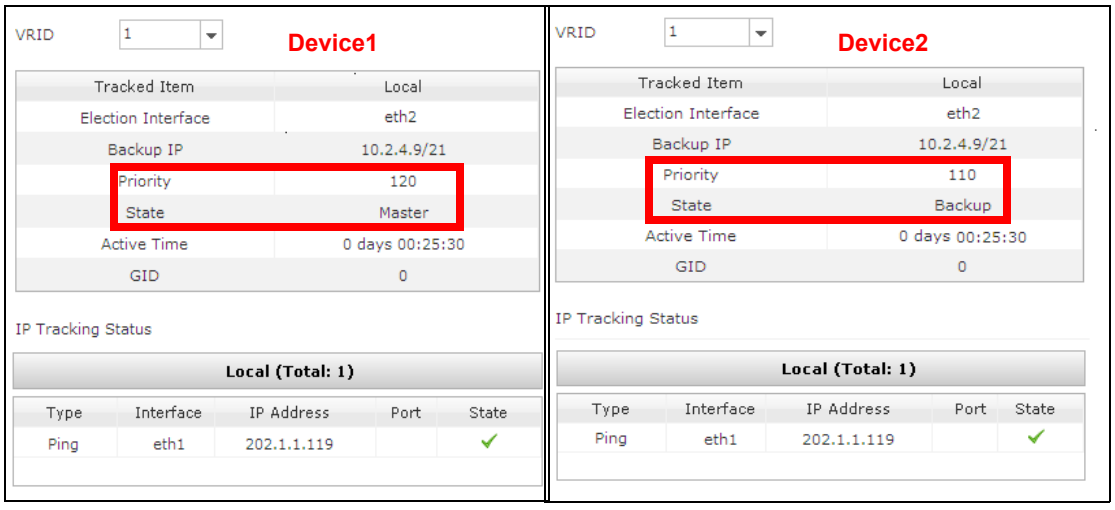
5. New VR with VRID=1, eth2, priority = 110, interval = 1, preempt enabled, VR enabled, and backup IP address 10.2.4.9/21; IP track type=Ping, tracking interface=eth1, tracked IP=202.1.1.119, interval=5, threshold=6, weight=20.

CLI

```
FGX@root-system] virtual router 1
FGX@root-system] priority 110
FGX@root-system-vr1] backup ip address 10.2.4.9 mask 255.255.248.0
FGX@root-system-vr1] election interface eth2
FGX@root-system-vr1] virtual-router enable
FGX@root-system-vr1] ip-track type ping interface eth1 ip 202.1.1.119
interval 5 threshold 6 weight 20
FGX@root-system-vr1] end
```

4.3 View tracking status

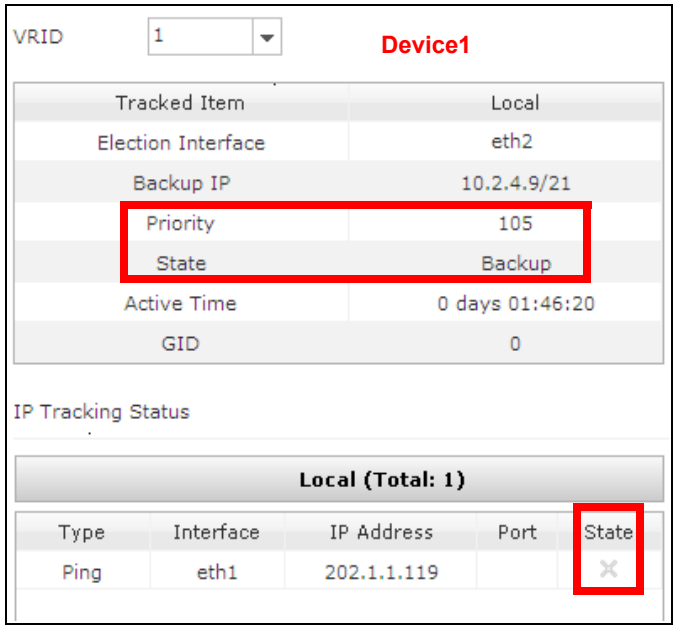
1. Choose **Monitor > High Availability > Virtual Routers**.
2. View the master/backup state. Device1 becomes the master.



4.4 Tracking failure on Device1

When Device1 IP tracking to 202.1.1.119 fails 5 times in a row within 20 seconds (interval=4 secs; 4x5=20s), the VR priority (120) on Device1 is degraded by the tracking weight (15), resulting in a new priority of 105. Device2 transitions to the master.

1. Choose **Monitor > High Availability > Virtual Routers**.
2. View Device1 state in the WebUI and CLI.

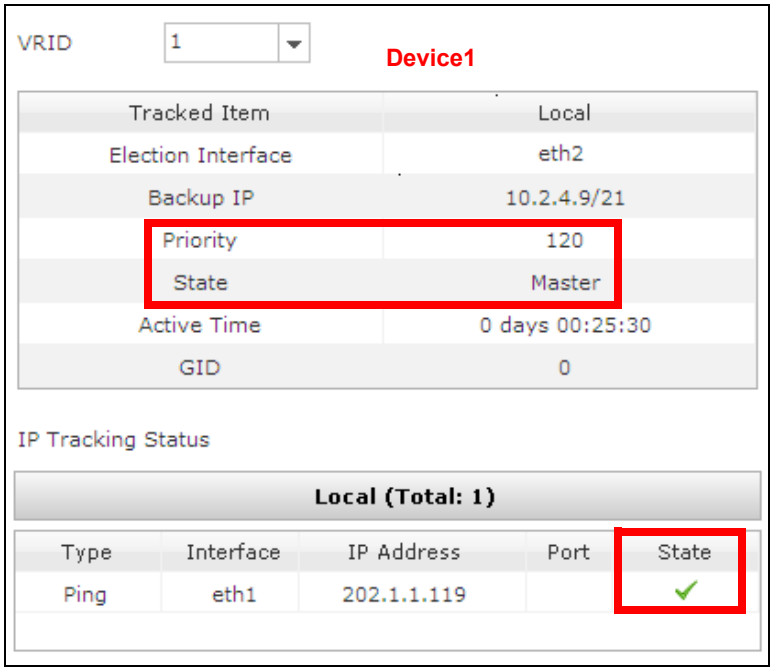



```
FGX@root> show virtual-router 1
VRID:           1
Enable:         on
Interface:      eth2
Interval:       1
Preempt:        Enable
Authentication: 0
Backup ip:      10.2.4.9/21
State:          backup
Detection Group:
Config Priority:        120
Election Priority:      105
Description:

Type      Interface IP              Port      Interval  Threshold Weight
Ping      eth1      202.1.1.119     -         4         5         15
```

4.5 Failure restore

When Device1 IP tracking recovers from failure, its VR will regain its original configuration priority (120) by adding the tracking weight (15) to current election priority (105).

1. Choose **Monitor > High Availability > Virtual Routers**.
2. View the state. Device1 restores the master.

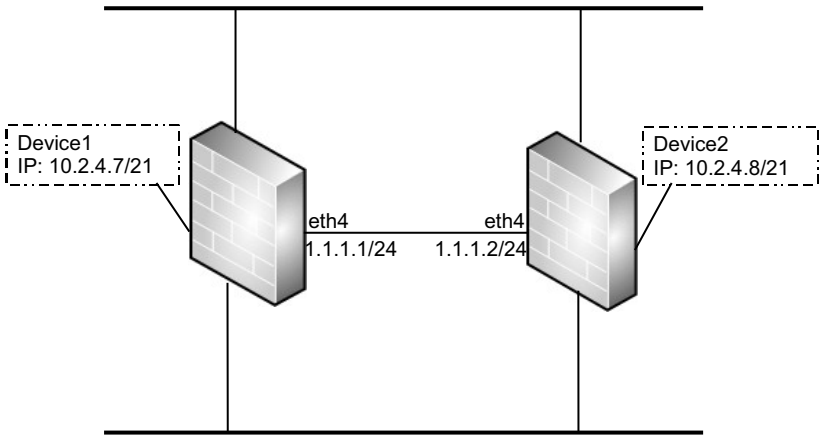


Example 5: Cluster synchronization

FGX provides clustering synchronization. Synchronization between two FGX devices does not require VR configurations.

The following shows a basic example of cluster synchronization without VR configuration.

Figure 52 Synchronization



Note: Recommended to configure two FGX devices in a cluster with the same hardware model and system version.

- Device1 is configured with DNS information:
  - DNS host: primary DNS=192.2.2.22; secondary DNS=202.2.2.234;
  - DNS proxy: domain name=abc, interface=any, primary DNS=192.123.23.23;
  - Static cache: state=Enable, domain name=abc, interface=any, IP address=192.168.2.4.
- You need to manually perform a complete synchronization from Device1 to Device2 to make configurations on the two devices consistent.
- When you modify new configurations on either device, they will synchronize to each other.
- Use Device1 as the reference point of time, by which its system time is synchronized to the other one whenever the device boots.

You need to:

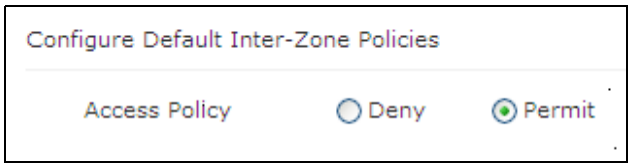
- 5.1 Configure cluster
- 5.2 Check differences between local and remote
- 5.3 Synchronize configuration manually
- 5.4 Synchronize configuration automatically
- 5.5 Synchronize system time

5.1 Configure cluster

- Device1. Default policy, cluster
- Device2. Default policy, cluster

Device1. Default policy, cluster

1. Choose **Firewall > Default Policy Settings**.



2. Click **OK**.
3. Choose **System > High Availability > Clusters**.
4. Configure basic information.

   - The interface used for synchronization should be a Layer 2 Ethernet or channel interface. Recommended to use Ethernet interfaces for synchronizing configurations and channels for synchronizing runtime information.
   - The local and remote devices should have the same cluster ID.
5. Click **OK**.
6. Click .

CLI

```
FGX@root> configure mode override
FGX@root-system] policy default inter-zone access permit
FGX@root-system] cluster
FGX@root-system-cluster] clusterid 1
FGX@root-system-cluster] local interface eth4
FGX@root-system-cluster] local ip address 1.1.1.1 mask 255.255.255.0
FGX@root-system-cluster] peer ip address 1.1.1.2
FGX@root-system-cluster] end
FGX@root> save config
```

Device2. Default policy, cluster

Do the same as for Device1 on Device2.

7. Access policy = Permit.
8. Interface=eth4, local IP address=1.1.1.2/24, remote IP address=1.1.1.1, cluster ID=1.

CLI

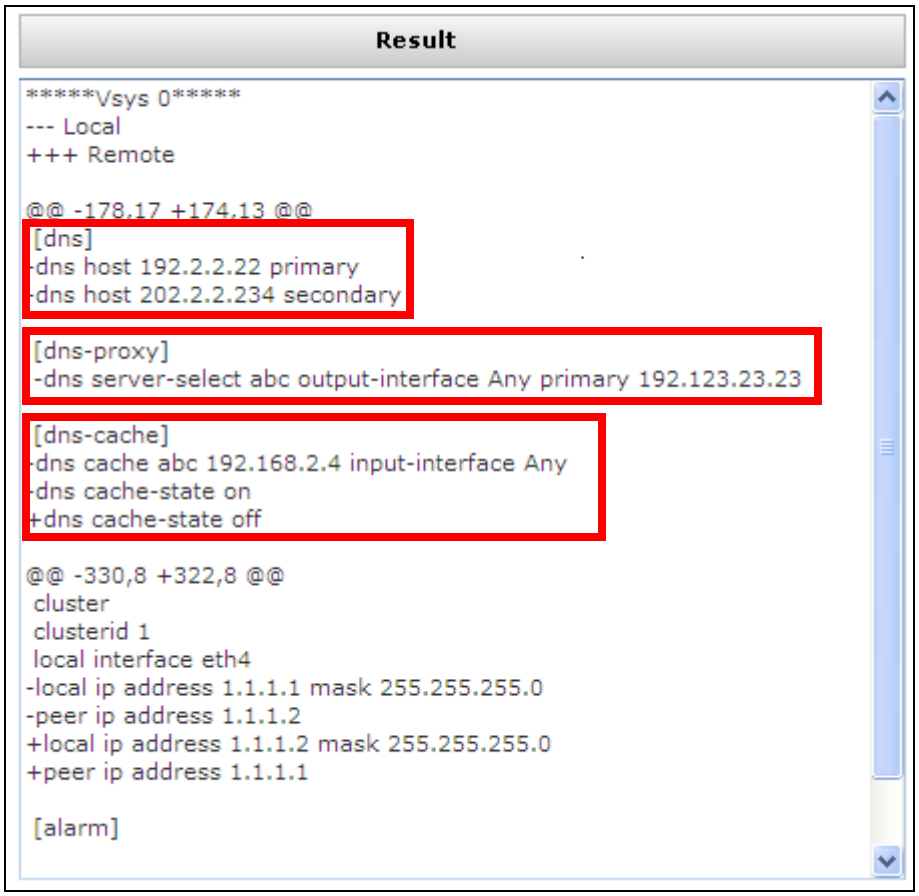
```
FGX@root> configure mode override
FGX@root-system] policy default inter-zone access permit
FGX@root-system] cluster
FGX@root-system-cluster] clusterid 1
FGX@root-system-cluster] local interface eth4
FGX@root-system-cluster] local ip address 1.1.1.2 mask 255.255.255.0
FGX@root-system-cluster] peer ip address 1.1.1.1
FGX@root-system-cluster] end
FGX@root> save config
```

5.2 Check differences between local and remote

On Device1, check the differences between both devices before synchronization.

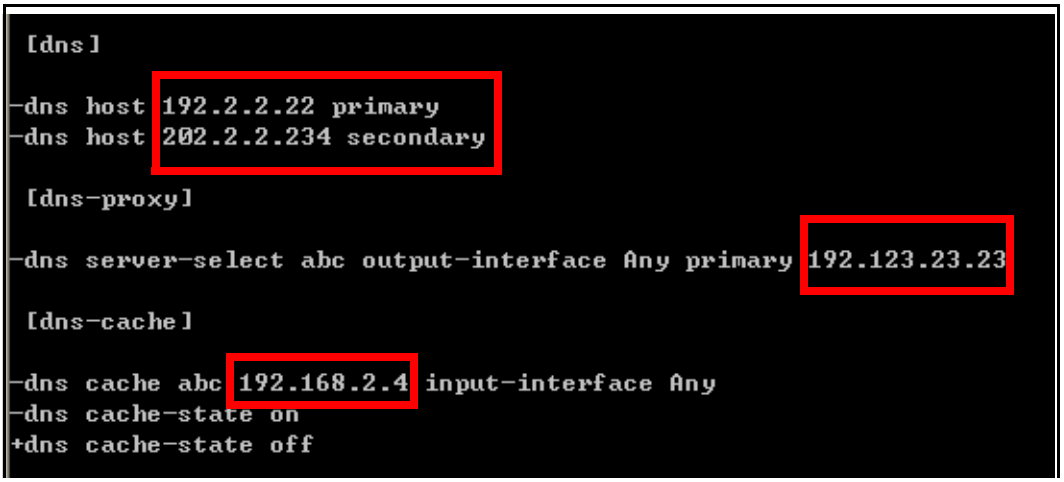
1. Check **View Differences Between Local and Remote Devices**.

2. View the differences. The minus (-) sign indicates local (Device1) and plus (+) indicates remote (Device2).



CLI

Use the **`config check`** command in the Cluster Configuration mode to view differences.

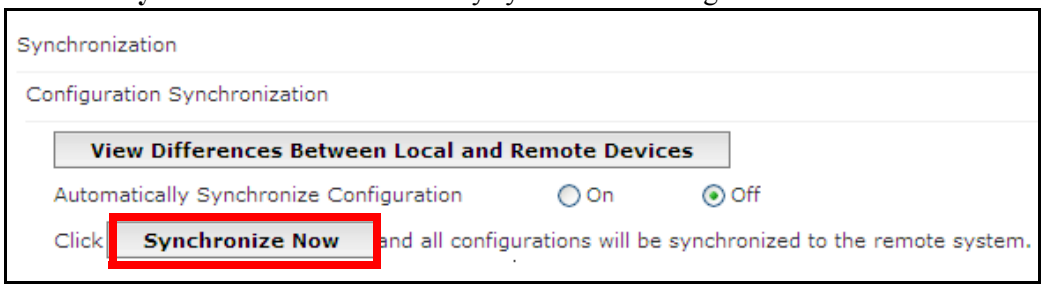


5.3 Synchronize configuration manually

- Device1. Perform manual synchronization
- Device2. View synchronization

Device1. Perform manual synchronization

1. Choose **System > High Availability > Clusters**.
2. Click **Synchronize Now** to manually synchronize configurations on Device1 to Device2.



   Recommended to manually perform a complete synchronization before automatic synchronization so configuration information of Device1 will overwrite that on Device2.

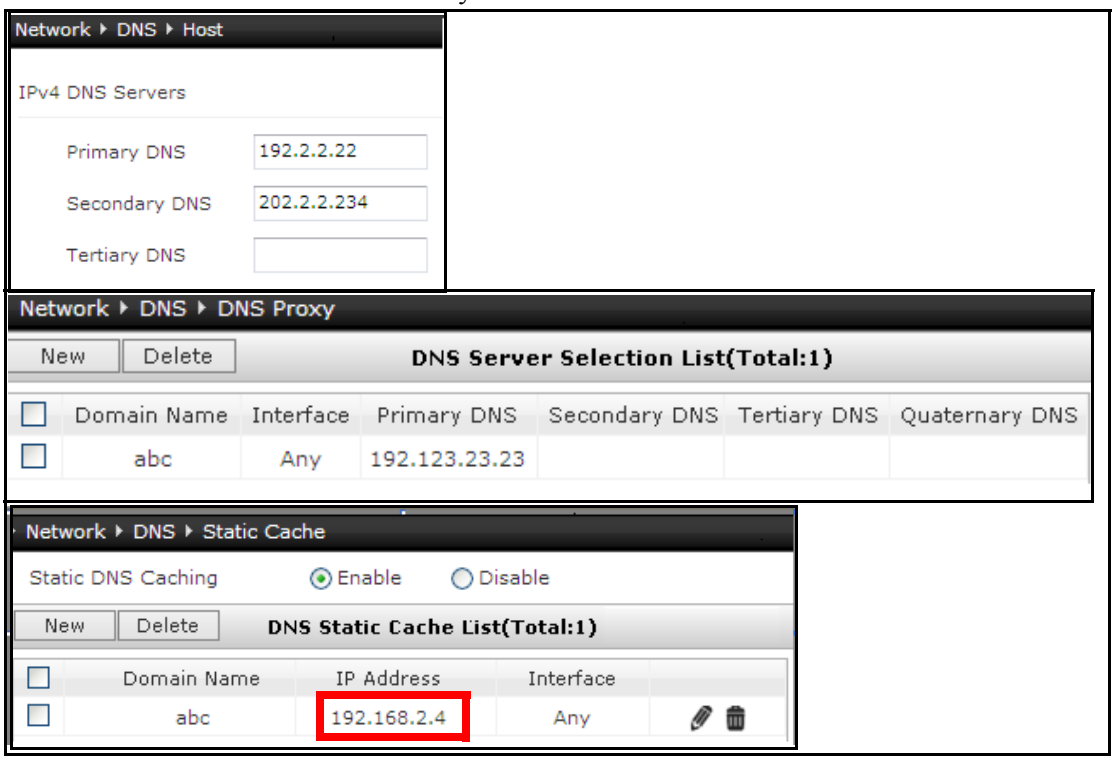
3. Click OK.

CLI

```
FGX@root-system] cluster
FGX@root-system-cluster] cluster 1
FGX@root-system-cluster] config sync
```

Device2. View synchronization

4. Choose **Network > DNS** to view synchronized DNS information.



If you manually synchronize from Device2 to Device1, Device2's configuration will overwrite Device1's. Device1's DNS information will be cleared because Device2 initially has no DNS configurations.

5.4 Synchronize configuration automatically

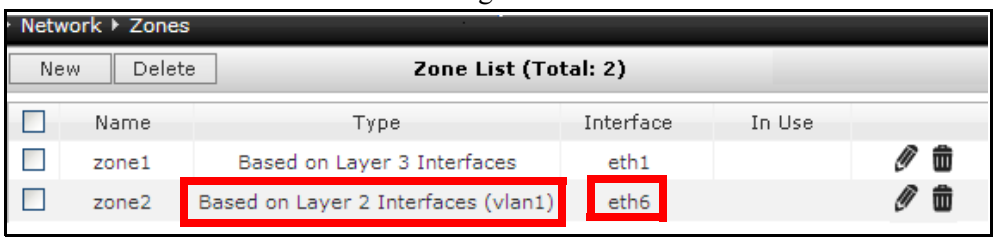
- Device1. Perform automatic synchronization
- Device2. View synchronization

Device1. Perform automatic synchronization

1. Choose **System > High Availability > Clusters**.
2. Click **On** corresponding to **Automatically Synchronize Configuration**.

   - Device1 will automatically synchronize its synchronizable configurations to Device2 even if automatic synchronization is disabled on Device2.
   - If automatic synchronization is enabled on both devices, they will synchronize to each other with synchronizable configurations that they currently have.

3. Click **OK**.
4. Choose **Network > Zones** and configure zones.



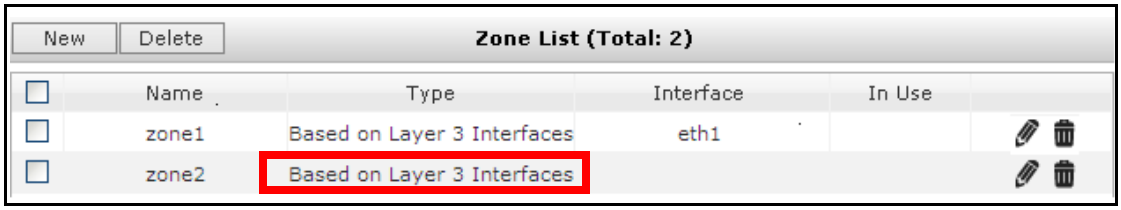
5. Click **OK**.

CLI

```
FGX@root-system] cluster
FGX@root-system-cluster] cluster 1
FGX@root-system-cluster] config sync auto enable
```

Device2. View synchronization

6. Choose **Network > Zones** and view zone information.



Interface (except tunnel interface) configurations cannot be synchronized so zone2 is defaulted to be based on Layer 3 interfaces. For configurations that cannot be synchronized, see 12.1.5.2. Cluster sync info.

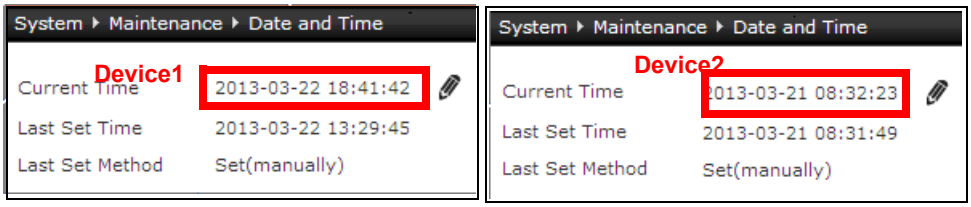
Note: Use the `show zone` command to view zone information in the CLI.

5.5 Synchronize system time

- Device1, Device2. View system time
- Device1. Synchronize time to Device2
- Device1, Device2. View synchronization

Device1, Device2. View system time

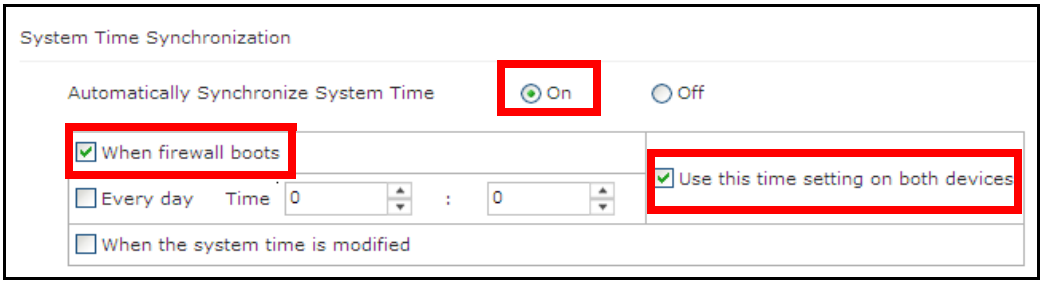
1. Choose **System > Maintenance > Date and Time**.



Note: Use the `show system time` command to view system time in the CLI.

Device1. Synchronize time to Device2

2. Choose **System > High Availability > Clusters**.
3. Enable automatic system time synchronization and set Device1 as the reference point for time synchronization.



- When Device1 boots up, it automatically synchronizes its system time to Device2 even if this function is disabled on Device2. Device2 will get the time synchronized.
- You can only set one device as the reference point of time.

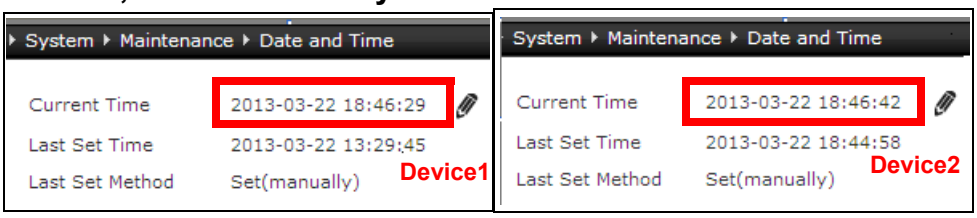
4. Click **OK**.

CLI

```
FGX@root-system] cluster
FGX@root-system-cluster] cluster 1
FGX@root-system-cluster] time sync enable
FGX@root-system-cluster] time boot on
FGX@root-system-cluster] time benchmark on
FGX@root-system-cluster] end
FGX@root> save config
```

5. Choose **System > Maintenance > Date and Time** to view system time on both devices. Now Device1 and 2 have consistent date and time.

Device1, Device2. View synchronization



12.4.Parameter reference

This section describe all the specifics about parameters.

- 12.4.1. Virtual Routers
- 12.4.2. Virtual Router Detection Groups
- 12.4.3. Clusters

12.4.1.Virtual Routers

You can configure virtual routers in the root system and Vsys.

- When a virtual router is removed from a detection group, its priority, interval, and preempt restores to the original.
- A virtual router is always in backup state when it is not configured with any election interface or backup IP address. Once it joins a detection group, the priority of the virtual router will be subtracted from the priority of the group.

Table 254 Parameters of Virtual Routers

Parameter	Description
VRID	The unique identifier of a virtual router. The VRID range is 1-255. You can click the **Generate a VRID Automatically** button on the right, and the system will automatically generate a unique VRID.
Description	Description about a virtual router, 0-255 UTF-8 characters. Cannot contain ?'\"<>&.
Interface	The election interface used for a virtual router. Can be a Layer 3 or shared Layer 3 Ethernet interface, Layer 3 or shared Layer 3 channel, or VLAN interface. The shared Layer 3 interface applies in Vsys.
Group	The ID of the detection group to which a virtual router belongs.
Priority	The priority of a virtual router. The configurable value range is 1-254, 100 by default.
Interval	The interval between advertisements sent by the master. VRRP routers of the same virtual router must have the same interval. 1-60 seconds, 1 second by default.
Preempt	Controls whether a backup device of a higher priority preempts a master device of a lower priority to become the new master. An IP address owner is always in preemption mode. Enabled by default.
Authentication	The simple plain-text authentication of VRRP messages and communication data transmitted between members in a virtual router. Authentication data should be 1-8 UTF-8 characters. Cannot contain ? or spaces. The same authentication data is required for both member devices. Disabled by default.
Enable this virtual router	FGX device will participate in the election of the virtual router. Disabled by default.

Table 254 Parameters of Virtual Routers (*continued*)

Parameter	Description
Backup IP	The backup IP address (es) of a virtual router. Up to 255 addresses supported. When a backup IP address is being used by a VPN tunnel, you cannot delete the address as well as the corresponding virtual router.
IP Tracking	Track whether an IP address is reachable. You can specify the following options: • **Type—**tracking types, include: **•ARP Ping—**sends an ARP request to hosts on the same LAN. **•Ping—**sends an ICMP echo request and listens to the reply. **•TCP Ping—**uses TCP to track IP addresses. • **Interface—**the Layer 3 interface through which tracking messages are sent. You can use: **•Any—**the interface to be used through route lookup. **•Specified interface—**any Layer 3 or shared Layer 3 Ethernet interface, Layer 3 or shared Layer 3 channel, and VLAN interface. • **IP address—**the IP address to be tracked for reachability. • **Track port—**required for TCP Ping only. The port number range is 1-65535. • **Track interval—**the interval between tracking messages. The interval range is 1-30,000 seconds, 3 seconds by default. • **Failure threshold—**maximum failed attempts in a row to send tracking messages. The threshold value range is 1-999, 3 by default. • **Weight—**weight by which the virtual router priority is degraded when IP tracking fails. The weight range is 1-254, 5 by default.
State	The state of a FGX device in a virtual router. Includes Initialize, Master, and Backup.

12.4.2.Virtual Router Detection Groups

You can configure detection groups in the root system and Vsys.

Table 255 Parameters of Detection Groups

Parameter	Description
Group ID	The ID of a detection group, and the ID range is 1-255.
Description	Description about a detection group, 0-255 UTF-8 characters. Cannot contain ?'\"<>&.
Priority	The priority of a detection group. The value range is 1-254, 100 by default.
Interval	The interval between advertisements sent by a detection group. The value range is 1-60 seconds, 1 second by default.
Preempt	Controls whether a detection group of a higher priority preempts that of a lower priority. Enabled by default.
Member	The virtual routers in a detection group. One virtual router can be assigned to one detection group only.
Weight	The weight of a member virtual router by which the priority of the whole detection group is degraded. The value range is 1-254, 5 by default.
IP Tracking	Track whether an IP address is reachable. This function is the same as that for virtual routers. For more information, see Table 254.
State	The state of a member virtual router within a detection group. Includes Initialize, Master, and Backup.

12.4.3.Clusters

You can configure clusters only in the root system.

Table 256 Parameters of Clusters

Parameter	Description
Interface	The HA interface used for synchronization. Can be an unused Layer 2 Ethernet interface or Layer 2 channel.
Local IP Address	The IP address and mask length of the local interface used for synchronization.
Remote IP Address	The IP address of the remote interface used for synchronization.
Cluster ID	The ID of the cluster to which FGX belongs, and the ID range is 1-63. Clustered devices should have the same cluster ID.
Configuration Synchronization	Manually or automatically synchronize configurations to make clustered devices acquire consistent configurations. Before the synchronization, you can click **View Differences Between Local and Remote Devices** to view the differences of configurations. Disabled by default.
Runtime Information Synchronization	Automatically synchronize runtime information to make clustered devices acquire consistent runtime information. After enabling this function, you can check the **Custom Session Information** check box to customize the session information for synchronization. Disabled by default.
System Time Synchronization	Automatically synchronize system time to make clustered devices acquire consistent system time. Enabled by default.
Encryption	Encrypt transmitted data between two devices in a cluster. The same encryption password is required for both local and remote devices. The password should be 1-255 UTF-8 characters. Cannot contain ? or spaces. Disabled by default.
Authentication	Verify the identities of both local and remote devices in a cluster. The same authentication password is required for both clustered devices. The password should be 1-255 UTF-8 characters. Cannot contain ? or spaces. Disabled by default.

13 Virtual Systems

This chapter describes virtual systems (Vsys) functionality.

- 13.1. Overview. Describes Vsys and Vnet concepts and fundamentals.
- 13.2. Basic configuration steps. Describes basic configuration steps and the UI dialogs. Your scenario will not require all of these steps.
- 13.3. Scenarios. Describes real-world threat scenarios and how to solve problems using FGX.
- 13.4. Examples. Gives detailed step-by-step examples.
- 13.5. Parameter reference. Describes in detail all Vsys parameters.

13.1. Overview

FGX system can be divided into multiple virtual systems and the maximum number is determined by the license. You initially login to the root system. Each Vsys works like a virtual device with its own administrators, auditors, policies, user authentication database, and so on. Virtual networks (Vnet) connect virtual systems through virtual interfaces (See 4.5.1 Overview).

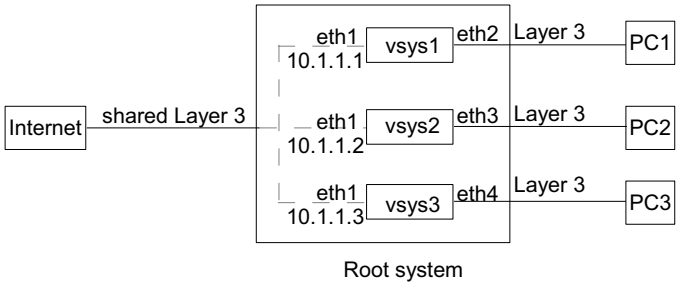
This section includes:

- 13.1.1. Vsys
- 13.1.2. Vnet

13.1.1. Vsys

The following diagram shows how to use Vsys.

Figure 53 Vsys



Use Vsys when you require:

- Separate administrators and

  Vsys administrators are created and managed by administrators. After the root system is divided into multiple virtual systems, Vsys administrators cannot change the network topology or change interface working modes. For details, see 3.13 Administrative Users.

- Separate security configurations.

  Each Vsys has its own settings for attack defense, policies, UTM, and other security functions. UTM functions include Anti-Virus, Anti-Spam, IPS, URL Filtering, and Application Control.

- Resource sharing.

  Session and rule resources (ARP/CAM tables, policies, routes, NAT rules, and profiles) are shared by all VSys.

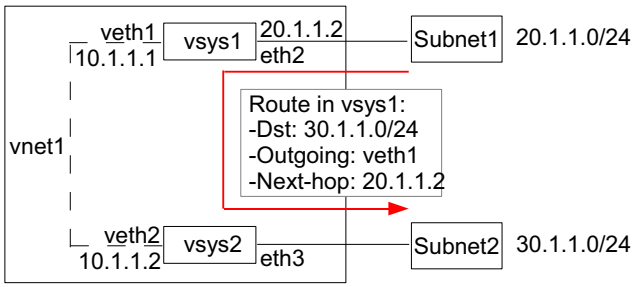
Management IP / interfaces are used to manage a Vsys remotely. If the management interface is:

- A Layer 3 interface, the management IP address can be the same as that of other Vsys or the root system.
- A shared Layer 3 interface, the management IP addresses cannot be the same.

13.1.2. Vnet

The following diagram shows virtual interfaces and networks.

Figure 54 Vnet



- Virtual interfaces
  - Layer 2 virtual interfaces can be assigned to VLAN interfaces, and VLAN interfaces can be assigned to a Vsys.
  - Layer 3 virtual interfaces can be directly assigned to a Vsys.
  - One virtual interface can be assigned to only one Vsys.
- Virtual networks

  Virtual systems connected by virtual interfaces compose a virtual network.

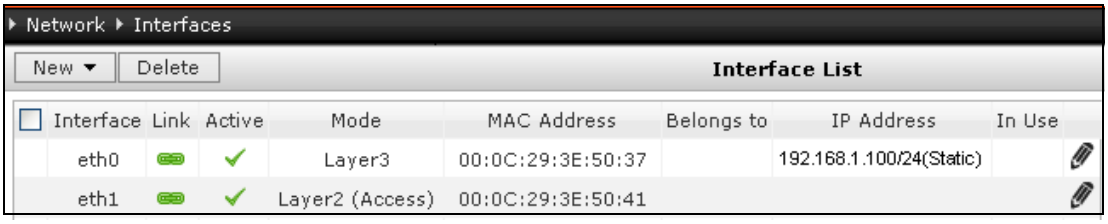
13.2. Basic configuration steps

This section describes the basic configuration procedure.

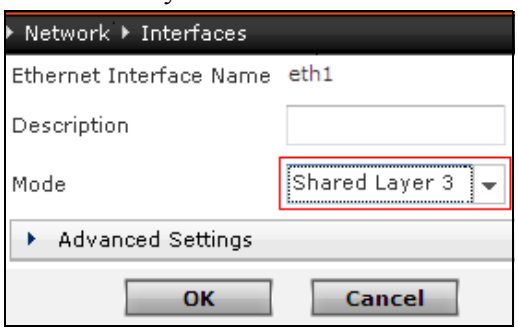
- 13.2.1. Create Layer 3 Interfaces
- 13.2.2. Create Vsys (resources, interfaces, management IP, UTM)
- 13.2.3. Create Vsys administrators
- 13.2.4. Logon to /switch Vsys
- 13.2.5. Manage Vsys
- 13.2.6. Create Vnet

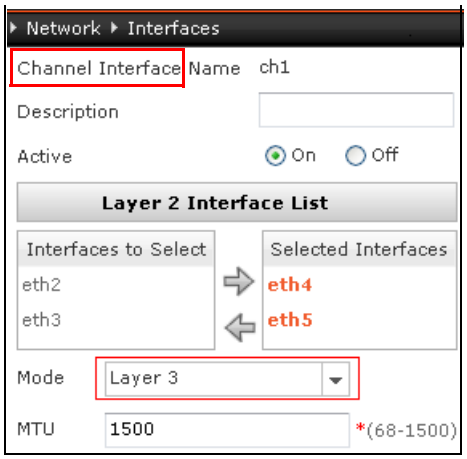
13.2.1. Create Layer 3 Interfaces

1. Choose **Network > Interfaces**.



2. Set Layer 2 interfaces as Layer 3 or shared Layer 3 interfaces, or create new Layer 3 or shared Layer 3 interfaces.





- After Layer 3 interfaces are allocated into Vsys,
  - their MAC addresses, MTU, and IP addresses can only be modified in Vsys (not in the root system).
  - Layer 2 interfaces bound by them cannot be modified in the Vsys (only in the root system).
- After a shared Layer 3 interface is allocated into different Vsys, the IP addresses configured for it in the Vsys cannot be the same, but they can be on the same segment.

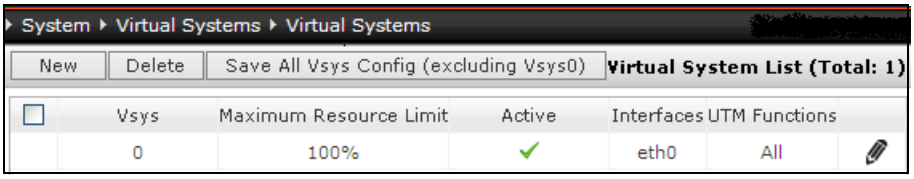
Table 257 Interface Commands

interface ethernet	Enter ethernet interface configuration mode.
working-type layer3-shared-interface	Set interface to shared Layer 3 mode.
channel	Enter channel configuration mode.
hold ethernet	Add Layer 2 interfaces to a channel.

For more interface commands, see **Network Configuration Commands** chapter in *CELESTIX FGX Integrated Security Software v4.2 CLI Reference Guide*.

13.2.2. Create Vsys (resources, interfaces, management IP, UTM)

3. Choose **System > Virtual Systems > Virtual Systems**.



vsys0 is the root system. By default, vsys0 is enabled, its maximum resource limit is 100% (100% indicates that the root system can use all system resources.), all Layer 3 interfaces are assigned to vsys0, and all UTM functions are enabled.

4. Create virtual systems and specify:
   - The max resource limit
   - Layer 3 interfaces
   - Management interface and IP address
   - UTM functions

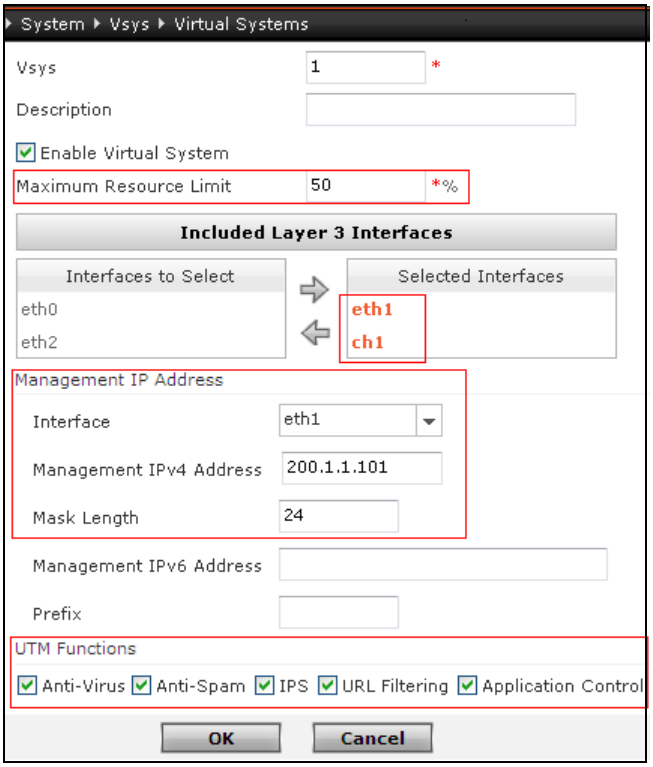


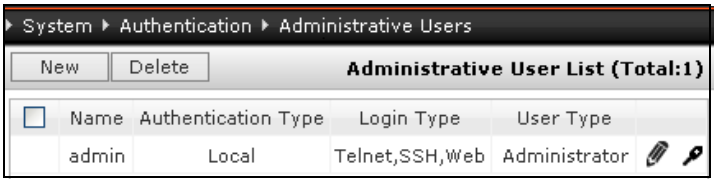
Table 258 Vsys Commands

show vsys [*vsys_id* | **root**]	View Vsys information.
vsys *vsys_id* **resource-limit** *num*	Create a Vsys.
unset vsys [*vsys_id*]	Delete a specified Vsys or all virtual systems.
vsys *vsys_id* **enable**	Enable a specified Vsys.
vsys *vsys_id* **disable**	Disable a specified Vsys.
hold	Add an ethernet, channel, VLAN, rint, veth, or PPPoE interface to a specified Vsys.
unset hold	Delete an ethernet, channel, VLAN, rint, veth, or PPPoE interface from a specified Vsys.
vsys *vsys_id* **resource-limit** *num*	Modify the resource limit for a specified Vsys.
manage-ip-address	Set the management IPv4 address for a specified Vsys.
manage-ipv6-address	Set the management IPv6 address for a specified Vsys.
save all-vsys-config	Save configurations of all virtual systems (except for the root system).
switch vsys *vsys_name*	Switch Vsys.

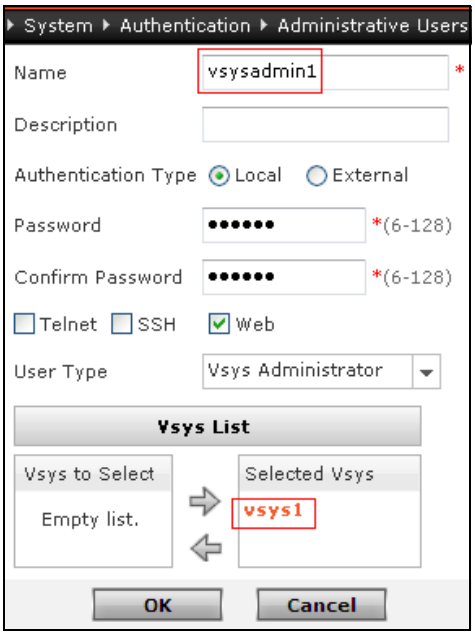
13.2.3. Create Vsys administrators

Administrators of the root system can create Vsys and manage Vsys resources.

5. Click **Administrative Users** or choose **System > Authentication > Administrators**.



6. Create Vsys administrators for Vsys.



7. Assign a Vsys to existing administrators of the root system or existing Vsys administrators. An administrator can be set as the administrator of multiple virtual systems.

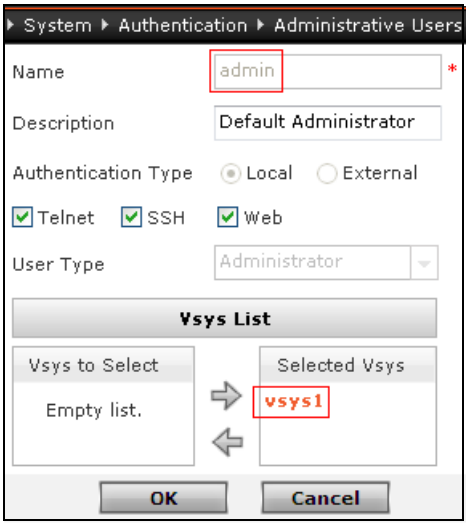


Table 259 Vsys Admin Commands

user administrator *user_name* **vsys-administrator vsys**	Create a Vsys administrator for a specified Vsys.
unset user administrator *user_name*	Delete a Vsys administrator.
user administrator *user_name* **allowed-vsys** *vsys_name*	Add the management permission on a Vsys for a specified administrator or Vsys administrator.
unset user administrator *user_name* **allowed-vsys** *vsys_name*	Remove the management permission of a specified administrator or Vsys administrator on a Vsys.
show user administrator [*user_name*]	Show information about all administrators of the current Vsys.
show line	Show information about all on-line administrators of the current Vsys.

13.2.4. Logon to /switch Vsys

The following lists steps of:

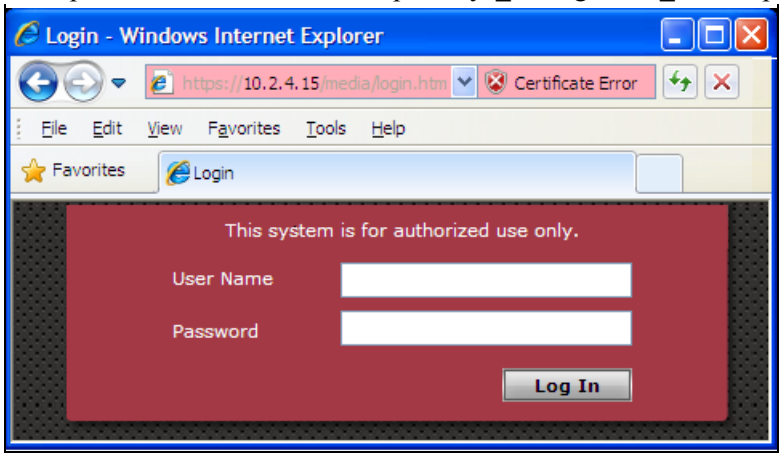
1. Logon through management IP.

2. Logon with CLI.

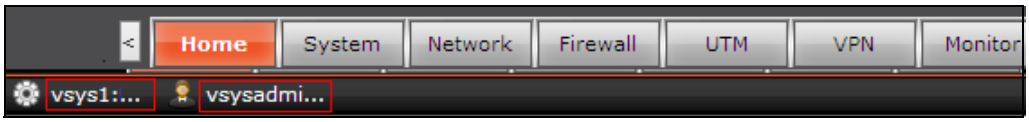
3. Switch Vsys.

To logon through management IP:

8. Open a browser and enter “https://vsys_management_IP” to open the login page of the Vsys.



9. Enter the user name and password to log on to the Vsys.



No command corresponds to these two steps, but you can do the following through the CLI console if the Vsys is assign to an administrator of the root system:

a. Exit the root system.

b. Type the vsys name and then press Enter.

c. Type the user name and password to log on to the Vsys.

Switching Vsys:

Administrators can switch between the root system and managed virtual systems, and Vsys administrators can only switch between managed virtual systems.

10. To switch to a Vsys, click **Switch Vsys** at the bottom of the **Virtual Systems** page to open the **Switch Vsys** page and click corresponding .

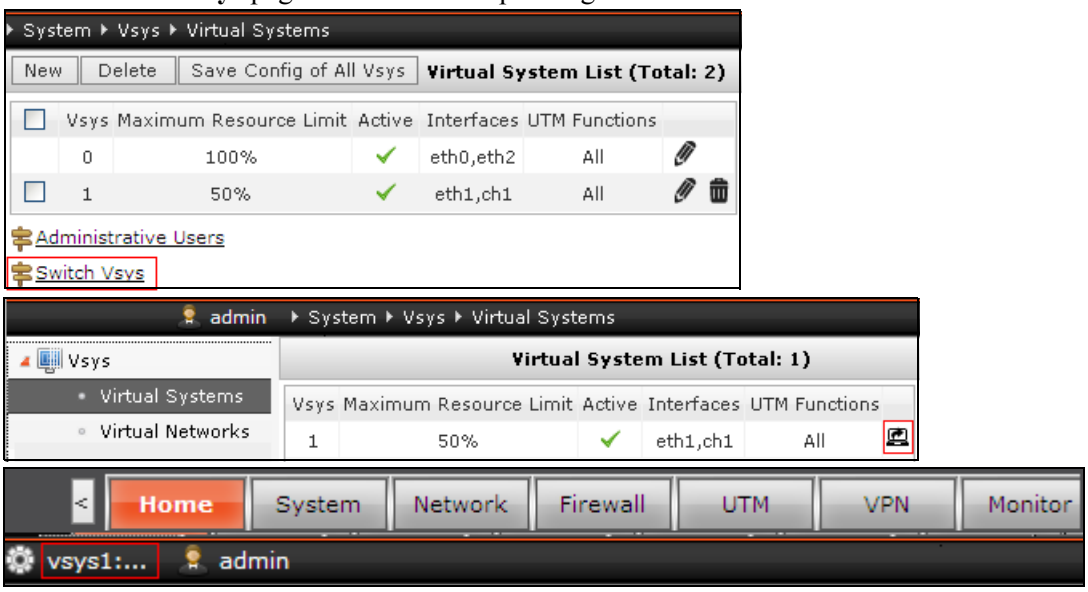


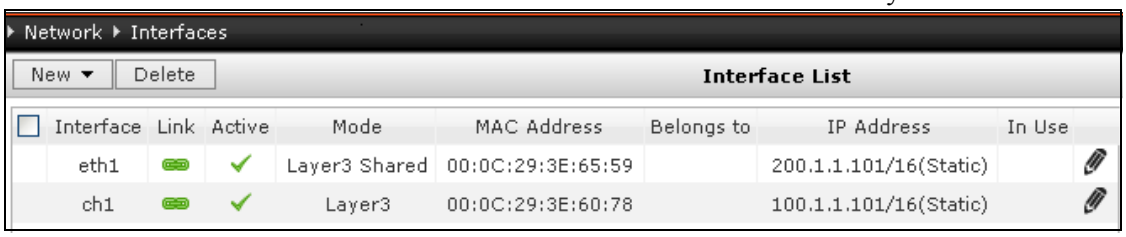
Table 260 Vsys Switch Command

switch vsys *vsys_name*	Switch Vsys.

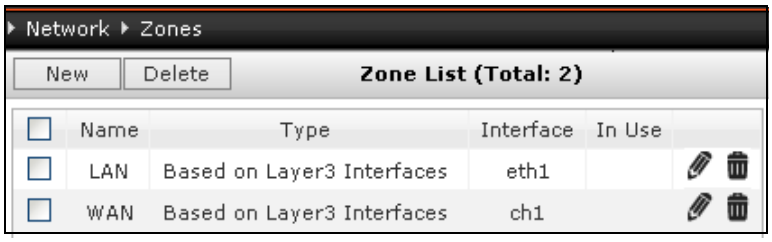
13.2.5. Manage Vsys

The following are the most common management steps required after creating a vsys.

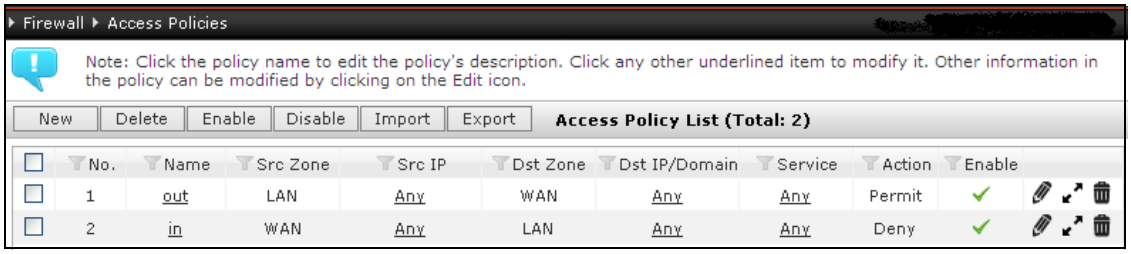
11. Choose **Network > Interfaces** and set interface IP addresses for the Vsys.



12. Choose **Network > Zones** and create zones.



13. Choose **Firewall > Access Policies** and create access policies to allow access through the Vsys.



14. Customize other functions in the Vsys. For details, see section 13.5.3. Functions Configurable in Vsys.

- Configurable only in the root vsys:
  - Anti-Virus, Anti-Spam and IPS profiles.
  - Updating the anti-virus rules, anti-spam rules, attack signature rules, URL filtering rules, and application list.
- Configurable in any vsys:
  - URL Filtering and Application Control profiles.
  - Sharing the UTM updates of the root system.
- No default UTM policies are provided in Vsys.

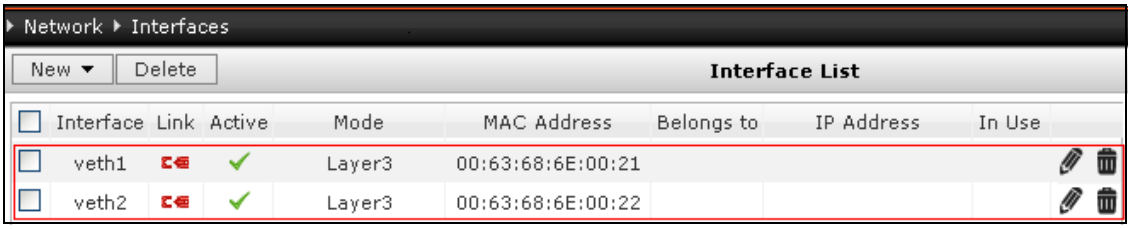
Table 261 Zone and Access Policy Commands

zone *zone_name*	Create a zone.
zone based-layer3	Configure a zone based on Layer 3 interfaces or shared Layer 3 interfaces.
policy access	Adds an access policy.

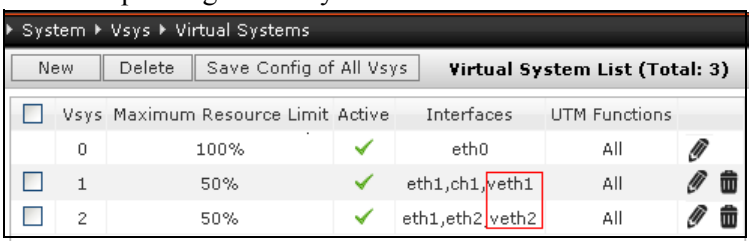
13.2.6. Create Vnet

15. Switch to the root system and choose a working mode. See section 13.3. Scenarios for details about working modes. (You can configure virtual networks only in the root system.)

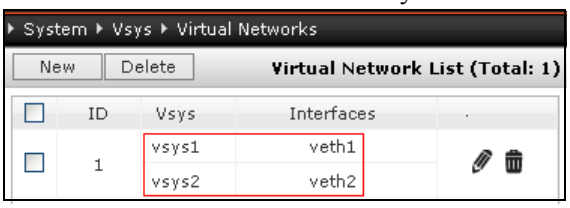
16. Choose **Network > Interfaces** and create Layer 3 virtual interfaces.



17. Choose **System > Virtual Systems > Virtual Systems** and allocate virtual interfaces to corresponding virtual systems.



18. Choose **System > Virtual Systems > Virtual Networks**, create virtual networks, and assign virtual interfaces and virtual systems to virtual networks.



19. Create access policies in Vsys for communication between Vsys. See 8.2.2 Create Access Policy.

20. Create static routes for communication between Vsys working in routing mode. See 6.2.1 L3 Unicast.

Table 262 Vnet Commands

vnet *vnet_id*	Create a virtual network.
unset vnet *vnet_id*	Delete a virtual network.
hold veth *veth_id*	Assign a virtual interface to a virtual network.
unhold veth *veth_id*	Delete a virtual interface from a virtual network.
description [*string*]	Add, modify, or delete description about a virtual network.
show vnet [*vnet_id* | **brief**]	View virtual network information.

For access policy and routing commands, see **Policies Commands** and **Routing Commands** chapters in *CELESTIX FGX Integrated Security Software v4.2 CLI Reference Guide*.

13.3. Scenarios

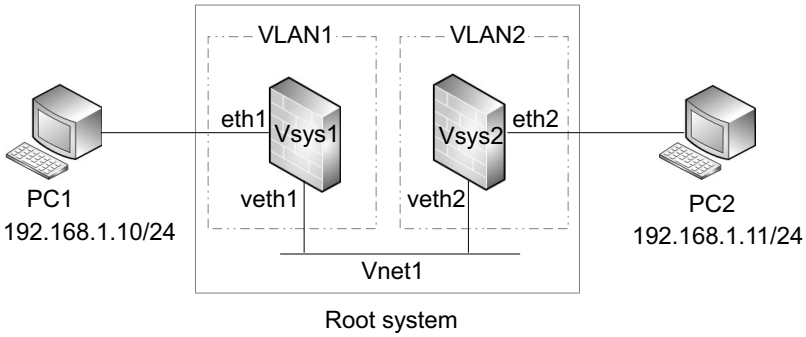
A virtual system supports the same working modes that a device does:

- 1. Transparent Mode
- 2. Routing Mode
- 3. Hybrid Mode

1. Transparent Mode

The transparent mode is mainly used for Layer 2 data forwarding.

Figure 55 Transparent Mode Typical Topology



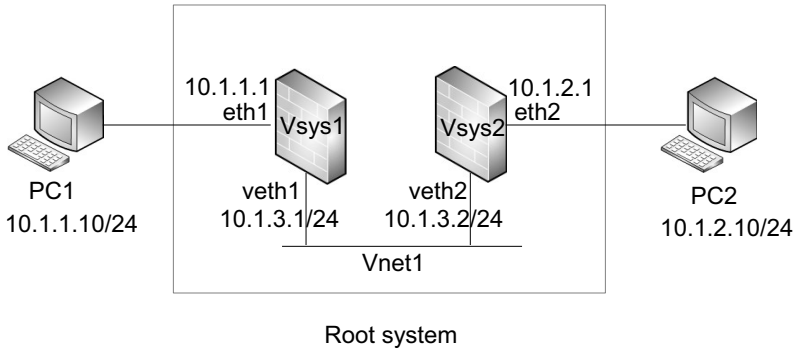
Configuration steps for the above example are:

1. Allocate eth1 and veth1 to VLAN1.
2. Allocate VLAN1 to Vsys1.
3. Allocate eth2 and veth2 to VLAN2.
4. Allocate VLAN2 to Vsys2.
5. Create virtual network Vnet1.
6. Allocate veth1 and Vsys1 to Vnet1.
7. Allocate veth2 and Vsys2 to Vnet1.
8. Configure access policies in Vsys1 and Vsys2 to allow communication between PC1 and PC2.

2. Routing Mode

The routing mode is used to allow hosts on different network segments to communicate with each other through Layer 3 routing. Interfaces must be on different segments, and you need to set IP addresses for those interfaces.

Figure 56 Routing Mode Typical Topology



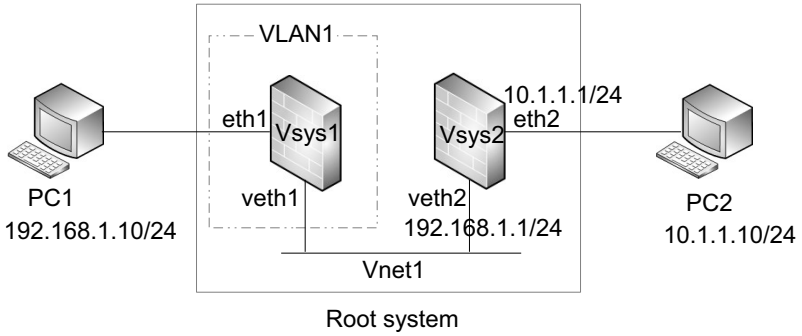
Configuration steps for the above example are:

1. Set eth1 and eth2 to Layer 3 interfaces, and create Layer 3 virtual interfaces veth1 and veth2;
2. Create virtual system Vsys1, and allocate eth1 and veth1 to Vsys1;
3. Create virtual system Vsys2, and allocate eth2 and veth2 to Vsys2;
4. In vsys1, set the IP address of eth1 to 10.1.1.1/24 and that of veth1 to 10.1.3.1/24;
5. In vsys2, set the IP address of eth2 to 10.1.2.1/24 and that of veth2 to 10.1.3.2/24;
6. Create virtual network Vnet1, allocate veth1 and Vsys1 to Vnet1, and allocate veth2 and Vsys2 to Vnet1;
7. Configure access policies in Vsys1 and Vsys2 to allow communication between PC1 and PC2;
8. Configure a static route to PC2 in Vsys1 with 10.1.3.2 as the next gateway and another one to PC1 in Vsys2 with 10.1.3.1 as the next gateway.
9. Set the gateway of PC1 to 10.1.1.1; set the gateway of PC2 to 10.1.2.1.

3. Hybrid Mode

The hybrid mode implement Layer 2 forwarding and Layer 3 routing.

Figure 57 Hybrid Mode Typical Topology



Configuration steps for the above example are:

1. Allocate veth1 and eth1 to VLAN1 and VLAN1 to Vsys1;
2. Set eth2 to a Layer 3 interface, create a Layer 3 virtual interface veth2, and then allocate eth2 and veth2 to Vsys2;
3. In Vsys2, set the IP address of eth2 as 10.1.1.1/24 and that of veth2 as 192.168.1.1/24;
4. Create a virtual network Vnet1, allocate veth1 and Vsys1 to Vnet1, and allocate veth2 and Vsys2 to Vnet1;
5. Configure access policies in Vsys1 and Vsys2 to allow communication between PC1 and PC2;
6. Set the gateway of PC1 to 192.168.1.1, and set the gateway of PC2 to 10.1.1.1.

13.4. Examples

This section gives two examples:

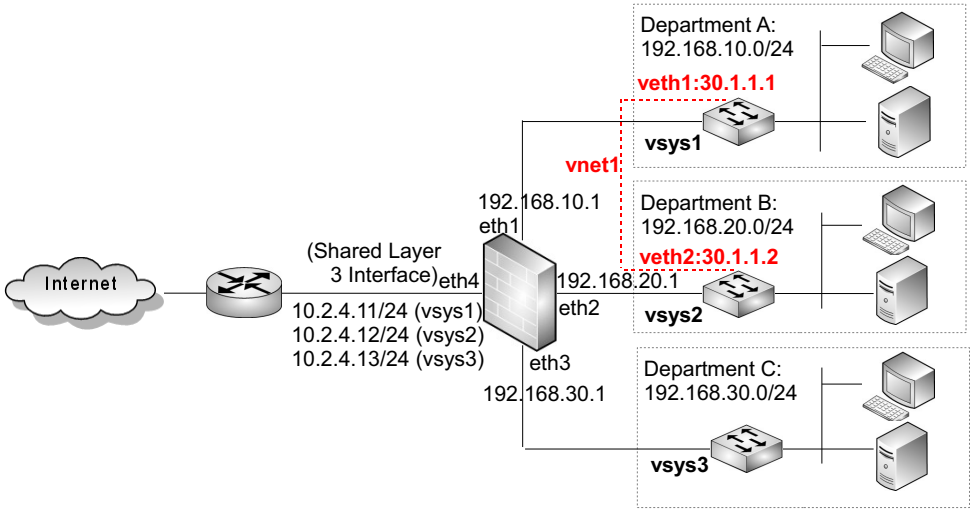
- Example 1: Multi-Vsys Based on Shared Layer 3 Interface
- Example 2: Multi-Vsys Based on Trunk Interface

Example 1: Multi-Vsys Based on Shared Layer 3 Interface

As shown below, a company has departments A, B, and C. They are located on different network segments, but they have different security requirements and there is only one Ethernet interface connected to the Internet.

- To allow each department to have their own security settings, create a Vsys for each department.
- To enable the departments to access the Internet, set the outgoing interface as a shared Layer 3 interface.
- Create a private network between A and B by creating a virtual network connecting the A and B vsys.

Figure 58 Multi-Vsys Based on Shared Layer 3 Interface

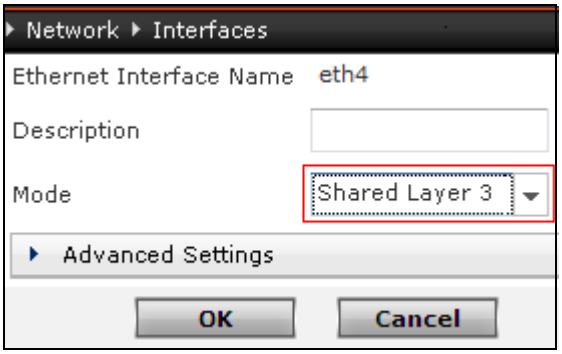


Configuration steps include:

1. Create Layer 3 Interfaces
2. Create Vsys and assign interfaces
3. Assign Vsys 1-3 to admin
4. Configure Vsys
5. Create Virtual Network
6. Create Vsys Administrators
7. Set Vsys Management IP Addresses

1. Create Layer 3 Interfaces

1. Choose **Network > Interfaces**, set eth4 as a shared Layer 3 interface:



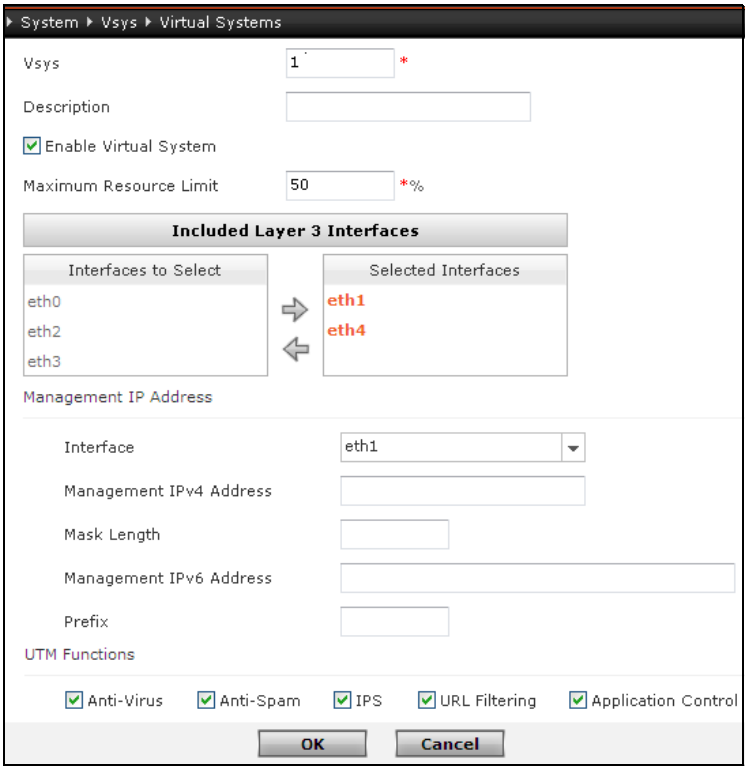
2. Click **OK**.
3. Set eth1, eth2, and eth3 to Layer 3 interfaces.
4. Click  .

CLI

```
FGX@root> configure mode override
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] working-type layer3-interface
FGX@root-system-if-eth1] exit
FGX@root-system] interface ethernet 2
FGX@root-system-if-eth2] working-type layer3-interface
FGX@root-system-if-eth2] exit
FGX@root-system] interface ethernet 3
FGX@root-system-if-eth3] working-type layer3-interface
FGX@root-system-if-eth3] exit
FGX@root-system] interface ethernet 4
FGX@root-system-if-eth4] working-type layer3-shared-interface
FGX@root-system-if-eth4] exit
FGX@vsys1-system] end
FGX@vsys1> save config
```

2. Create Vsys and assign interfaces

1. Choose **System > Virtual Systems > Virtual Systems**, create virtual system vsys1, and assign eth1 and eth4 to vsys1:



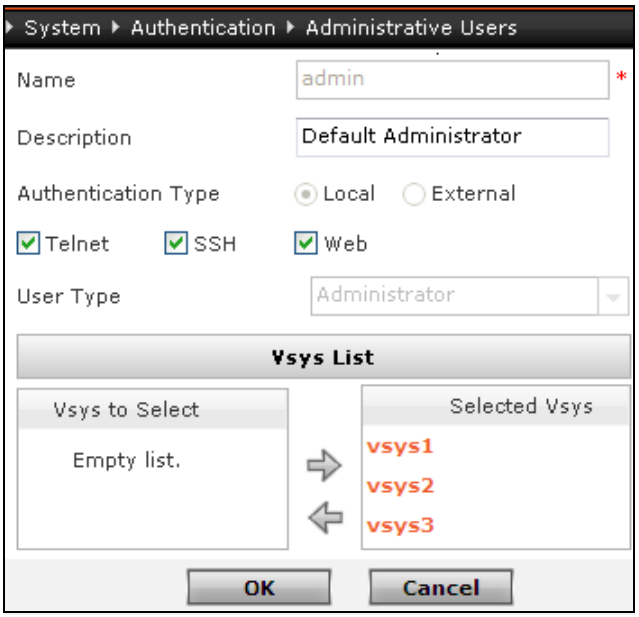
2. Click **OK**.
3. Create virtual system vsys2 and assign eth2 and eth4 to vsys2, and create virtual system vsys3 and assign eth3 and eth4 to vsys3.
4. Click  .

CLI

```
FGX@root> configure mode override
FGX@root-system] vsys 1 resource-limit 50
FGX@root-system-vsys1] hold ethernet 1
FGX@root-system-vsys1] hold ethernet 4
FGX@root-system-vsys1] exit
FGX@root-system] vsys 2 resource-limit 50
FGX@root-system-vsys2] hold ethernet 2
FGX@root-system-vsys2] hold ethernet 4
FGX@root-system-vsys2] exit
FGX@root-system] vsys 3 resource-limit 50
FGX@root-system-vsys3] hold ethernet 3
FGX@root-system-vsys3] hold ethernet 4
FGX@root-system-vsys3] exit
FGX@vsys1-system] end
FGX@vsys1> save config
```

3. Assign Vsys 1-3 to admin

1. Choose **System > Authentication > Administrative Users**, click corresponding to admin to open the **Edit** page, and add vsys1, vsys2, and vsys3 to the managed Vsys list:



2. Click **OK**.
3. Click .

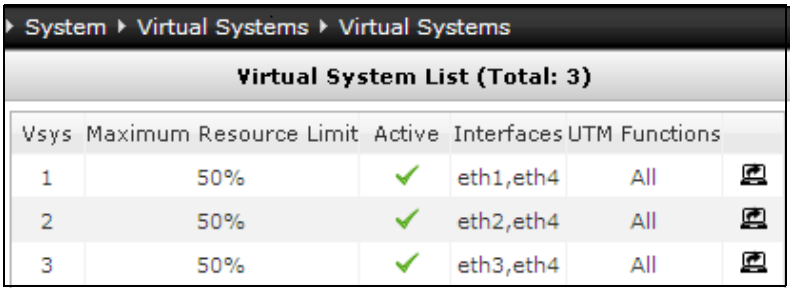
CLI

```
FGX@root> configure mode override
FGX@root-system] user administrator admin allowed-vsys vsys1
FGX@root-system] user administrator admin allowed-vsys vsys2
FGX@root-system] user administrator admin allowed-vsys vsys3
FGX@root-system] end
FGX@root> save config
```

4. Configure Vsys

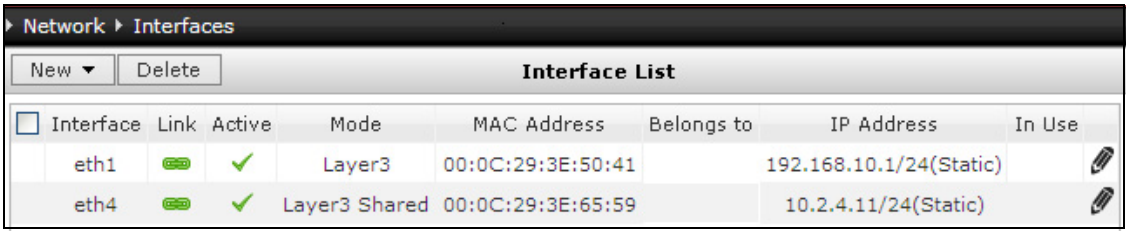
WebUI

1. Choose **System > Virtual Systems > Virtual Systems**, click **Switch Vsys**.

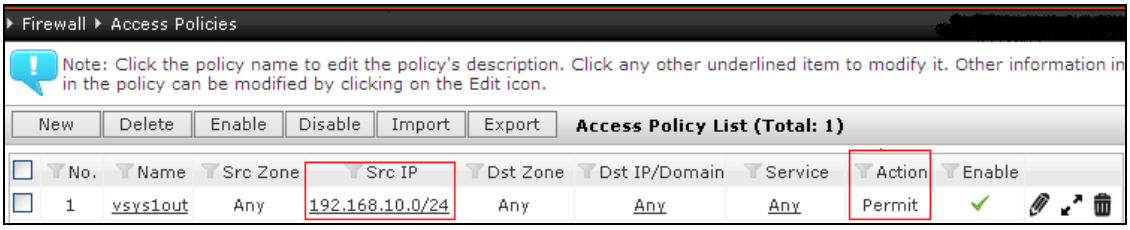


2. Click  corresponding to Vsys 1 to switch to vsys1:

   a. Choose **Network > Interfaces**, and set the IP address of eth1 to 192.168.10.1/24 and that of eth4 to 10.2.4.11/24:



   b. Choose **Firewall > Access Policies**, and add an access policy named vsys1out to permit access from 192.168.10.0/24 to any:



3. Switch to vsys2:

   a. Choose **Network > Interfaces**, and set the IP address of eth2 to 192.168.20.1/24 and that of eth4 to 10.2.4.12/24.

   b. Choose **Firewall > Access Policies**, add an access policy named vsys2out to permit access from 192.168.20.0/24 to any.

4. Switch to vsys3:

   a. Choose **Network > Interfaces**, and set the IP address of eth3 to 192.168.30.1/24 and that of eth4 to 10.2.4.13/24.

   b. Choose **Firewall > Access Policies**, add an access policy named vsys3out to permit access from 192.168.30.0/24 to any.

5. Click  .

CLI

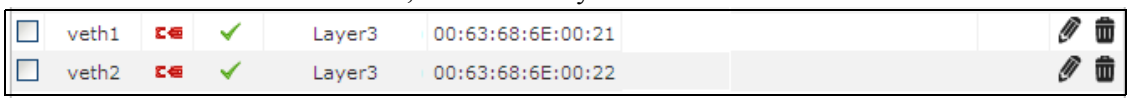
```
FGX@root> switch vsys vsys1
FGX@vsys1> configure mode override
FGX@vsys1-system] interface ethernet 1
FGX@vsys1-system-if-eth1] ip address 192.168.10.1 255.255.255.0
FGX@vsys1-system-if-eth1] exit
FGX@vsys1-system] interface ethernet 4
FGX@vsys1-system-if-eth4] ip address 10.2.4.11 255.255.255.0
FGX@vsys1-system-if-eth4] exit
FGX@vsys1-system] policy access vsys1out any 192.168.10.0/24 any any
any any permit enable
FGX@vsys1-system] end
FGX@vsys1> save config
FGX@vsys1> switch vsys vsys2
FGX@vsys2> configure mode override
FGX@vsys2-system] interface ethernet 2
FGX@vsys2-system-if-eth2] ip address 192.168.20.1 255.255.255.0
FGX@vsys2-system-if-eth2] exit
FGX@vsys2-system] interface ethernet 4
FGX@vsys2-system-if-eth4] ip address 10.2.4.12 255.255.255.0
FGX@vsys2-system-if-eth4] exit
FGX@vsys2-system] policy access vsys2out any 192.168.20.0/24 any any
any any permit enable
FGX@vsys2-system] end
FGX@vsys2> save config
FGX@vsys2> switch vsys vsys3
FGX@vsys3> configure mode override
FGX@vsys3-system] interface ethernet 3
FGX@vsys3-system-if-eth3] ip address 192.168.30.1 255.255.255.0
FGX@vsys3-system-if-eth3] exit
FGX@vsys3-system] interface ethernet 4
FGX@vsys3-system-if-eth4] ip address 10.2.4.13 255.255.255.0
FGX@vsys3-system-if-eth4] exit
FGX@vsys3-system] policy access vsys3out any 192.168.30.0/24 any any
any any permit enable
FGX@vsys3-system] end
FGX@vsys3> save config
```

5. Create Virtual Network

- 5.1. Create virtual interfaces
- 5.2. Allocate virtual interfaces to Vsys
- 5.3. Create Virtual Network
- 5.4. Set virtual interface IP, static routes, and access policies in Vsys

5.1. Create virtual interfaces

1. Choose **System > Virtual Systems > Virtual Systems** and click corresponding to Vsys 0 to switch to the root system.
2. Choose **Network > Interfaces**, create two Layer 3 virtual interfaces named veth1 and veth2.



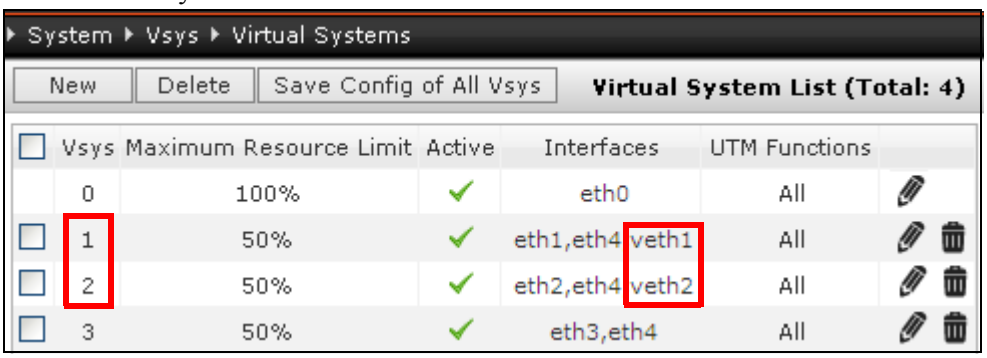
3. Click .

CLI

```
FGX@vsys4> switch vsys root
FGX@root> configure mode override
FGX@root-system] veth 1
FGX@root-system-veth1] working-type layer3-interface
FGX@root-system-veth1] exit
FGX@root-system] veth 2
FGX@root-system-veth2] working-type layer3-interface
FGX@root-system-veth2] end
FGX@root> save config
```

5.2. Allocate virtual interfaces to Vsys

1. Choose **System > Virtual Systems > Virtual Systems**, and allocate veth1 to vsys1 and veth2 to vsys2.



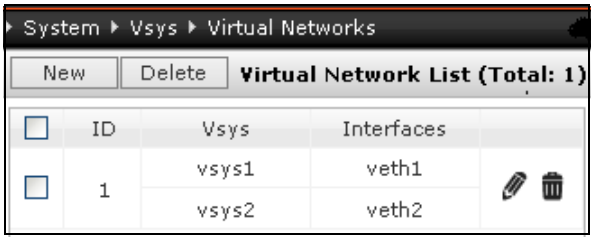
2. Click .

CLI

```
FGX@root> configure mode override
FGX@root-system] vsys 1
FGX@root-system-vsys1] hold veth 1
FGX@root-system-vsys1] exit
FGX@root-system] vsys 2
FGX@root-system-vsys2] hold veth 2
FGX@root-system-vsys2] end
FGX@root> save config
```

5.3. Create Virtual Network

1. Choose **System > Virtual Systems > Virtual Networks**, create a new virtual network named vnet1, assign vsys1 and veth1 to vnet1, and assign vsys2 and veth2 to vnet1:



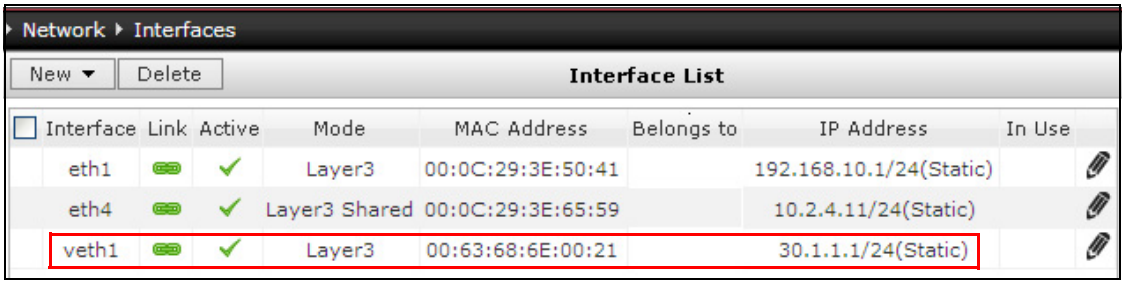
2. Click  .

CLI

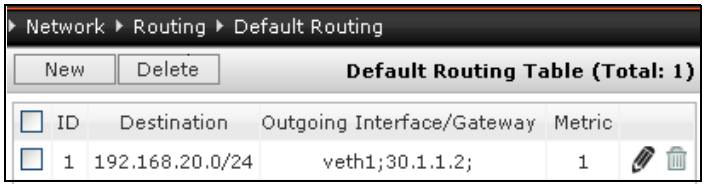
```
FGX@root> configure mode override
FGX@root-system] vnet 1
FGX@root-system-vnet1] hold veth 1
FGX@root-system-vnet1] hold veth 2
FGX@root-system-vnet1] end
FGX@root> save config
```

5.4. Set virtual interface IP, static routes, and access policies in Vsys

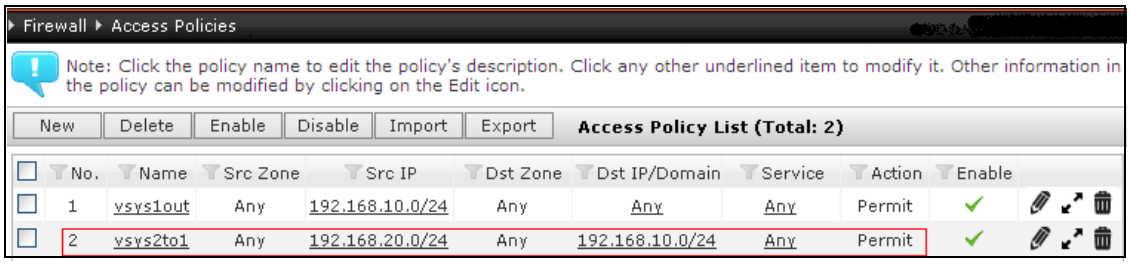
1. Choose **System > Virtual Systems > Virtual Systems**, click **Switch Vsys** at the bottom of the page, and click  corresponding to Vsys 1 to switch to vsys1.
2. Choose **Network > Interfaces**, and set the IP address of veth1 to 30.1.1.1/24:



3. Choose **Network > Routing > Default Routing**, and add a static route to 192.168.20.0/24 with veth1 as the outgoing interface and 30.1.1.2 as the next-hop gateway:



4. Choose **Firewall > Access Policies**, and add an access policy named vsys2to1 to permit access from 192.168.20.0/24 to 192.168.10.0/24:



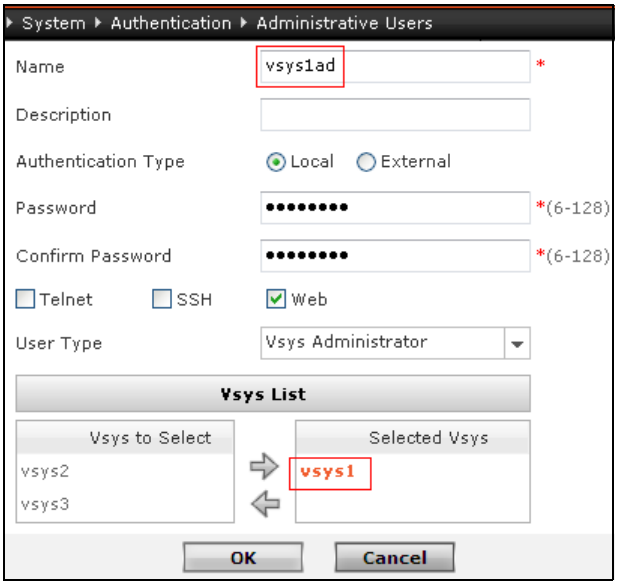
5. Switch to vsys2:
   a. Choose **Network > Interfaces**, and set the IP address of veth2 to 30.1.1.2/24.
   b. Choose **Network > Routing > Default Routing**, and add a static route to 192.168.10.0/24 with veth2 as the outgoing interface and 30.1.1.1 as the next gateway.
   c. Choose **Firewall > Access Policies**, and add an access policy named vsys1to2 to permit access from 192.168.10.0/24 to 192.168.20.0/24.
6. Click .

CLI

```
FGX@root> switch vsys vsys1
FGX@vsys1> configure mode override
FGX@vsys1-system] veth 1
FGX@vsys1-system-veth1] ip address 30.1.1.1 255.255.255.0
FGX@vsys1-system-veth1] exit
FGX@vsys1-system] route 192.168.20.0 255.255.255.0 interface veth1
gateway 30.1.1.2
FGX@vsys1-system] policy access vsys2to1 any 192.168.20.0 any
192.168.10.0 any any permit enable
FGX@vsys1-system] end
FGX@vsys1> save config

FGX@vsys1> switch vsys vsys2

FGX@vsys2> configure mode override

FGX@vsys2-system] veth 2

FGX@vsys2-system-veth2] ip address 30.1.1.2 255.255.255.0

FGX@vsys2-system-veth2] exit

FGX@vsys2-system] route 192.168.10.0 255.255.255.0 interface veth2
gateway 30.1.1.1

FGX@vsys2-system] policy access vsys1to2 any 192.168.10.0 any
192.168.20.0 any any permit enable

FGX@vsys2-system] end

FGX@vsys2> save config
```

6. Create Vsys Administrators

1. Choose **System > Virtual Systems > Virtual Systems**, click corresponding to Vsys 0 to switch to the root system.
2. Choose **System > Authentication**, create Vsys administrators vsys1ad for vsys1 and set the password to test_123.



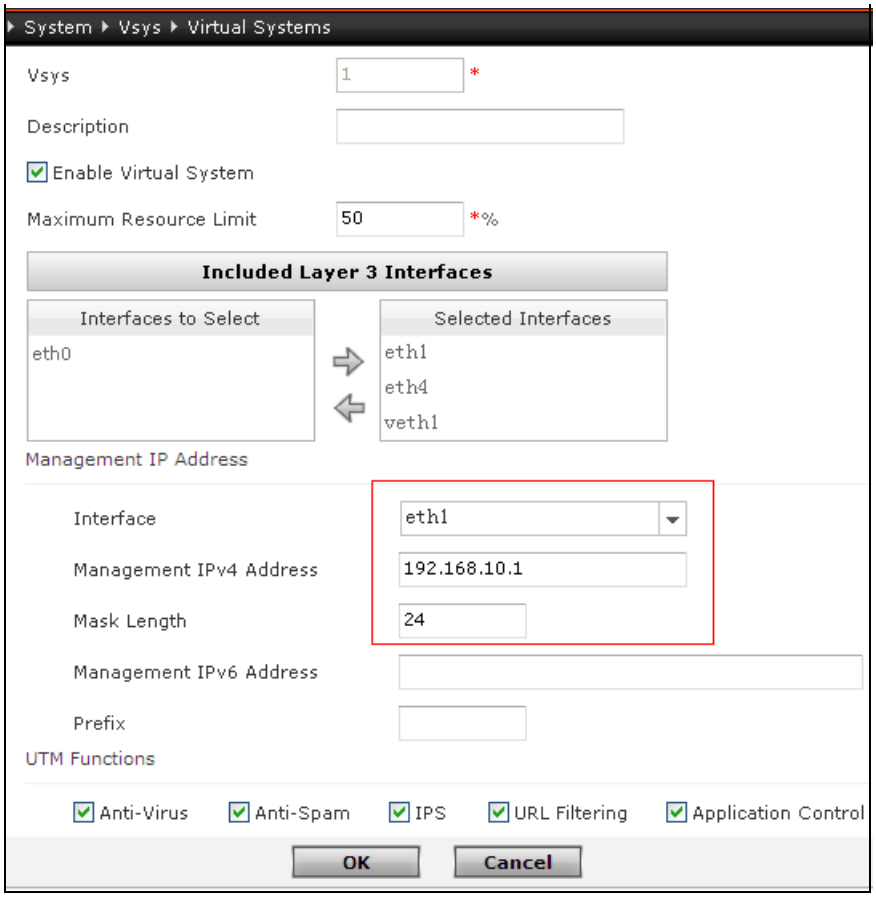
3. Click **OK**.
4. Create vsys2ad for vsys2, and vsys3ad for vsys3.
5. Click .

CLI

```
FGX@vsys2> switch vsys root
FGX@root> configure mode override
FGX@root-system] user administrator vsys1ad vsys-administrator vsys
vsys1 authtype local password simple
Password(6-128): <test_123>
Repeat Password(6-128): <test_123>
FGX@root-system] user administrator vsys1ad logintype web,ssh,telnet
FGX@root-system] user administrator vsys2ad vsys-administrator vsys
vsys2 authtype local password simple
Password(6-128): <test_123>
Repeat Password(6-128): <test_123>
FGX@root-system] user administrator vsys2ad logintype web,ssh,telnet
FGX@root-system] user administrator vsys3ad vsys-administrator vsys
vsys3 authtype local password simple
Password(6-128): <test_123>
Repeat Password(6-128): <test_123>
FGX@root-system] user administrator vsys3ad logintype web,ssh,telnet
FGX@root-system] end
FGX@root> save config
```

7. Set Vsys Management IP Addresses

1. Choose **System > Virtual Systems > Virtual Systems**, click corresponding to Vsys 1 to open the **Edit** page, and set the management interface as eth1 and management IP address as 192.168.10.1/24:



2. Click **OK**.
3. Set the management interfaces and IP addresses of vsys 2 and 3 in the same way:
   - vsys2: eth2, 192.168.20.1/24.
   - vsys3: eth3, 192.168.30.1/24.
4. Click .
5. Log on to the Vsys in the same way as you log on to the root system and manage the Vsys.

Note: If you want to use Ping to test the network connection, you need to log on to each Vsys and enable the Ping service.

CLI

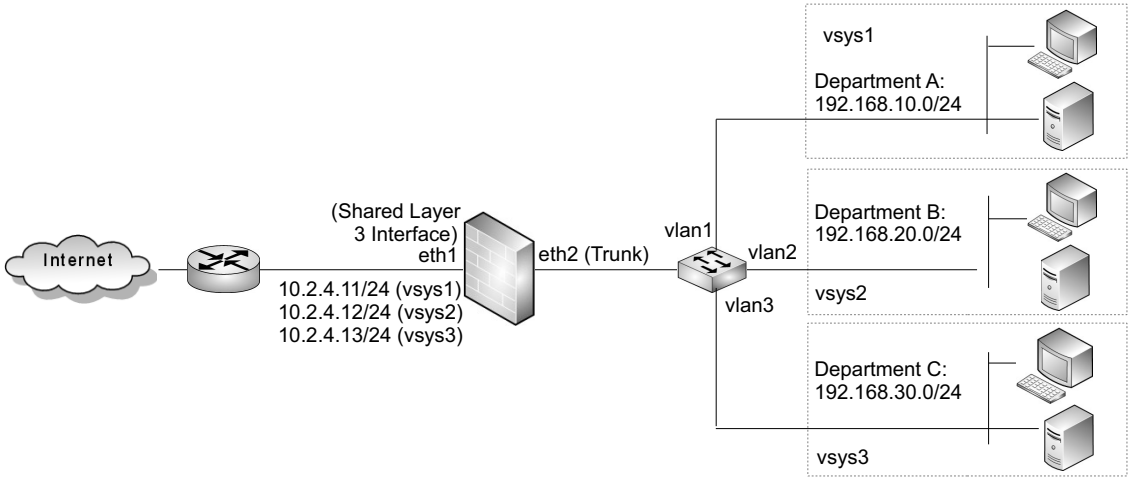
```
FGX@root> configure mode override
FGX@root-system] vsys 1
FGX@root-system-vsys1] manage-ip-address 192.168.10.1 255.255.255.0
ethernet 1
FGX@root-system-vsys1] exit
FGX@root-system] vsys 2
FGX@root-system-vsys2] manage-ip-address 192.168.20.1 255.255.255.0
ethernet 2
FGX@root-system-vsys2] exit
FGX@root-system] vsys 3
FGX@root-system-vsys3] manage-ip-address 192.168.30.1 255.255.255.0
ethernet 3
FGX@root-system-vsys4] end
FGX@root> save config
```

Example 2: Multi-Vsys Based on Trunk Interface

As shown below, a company has departments: A, B, and C. They are located on different network segments and they have different security configurations.

- To allow these three departments to have their own security settings, create a Vsys for each department.
- To enable three departments to access the Internet simultaneously, set the outgoing interface as a shared Layer 3 interface, and set the incoming interface as a Layer 2 Trunk interface.

Figure 59 Multi-Vsys Based on Trunk Interface



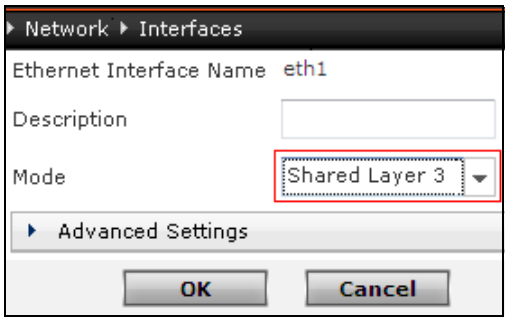
Configuration steps include:

1. Create Layer 3 Interfaces
2. Create Vsys
3. Assign Vsys to admin
4. Set Interface IP and Access Policy for Vsys

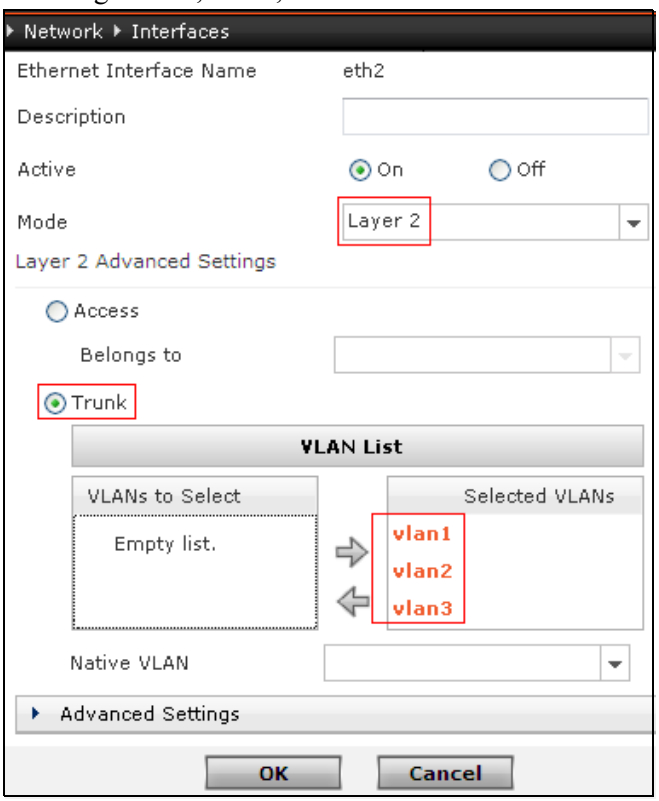
Note: For information about how to create Vsys administrators and set Vsys management IP addresses, see Example 1.

1. Create Layer 3 Interfaces

1. Choose **Network > Interfaces**, set eth1 as a shared Layer 3 interface.



2. Click **OK**.
3. Create VLAN interfaces vlan1, vlan2, and vlan3, set eth2 as a **Layer 2 Trunk** interface, and assign vlan1, vlan2, and vlan3 to eth2:



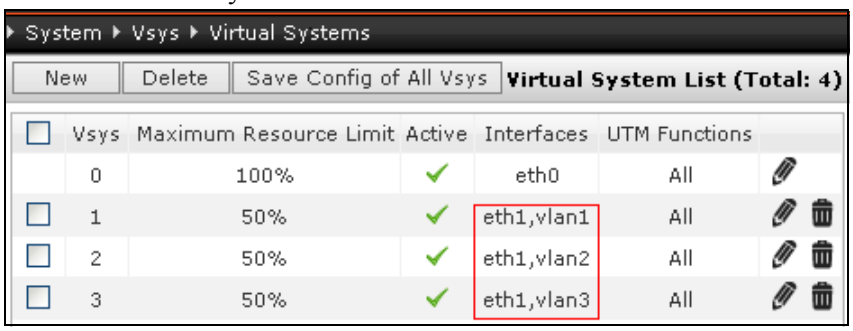
4. Configure the corresponding Trunk interface and VLAN interfaces on the Intranet switch.
5. Click **OK**.
6. Click .

CLI

```
FGX@root> configure mode override
FGX@root-system] interface ethernet 1
FGX@root-system-if-eth1] working-type layer3-shared-interface
FGX@root-system-if-eth1] exit
FGX@root-system] vlan 1
FGX@root-system-vlan1] exit
FGX@root-system] vlan 2
FGX@root-system-vlan2] exit
FGX@root-system] vlan 3
FGX@root-system-vlan3] exit
FGX@root-system] interface ethernet 2
FGX@root-system-if-eth2] port mode trunk
FGX@root-system-if-eth2] port trunk allowed vlan 1,2,3
FGX@root-system] end
FGX@root> save config
```

2. Create Vsys

1. Choose **System > Virtual Systems > Virtual Systems**, click **New** to create virtual systems vsys1, vsys2, and vsys3. Assign eth1 and vlan1 to vsys1, eth1 and vlan2 to vsys2, and eth1 and vlan3 to vsys3:



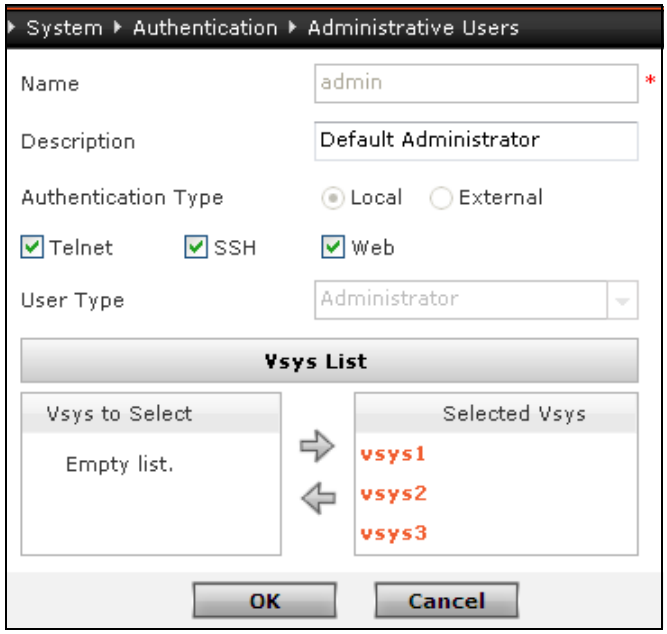
2. Click .

CLI

```
FGX@root> configure mode override
FGX@root-system] vsys 1 resource-limit 50
FGX@root-system-vsys1] hold ethernet 1
FGX@root-system-vsys1] hold vlan 1
FGX@root-system-vsys1] exit
FGX@root-system] vsys 2 resource-limit 50
FGX@root-system-vsys2] hold ethernet 1
FGX@root-system-vsys2] hold vlan 2
FGX@root-system-vsys2] exit
FGX@root-system] vsys 3 resource-limit 50
FGX@root-system-vsys3] hold ethernet 1
FGX@root-system-vsys3] hold vlan 3
FGX@root-system] end
FGX@root> save config
```

3. Assign Vsys to admin

1. Choose **System > Authentication > Administrative Users**, click corresponding to admin to open the **Edit** page, and add vsys1, vsys2, and vsys3 to the managed Vsys list:



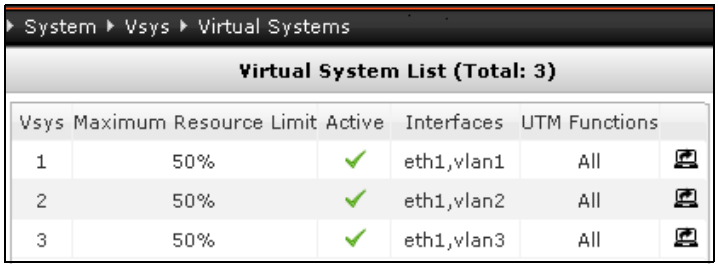
2. Click **OK**.
3. Click .

CLI

```
FGX@root> configure mode override
FGX@root-system] user administrator admin allowed-vsys vsys1
FGX@root-system] user administrator admin allowed-vsys vsys2
FGX@root-system] user administrator admin allowed-vsys vsys3
FGX@root-system] end
FGX@root> save config
```

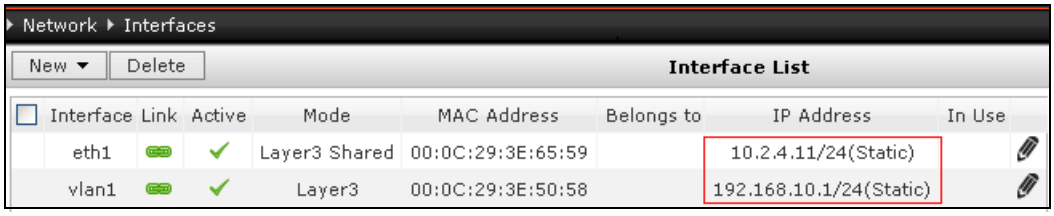
4. Set Interface IP and Access Policy for Vsys

1. Choose **System > Virtual Systems > Virtual Systems**, click **Switch Vsys** at the bottom of the page.



2. Click  corresponding to Vsys 1 to switch to vsys1.

3. Choose **Network > Interfaces**, and set the IP address of eth1 to 10.2.4.11/24 and that of vlan1 to 192.168.10.1/24:



4. Choose **Firewall > Access Policies**, add an access policy named vsys1out to permit access from 192.168.10.0/24 to any:

5. Switch to vsys2:

   a. Choose **Network > Interfaces**, and set the IP address of eth1 to 10.2.4.12/24 and that of vlan2 to 192.168.20.1/24.

   b. Choose **Firewall > Access Policies**, add an access policy named vsys2out to permit access from 192.168.20.0/24 to any.

6. Switch to vsys3:

   a. Choose **Network > Interfaces**, and set the IP address of eth1 to 10.2.4.13/24 and that of vlan3 to 192.168.30.1/24.

   b. Choose **Firewall > Access Policies**, add an access policy named vsys3out to permit access from 192.168.30.0/24 to any.

   The IP addresses of eth1 in vsys1, vsys2, and vsys3 cannot be the same. Configure a permit-all access policy on the Intranet switch.

7. Click  .

Note: If you want to use Ping to test the network connection, you need to log on to each Vsys and enable the Ping service.

CLI

```
FGX@root> switch vsys vsys1
FGX@vsys1> configure mode override
FGX@vsys1-system] interface ethernet 1
FGX@vsys1-system-if-eth1] ip address 10.2.4.11 255.255.255.0
FGX@vsys1-system-if-eth1] exit
FGX@vsys1-system] vlan 1
FGX@vsys1-system-vlan1] ip address 192.168.10.1 255.255.255.0
FGX@vsys1-system-vlan1] exit
FGX@vsys1-system] policy access vsys1out any 192.168.10.0 any any any
any permit enable
FGX@vsys1-system] end
FGX@vsys1> save config
FGX@vsys1> switch vsys vsys2
FGX@vsys2> configure mode override
FGX@vsys2-system] interface ethernet 1
FGX@vsys2-system-if-eth1] ip address 10.2.4.12 255.255.255.0
FGX@vsys2-system-if-eth1] exit
FGX@vsys2-system] vlan 2
FGX@vsys2-system-vlan2] ip address 192.168.20.1 255.255.255.0
FGX@vsys2-system-vlan2] exit
FGX@vsys2-system] policy access vsys2out any 192.168.20.0 any any any
any permit enable
FGX@vsys2-system] end
FGX@vsys2> save config
FGX@vsys2> switch vsys vsys3
FGX@vsys3> configure mode override
FGX@vsys3-system] interface ethernet 1
FGX@vsys3-system-if-eth1] ip address 10.2.4.13 255.255.255.0
FGX@vsys3-system-if-eth1] exit
FGX@vsys3-system] vlan 3
FGX@vsys3-system-vlan3] ip address 192.168.30.1 255.255.255.0
FGX@vsys3-system-vlan3] exit
FGX@vsys3-system] policy access vsys3out any 192.168.30.0 any any any
any permit enable
FGX@vsys3-system] end
FGX@vsys3> save config
```

13.5. Parameter reference

This section describes parameters for:

- 13.5.1. Virtual Systems
- 13.5.2. Virtual Networks
- 13.5.3. Functions Configurable in Vsys

13.5.1. Virtual Systems

Table 263 Parameters of Virtual Systems

Parameter	Description
Vsys	The identifier of a Vsys. A Vsys name is composed of “vsys,” followed by the Vsys ID. The ID range is 1-255.
Maximum Resource Limit	The maximum proportion of resources allocated to a Vsys. 1%-100%. If you reduce the maximum resource limit of a Vsys, the new maximum limit will take effect only when the Vsys releases resources. If the maximum resource limit is increased, the new maximum limit will take effect immediately.
Active	Vsys status.  indicates Vsys is activated, and indicates a Vsys is not activated.
Interfaces (Included Layer 3 Interfaces)	Interfaces allocated to a Vsys, can include: • Layer 3 or shared Layer 3 Ethernet interfaces, • virtual interfaces, • VLAN interfaces, • Layer 3 or shared Layer 3 Ethernet channels, • Layer 3 or shared Layer 3 redundant interfaces, and • PPPoE interfaces.
UTM Functions	UTM functions for a Vsys, including Anti-Virus (AV), Anti-Spam (AS), IPS, URL Filtering (URL), and Application Control (APP). All are enabled by default.
Description	0-255 UTF-8 characters. It cannot contain ? " ' \ < > & or #.
Enable Virtual System	Enable or disable a virtual system.
Management IP Address	Choose a Layer 3 interface as the management interface and set an IPv4 or IPv6 address as the management IP address and for a Vsys.
Save All Vsys Config (excluding Vsys0)	Save configurations of all virtual systems except for the root system.
Administrative Users	Link to the Administrative Users page on which administrators can create Vsys administrators or specify administrators for Vsys. Vsys administrators cannot edit Vsys Layer 3 interfaces, maximum resource limit, and management IP address.
Switch Vsys	Link to the Switch Vsys page.

13.5.2. Virtual Networks

Table 264 Parameters of Virtual Networks

Parameter	Description
ID	The identifier of a virtual network. 1-255.
Vsys	The virtual systems connected to a virtual network.
Interfaces	The virtual interface a Vsys uses to connect to a virtual network.
Description	0-255 UTF-8 characters. It cannot contain ? " ' \ < > & or #.
Virtual Interface List	Add virtual interfaces connecting virtual systems into a virtual network.

13.5.3. Functions Configurable in Vsys

In Vsys, you can configure the following functions:

- **Home**
- **System > Overview > Access Settings**
- **System > Maintenance > Backup/Restore/Centralized Management**
- **System > Authentication/Certificates/Objects**
- **System > High Availability > Virtual Routers/Virtual Router Detection Groups**
- **System > Virtual Systems > Virtual Systems**: You can only switch to another Vsys.
- **System > Service Configuration > Access Settings** (except root login)**/Banners**
- **System > Logging Configuration**
- **Network > Interfaces**: Only loopback interfaces can be created and assigned Ethernet interfaces can be edited.
- **Network > Zones**
- **Network > DNS**
- **Network > DHCP**
- **Network > Routing/NAT/Multicast/IPv6**
- **Firewall** (including policies and attack defense)
- **UTM > Overview**
- **UTM > Export Control > Policies**
- **UTM > Export Control > Application Control**
- **UTM > Export Control > URL Filtering > General Settings** (URL Category Search)
- **UTM > Export Control > URL Filtering > Profiles/Blacklists and Whitelists**
- **UTM > Export Control > DNS Domain Blacklist/Page Filtering**
- **UTM > Client Protection/Server Protection**
- **UTM > Anti-Virus > Trusted URLs/Trusted Web Servers/Trusted Clients**
- **UTM > Anti-Spam > Allow List/Block List/Spam Word List**
- **UTM > Notification Messages**
- **UTM > QoS**
- **VPN** (including IPSec VPN and SSL VPN)
- **Monitor** (only for current system)

14 Monitoring

This chapter describes monitoring functions, including:

- 14.1 Topology
- 14.2 Traffic Statistics
- 14.3 Virtual Systems
- STP
- 14.4 Route
- 14.5 NAT
- 14.6 ARP
- 14.7 CAM
- 14.8 DHCP IP Address Binding Status
- 14.9 DHCPv6 Client
- 14.10 DNS Cache
- 14.11 High Availability
- 14.12 System Utilization
- 14.13 Online Users
- 14.14 IPSec VPN Tunnels
- 14.15 Multicast
- 14.16 Alerts/Logs

14.1 Topology

Monitors topological relationships among Layer 2 and Layer 3 interfaces in zones.

Choose **Monitor** > **Topology**.

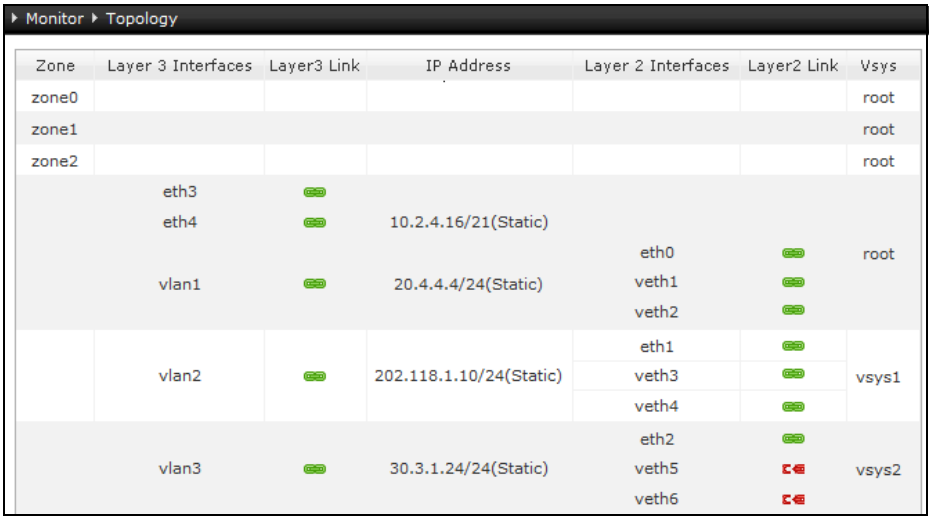


Table 265 Parameters of Topology

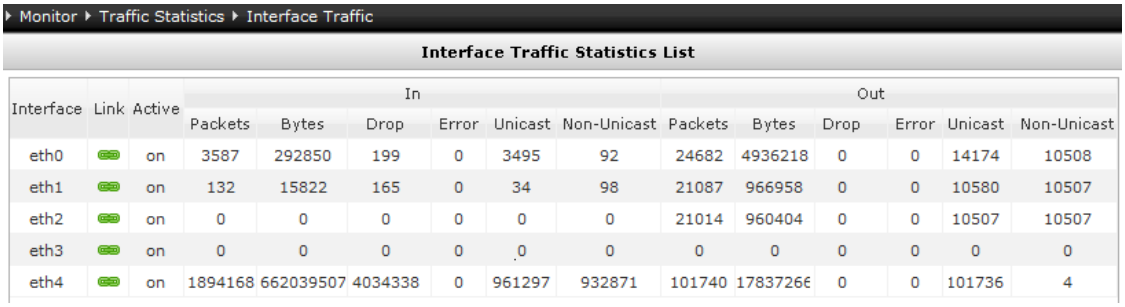
Parameter	Description
Zone	The zone that a Layer 3 interface belongs to.
Layer 3 Interface	Layer 3 interfaces in a zone. A Layer 3 zone includes Layer 3 interfaces, while a Layer 2 zone includes VLAN interfaces.
IP Address	Interface IP address. Only the primary IPv4 address is displayed (all IPv6 addresses are displayed). This can be the IP address of Layer 3 zone interfaces or layer 2 (VLAN) zone interfaces.
Layer 2 Interfaces	Layer 2 interfaces included in a Layer 3 interface.
Link	Physical connection state of a Layer 2 or Layer 3 interface, connected or disconnected.
Vsys	The Vsys to which a zone belongs.

14.2 Traffic Statistics

- 14.2.1 Interface Traffic
- 14.2.2 Top Applications
- 14.2.3 Top URLs
- 14.2.4 Top Users
- 14.2.5 Top IP Addresses

14.2.1 Interface Traffic

Choose **Monitor** > **Traffic Statistics** > **Interface Traffic**.



Interface	Link	Active	In						Out					
			Packets	Bytes	Drop	Error	Unicast	Non-Unicast	Packets	Bytes	Drop	Error	Unicast	Non-Unicast
eth0		on	3587	292850	199	0	3495	92	24682	4936218	0	0	14174	10508
eth1		on	132	15822	165	0	34	98	21087	966958	0	0	10580	10507
eth2		on	0	0	0	0	0	0	21014	960404	0	0	10507	10507
eth3		on	0	0	0	0	0	0	0	0	0	0	0	0
eth4		on	1894168	662039507	4034338	0	961297	932871	101740	17837266	0	0	101736	4

Table 266 Parameters of Interface Traffic

Parameter	Description
Interface	Interface name.
Link	Physical connection state of an interface, connected or disconnected.
Active	Interface state, on or off.
In Packets/Bytes	Number of received packets/traffic.
In Drop	Number of packets dropped while being received.
In Error/Unicast/Non-Unicast	Number of received error/unicast/non-unicast packets.
Out Packets/Bytes	Number of sent packets/traffic.
Out Drop	Number of dropped packets while being sent.
Out Error/Unicast/Non-Unicast	Number of sent error/unicast/non-unicast packets.

14.2.2 Top Applications

Choose **Monitor** > **Traffic Statistics** > **Top Applications**. Specify the number of top applications to show, the refresh method (manual and automatic), and the refresh interval.

14.2.3 Top URLs

Choose **Monitor** > **Traffic Statistics** > **Top URLs**. Specify the number of top URLs to show, the refresh method (manual and automatic), and the refresh interval.

14.2.4 Top Users

Choose **Monitor** > **Traffic Statistics** > **Top Users**. Specify the number of top users to show, the refresh method (manual and automatic), and the refresh interval.

14.2.5 Top IP Addresses

Choose **Monitor** > **Traffic Statistics** > **Top IP Addresses**. Specify the number of top IP addresses to show, the refresh method (manual and automatic), and the refresh interval.

14.3 Virtual Systems

Monitors all Vsys. For more information, see Chapter 13, “Virtual Systems.”

Choose **Monitor** > **Vsys**.

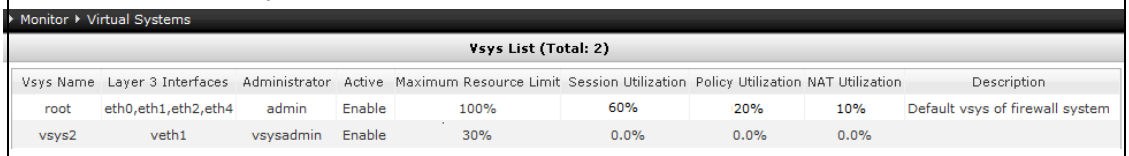


Table 267 Parameters of Vsys

Parameters	Description
Vsys Name	Vsys name.
Layer 3 Interfaces	Layer 3 interfaces within a Vsys.
Administrator	Vsys administrator.
Active	Vsys state, enabled or disabled.
Allocated Resource	Percentage of resources allocated to a Vsys.
Session Utilization	Percentage of session table resources available to a Vsys.
Policy Utilization	Percentage of policy resources available to a Vsys.
NAT Utilization	Percentage of NAT resources available to a Vsys.
Description	Description about a Vsys.

STP

Monitors Layer 2 interfaces in VLANs or instances. For more information, see 4.19.1 Overview. To view STP monitoring information, enable STP first.

Choose **Monitor** > **STP**.

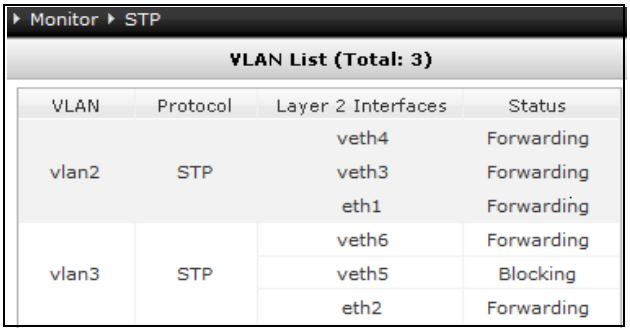


Table 268 STP Information When Per-VLAN STP is Enabled

Parameter	Description
VLAN	VLANs in which STP is enabled.
Protocol	Protocols enabled in a VLAN, STP or RSTP.
Layer 2 Interfaces	Layer 2 interfaces in a VLAN, Ethernet interfaces, channel interfaces, redundant interfaces, or virtual interfaces.
Status	Working status of Layer 2 interfaces in a VLAN, Disabled, Blocking, Learning, Forwarding, or Discarding.

14.4 Route

Monitors default routing, policy-based routing, and multicast routing. For more information, see Chapter 6, "Routing."

Choose **Monitor** > **Route** or click **Default Routing Table** to open the **Default Routing** page.

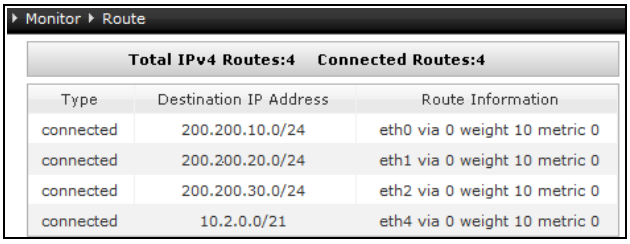


Table 269 Parameters of Default Routes

Parameter	Description
Type	Route types, Connected or Static.
Destination IP Address	IPv4 or v6 address to which packets are sent.
Route Information	Detailed information about routing process.

Choose **Monitor** > **Route** or click **Policy-Based Routing** to open the **Policy-Based Routing** page.

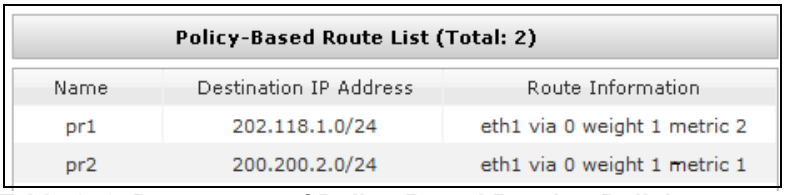


Table 270 Parameters of Policy-Based Routing Policies

Parameter	Description
Name	Policy-based routing policy name.
Destination IP Address	IPv4 or v6 address to which packets are sent.
Route Information	Detailed information about routing process.

Choose **Monitor** > **Route** or click **Multicast Routing** to open the **Multicast Routing** page.

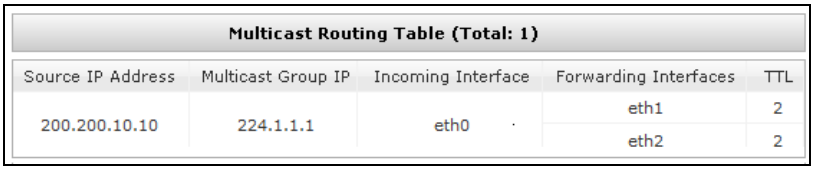


Table 271 Parameters of Multicast Routes

Parameter	Description
Source IP Address	IP address from which multicast packets are sent.
Multicast Group IP	IP address of a destination multicast group.
Incoming Interface	Layer 3 interface through which packets are received.

Table 271 Parameters of Multicast Routes (*continued*)

Parameter	Description
Forwarding Interfaces	Layer 3 interface through which packets are forwarded.
TTL	Maximum number of routing devices a multicast packet can pass before being dropped.

14.5 NAT

Monitors real-time NAT information. For more information, see Chapter 5, "Network Address Translation."

Choose **Monitor** > **NAT**.

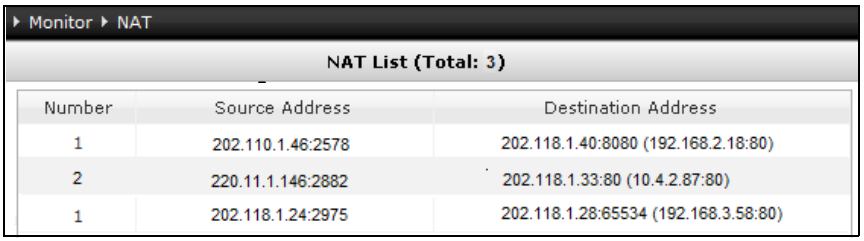


Table 272 Parameters of NAT

Parameter	Description
Source Address	The IP address from which packets are sent.
Destination Address	The original and translated destination IP address (in parentheses) of packets.

14.6 ARP

Monitors ARP table and ARP proxy table. For more information, see 4.10 ARP.

14.6.1 ARP Table

Choose **Monitor** > **ARP** > **ARP Table**. Click **Refresh** to refresh the ARP table. Click to edit filter conditions.

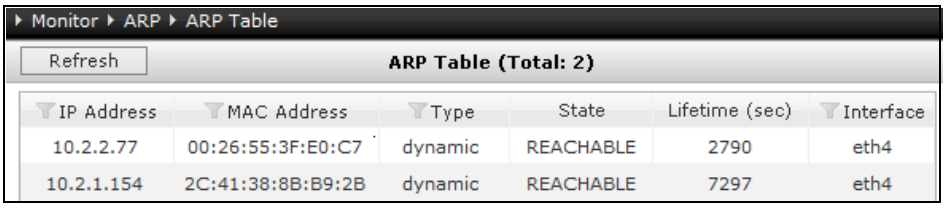


Table 273 Parameters of the ARP Table

Parameter	Description
IP Address	Destination host IP address. Cannot be a loopback address, multicast address, broadcast address of a subnet, or limited broadcast address.
MAC Address	MAC address corresponding to an IP address. Cannot be broadcast/multicast address.
Type	ARP entry types, Static, Dynamic, or Proxy.
State	ARP entry states: • **INCOMPLETE—**an ARP request already been sent, but no reply has been received. • **REACHABLE—**an entry is available. • **STALE—**entry available, but lifetime is running out. The entry needs to be renewed. • **FAILED—**an entry is unavailable. This state cannot be seen.
Lifetime (sec)	Dynamic ARP entry lifetime.
Interface	Layer 3 interface to which an entry belongs. Can be all Layer 3 interfaces except tunnel interfaces, PPPoE interfaces, and loopback interfaces.

14.6.2 ARP Proxy Table

Choose **Monitor** > **ARP** > **ARP Proxy Table**. Click **Refresh** to refresh the ARP proxy table. Click to edit filter conditions.

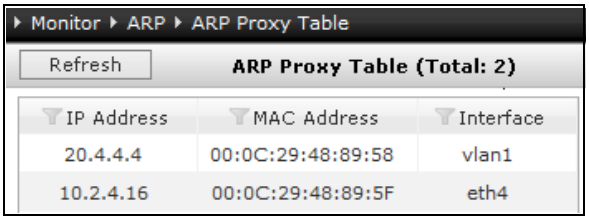


Table 274 Parameters of ARP Proxy Table

Parameter	Description
IP Address	Destination host IPv4 address.
MAC Address	MAC address corresponding to the IP address.
Interface	Layer 3 interface to which an entry belongs. Cannot be tunnel interfaces, PPPoE interfaces, or loopback interfaces.

14.7 CAM

Monitors the summary information and address table information about the CAM table. For more, see 4.11.1 Overview.

Choose **Monitor** > **CAM**. Click **Refresh** to refresh the address table. Click to edit filter conditions.

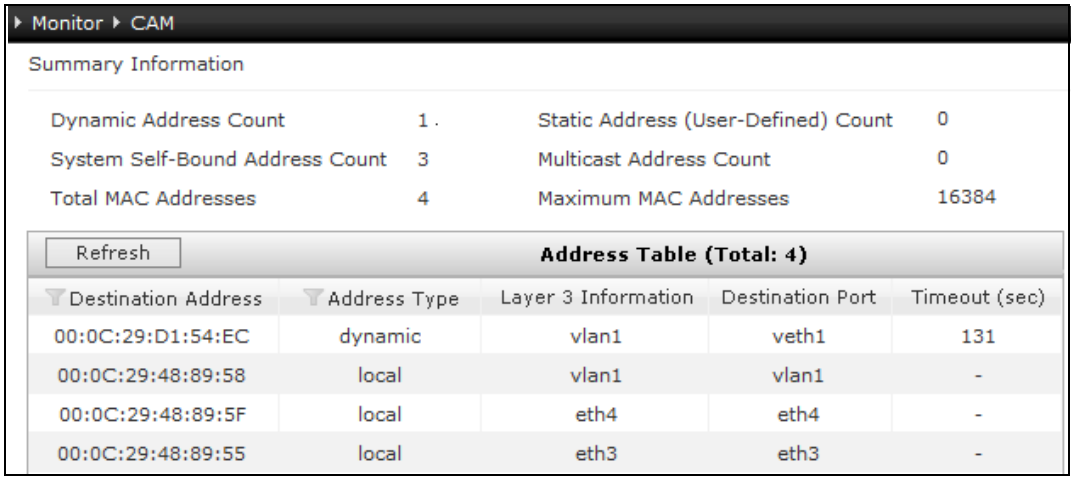


Table 275 Parameters of Summary Information

Parameter	Description
Dynamic Address Count	Number of dynamic entries in a CAM table.
Static Address (User-Defined) Count	Number of static entries.
System Self-Bound Address Count	Number of system addresses.
Multicast Address Count	Number of multicast addresses.
Total MAC Addresses	Total number of MAC addresses.
Maximum MAC Addresses	Maximum number of MAC addresses.

Table 276 Parameters of the Address Table

Parameter	Description
Destination Address	MAC address to which a packet is sent.
Address Type	Address types in a CAM table, Local, Dynamic, Static, or Multicast.
Layer 3 Information	VLAN to which a CAM entry belongs.
Destination Port	Destination port that receives packets.
Timeout (sec)	Dynamic CAM entry timeout. 10-30,000 seconds. 300 seconds by default.

14.8 DHCP IP Address Binding Status

Shows the binding status between DHCP interfaces and IP addresses. For more information, see 4.16.1 Overview. Choose **Monitor** > **DHCP IP Address Binding Status**. Select a subnet from the **Subnet** drop-down list.

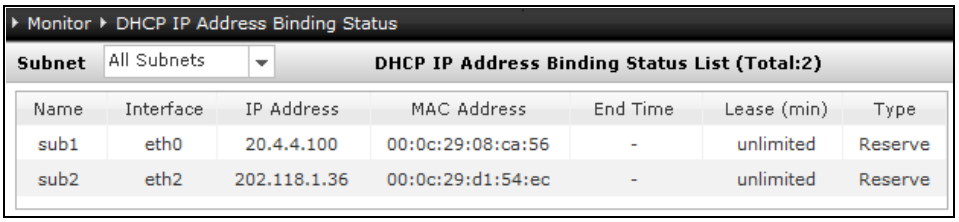


Table 277 Parameters of DHCP IP Address Binding Status

Parameter	Description
Name	DHCP server subnet name.
Interface	Layer 3 interface on which DHCP is enabled.
IP Address	IP address set in a DHCP server subnet.
MAC Address	MAC address bound to an IP address.
End Time	Time when IP address lease expires.
Lease (min)	Lease duration of an IP address in the server subnet.
Type	IP address types, dynamic or reserved.

14.9 DHCPv6 Client

Monitors DHCPv6 clients. For more information, see 4.18.1 Overview. Choose **Monitor** > **DHCPv6 Client**.

Table 278 Parameters of DHCPv6 Clients

Parameter	Description
Interface	Interface on which DHCP client is enabled.
Prefix Delegated	Prefix acquired by the client.
Preferred Lifetime	Preferred lifetime of the prefix acquired, in seconds.
Valid Lifetime	Valid lifetime of the prefix acquired, in seconds.
DNS	Address of the DNS server acquired by the client.
Domain Search List	Domain search list acquired by the client.
SNTP	SNTP server address acquired by the client to synchronize the system time.

14.10 DNS Cache

Monitors dynamic DNS cache entries. For more information, see 4.15.1 Overview. Choose **Monitor** > **DNS Cache**.

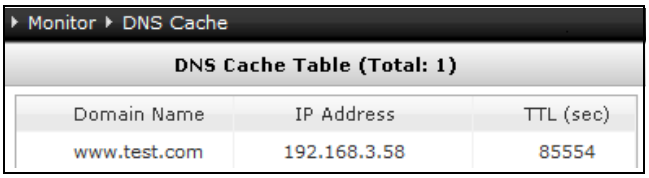


Table 279 Parameters of the Dynamic DNS Cache Table

Parameter	Description
Domain Name	Dynamic cache entry domain name.
IP Address	IPv4 or v6 address corresponding to a domain name.
TTL (sec)	Dynamic DNS cache entry lifetime.

14.11 High Availability

Shows information about:

- 14.11.1 Virtual Routers
- 14.11.2 Virtual Router Detection Groups
- 14.11.3 Clusters

For more information, see Chapter 12, “High Availability.”

14.11.1 Virtual Routers

Shows information about virtual routers and IP tracking status.

Choose **Monitor** > **High Availability** > **Virtual Routers**. Select a router ID from the **VRID** drop-down list.

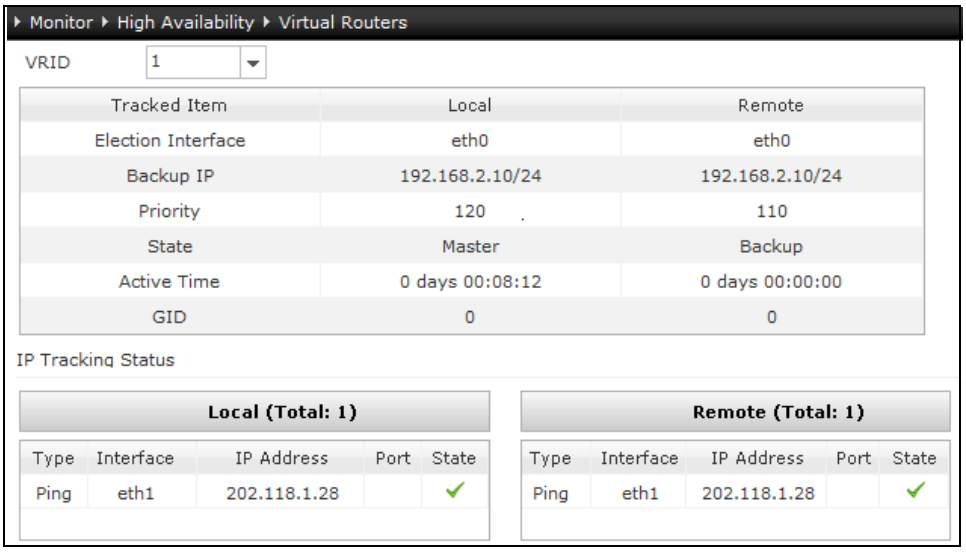


Table 280 Parameters of Virtual Routers

Parameter	Description
Tracked Item	Items tracked by FGX: • **Election Interface**—the interface used for communications between local and remote FGX devices • **Backup IP**—the backup IP addresses of local and remote FGX devices. • State—the working states of local and remote FGX devices, Master or Backup. • **Active Time**—the length of time local and remote FGX devices have been active. • **Group ID—**virtual router detection group ID.
Local	Information about the local FGX device.
Remote	Information about the remote FGX device.

Table 281 Parameters of IP Tracking Status

Parameter	Description
Type	IP tracking types, ARP ping, ping, or TCP ping.
Interface	A Layer 3 interface used for IP tracking.
IP Address	IP address to be tracked for reachability.
Port	Port to be tracked, required for TCP ping only.
State	Indicates whether an IP address is reachable.

14.11.2 Virtual Router Detection Groups

Shows information about virtual router detection groups and IP tracking status.

Choose **Monitor** > **High Availability** > **Virtual Router Detection Groups**. Select a group ID from the **Group ID** drop-down list.

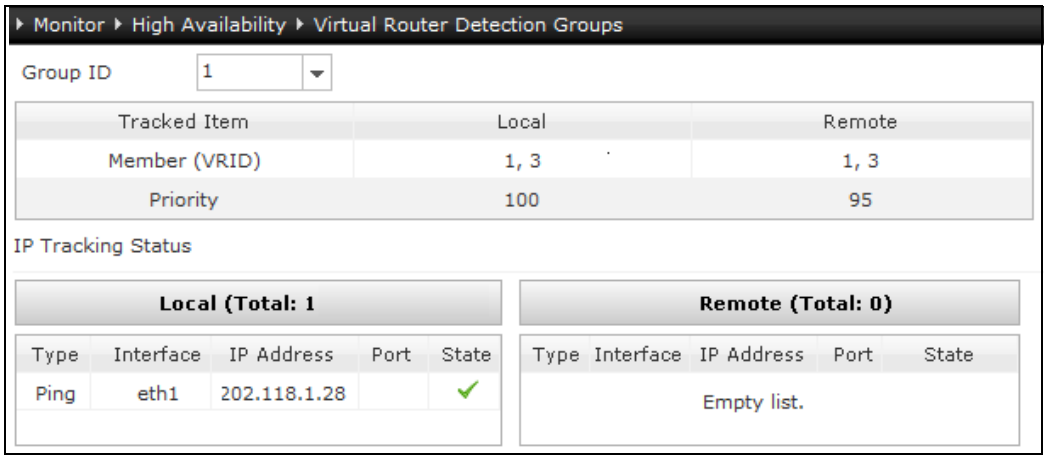


Table 282 Parameters of Virtual Router Detection Groups

Parameter	Description
Tracked Item	Members within a virtual router detection group.
Local	Information about the local FGX device.
Remote	Information about the remote FGX device.

Table 283 Parameters of IP Tracking Status

Parameter	Description
Type	IP tracking types, ARP ping, ping, or TCP ping.
Interface	A Layer 3 interface used for IP tracking.
IP Address	IP address to be tracked for reachability.
Port	Port to be tracked, required for TCP ping only.
State	Indicates whether an IP address is reachable.

14.11.3 Clusters

Choose **Monitor** > **High Availability** > **Clusters**.

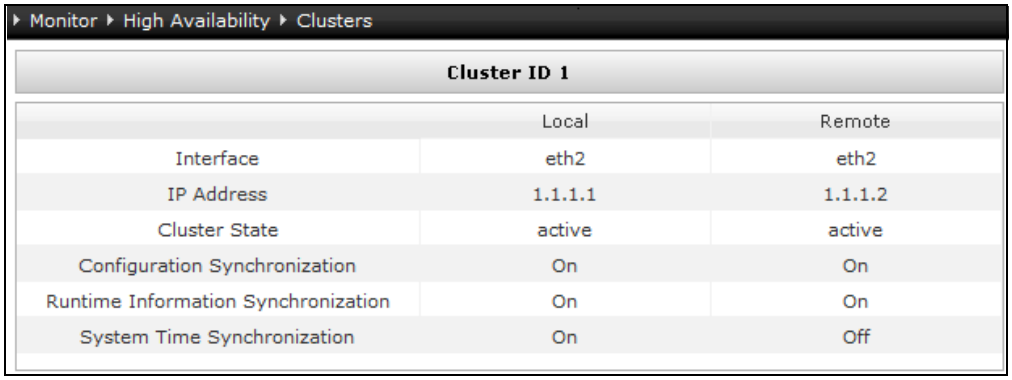


Table 284 Parameters of Clusters

Parameter	Description
Tracked Item	Items tracked by FGX: • **Interface—**the interface used for transmitting synchronization data within a cluster. • **IP Address—**the IP address of the interface for synchronization. • **Cluster State—**working states of cluster members. • **Configuration Synchronization—**states of configuration synchronization. • **Runtime Information Synchronization—**states of runtime information synchronization. • **System Time Synchronization—**states of system time synchronization.
Local	Information about the local FGX device.
Remote	Information about the remote FGX device.

14.12 System Utilization

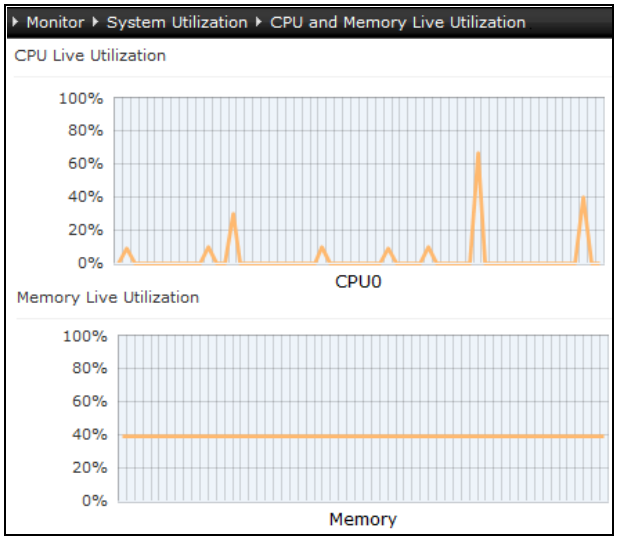
Shows information about:

- 14.12.1 CPU and Memory Live Utilization
- 14.12.2 Disk Utilization
- 14.12.3 Processes

14.12.1 CPU and Memory Live Utilization

Shows the CPU and memory utilization of the current system.

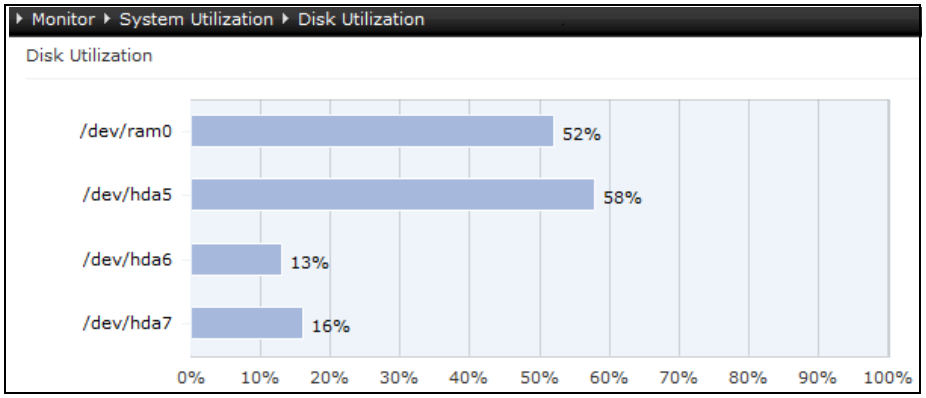
Choose **Monitor** > **System Utilization** > **CPU and Memory Live Utilization**.



14.12.2 Disk Utilization

Shows information about disk utilization and log storage utilization.

Choose **Monitor** > **System Utilization** > **Disk Utilization**.



14.12.3 Processes

Shows the utilization of the current processes.

Choose **Monitor** > **System Utilization** > **Processes**.

Table 285 Parameters of Process Utilization

Parameter	Description
USER	The user that initiated or executed the process.
PID	Process ID, the unique identifier used by the kernel to identify the process.
%CPU	Percentage of CPU used by the active process.
%MEM	Percentage of memory used by the active process.
VSZ	Virtual memory size used by the process, in KB.
RSS	Process memory size (resident set size), in KB.
TTY	Terminal type of the current process.
STATE	Process state.
START	Time when the process started.
TIME	Duration the process has been running.
COMMAND	Commands corresponding to the process.

14.13 Online Users

Monitors online WebAuth users and SSL VPN users. For more information, see 3.14 Users.

14.13.1 WebAuth Users

Choose **Monitor** > **Online Users** > **WebAuth Users**. Click **Refresh** to refresh online WebAuth users. Check the check box corresponding to an online WebAuth user and click **Offline** to force the user to get offline. Click to edit filter conditions.

Table 286 Parameters of WebAuth Users

Parameter	Description
Name	Online WebAuth user name.
IP Address	Online WebAuth user IP address.
Online Time (sec)	Length of time a WebAuth user has been online.
Real-time Traffic (KB/s)	Real-time traffic from a WebAuth user.
Traffic (KB)	Total traffic of an online WebAuth user.
Idle Time (sec)	Length of time an online WebAuth user has been idle before being forced offline.

14.13.2 SSL VPN Users

Choose **Monitor** > **Online Users** > **SSL VPN Users**. Click **Refresh** to refresh online SSL VPN users. Check the check box corresponding to an online SSL VPN user and click **Offline** to force the user to get offline. Click to edit filter conditions.

Table 287 Parameters of SSL VPN Users

Parameter	Description
User	Online SSL VPN user name.
User Group	Group an online SSL VPN user belongs to.
Login Type	Login types of an online SSL VPN user, Web-portal or tunnel.
Tunnel/Portal	Tunnel or portal page used by an online SSL VPN user to access the protected network.
IP Address	IP address used by an SSL VPN user to log in.
Online Time (sec)	Length of time an SSL VPN user has been online.
Sent (bytes)	Bytes sent by an online SSL VPN user.
Received (bytes)	Bytes received by an online SSL VPN user.
Idle Time (sec)	Length of time an online SSL VPN user has been idle before being forced offline.

14.14 IPSec VPN Tunnels

Monitors auto IKE tunnels, manual tunnels, accelerator card statistics, soft encryption statistics, and tunnel groups. For more information, see Chapter 11, "Virtual Private Network 2."

14.14.1 Auto IKE Tunnels

Choose **Monitor** > **IPSec VPN Tunnel** > **Auto IKE**. Select a tunnel type from the **Tunnel Type** drop-down list, **All**, **Dynamic IP Address**, **Static IP Address**, **Dial-Up User**, or **Dial-Up User Group**. When you choose **Dial-Up User Group**, you can specify a dial-up user group to view. Click to view auto IKE tunnel information.

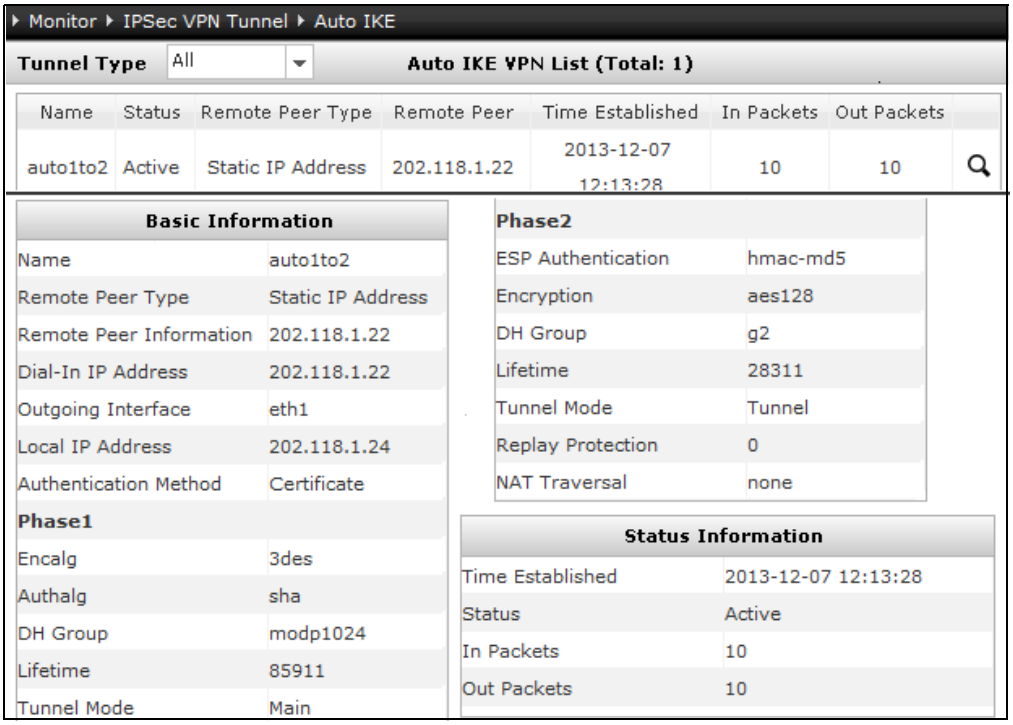


Table 288 Parameters of Auto IKE Tunnels

Parameter	Description
Name	Auto IKE tunnel name.
Status	Auto IKE tunnel states: • **Closed—**the tunnel cannot forward packets. • **Active—**the tunnel can forward packets. • **Negotiate—**when an auto IKE site-to-site VPN tunnel is enabled, the tunnel first enters this state and then enters the open state after the negotiation is successful.
Remote Peer Type	Remote peer types for site-to-site IPSec VPN tunnels, Static IP Address, Dynamic IP Address, Dial-up User, or Dial-up User Group.
Remote Peer	Remote peer identifier of an auto IKE tunnel, depending on the remote peer type.
Time Established	Time when an auto IKE tunnel was established.
In Packets	Number of packets received.
Out Packets	Number of packets sent.

14.14.2 Manual Tunnels

Choose **Monitor** > **IPSec VPN Tunnel** > **Manual Tunnels**. Click to view the manual tunnel information.

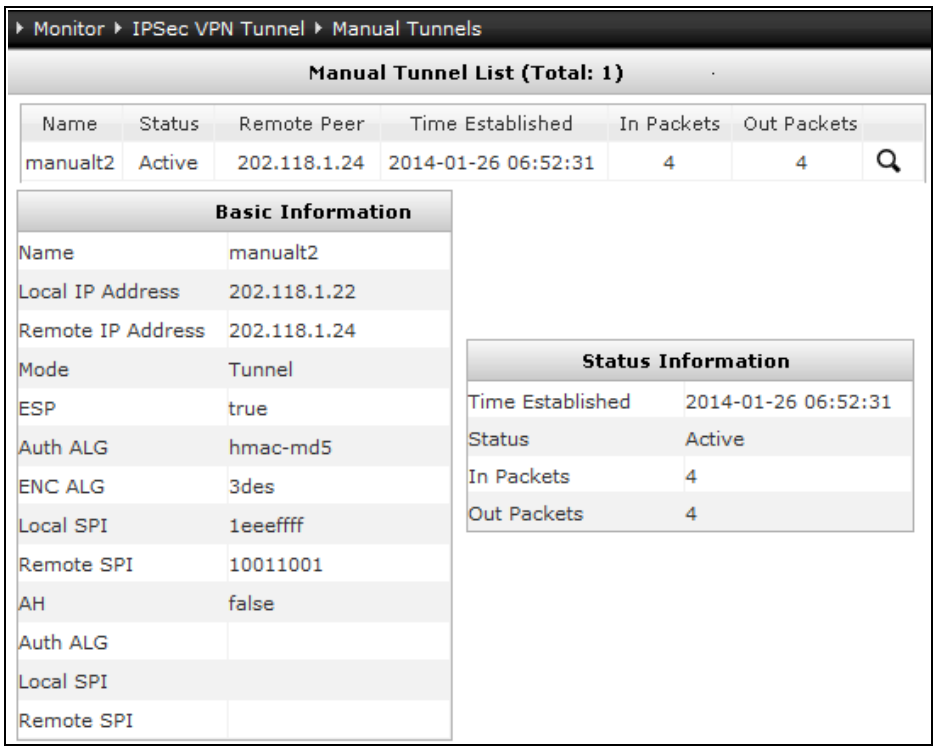


Table 289 Parameters of Manual Tunnels

Parameter	Description
Name	Manual tunnel name.
Status	Manual tunnel status: • **Closed—**cannot forward packets. • **Active—**can forward packets.
Remote Peer	IP address of the remote peer of a manual tunnel.
Time Established	Time a manual tunnel was established.
In Packets	Number of packets received.
Out Packets	Number of packets sent.

14.14.3 Accelerator Card Statistics

Choose **Monitor** > **IPSec VPN Tunnel** > **Accelerator Card Statistics**.

Table 290 Parameters of Accelerator Card Statistics

Parameter	Description
Name	An accelerator card name. Devices of different models have different accelerator card names.
State	Accelerator card states, enabled or disabled.
Encrypted Packets	Number of packets encrypted by an accelerator card.
Encrypted Bytes	Number of bytes encrypted by an accelerator card.
Decrypted Packets	Number of packets decrypted by an accelerator card.
Decrypted Bytes	Number of bytes decrypted by an accelerator card.
Error Count	Number of error packets sent and received by an accelerator card.

14.14.4 Soft Encryption Statistics

Choose **Monitor** > **IPSec VPN Tunnel** > **Soft Encryption Statistics**.

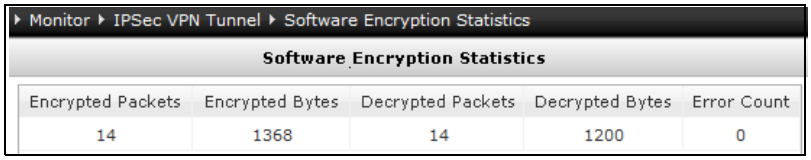


Table 291 Parameters for Soft Encryption Statistics

Parameter	Description
Encrypted Packets	Number of packets encrypted through soft encryption.
Encrypted Bytes	Number of bytes encrypted through soft encryption.
Decrypted Packets	Number of packets decrypted through soft encryption.
Decrypted Bytes	Number of bytes decrypted through soft encryption.
Error Count	Number of error packets detected in sending or receiving soft encryption packets.

14.14.5 Tunnel Groups

Choose **Monitor** > **IPSec VPN Tunnel** > **Tunnel Groups**.

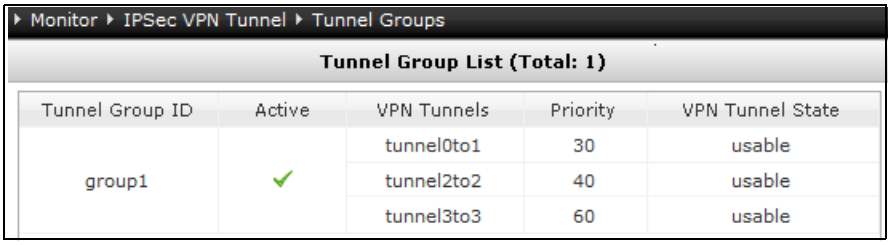


Table 292 Parameters of Tunnel Groups

Parameter	Description
Tunnel Group ID	Unique identifier of a tunnel group.
Active	Tunnel group states: • —disabled. • —enabled.
VPN Tunnels	IPSec VPN tunnels in a tunnel group.
Priority	Priority of IPSec VPN tunnels in a group.
VPN Tunnel State	State of IPSec VPN tunnels in a group.

14.15 Multicast

Monitors the real-time information of multicast, including DVMRP neighbors and IGMP snooping state. For more information, see 6.1.2 L3 Multicast and 6.1.3 L2 Multicast.

14.15.1 DVMRP Neighbors

Choose **Monitor** > **Multicast** > **DVMRP Neighbors**.

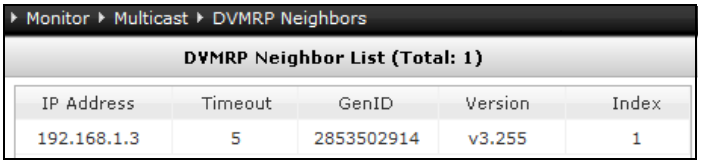


Table 293 Parameters of DVMRP Neighbors

Parameter	Description
IP Address	DVMRP neighbor IP address.
Timeout	DVMRP neighbor timeout, in seconds.
GenID	Multicast ID of a DVMRP neighbor.
Version	DVMRP protocol version.
Index	DVMRP neighbor sequence number.

14.15.2 IGMP Snooping State

Choose **Monitor** > **Multicast** > **IGMP Snooping State**.

Table 294 Parameters of IGMP Snooping State

Parameter	Description
VLAN	Information about a VLAN that receives multicast packets.
Active	IGMP snooping state in a VLAN, enabled or disabled.
Layer 2 Interfaces	Layer 2 interfaces in a VLAN.
IGMP Version	IGMP versions used by the system, v1, v2, or Auto. The default version is Auto.
IGMP Mode	Types of network devices directly connected to FGX: • **Router—**the device is a router. Multicast packets are sent to interfaces of this type. • **Host—**the device is a host. • **Auto—**the interface identifies the device type dynamically according to received packets. This is the default mode.
Multicast CAM Table	Multicast CAM table of a VLAN.

14.16 Alerts/Logs

Shows the real-time information about:

- 14.16.1 System Logs
- 14.16.2 Anti-Virus Alerts
- 14.16.3 Anti-Spam Alerts
- 14.16.4 URL Filtering Alerts
- 14.16.5 IPS Alerts
- 14.16.6 Application Control Alerts

14.16.1 System Logs

Choose **Monitor** > **Alerts/Logs** > **System Logs**. Click **Refresh** to get the most recent system logs. Click to edit filter conditions.

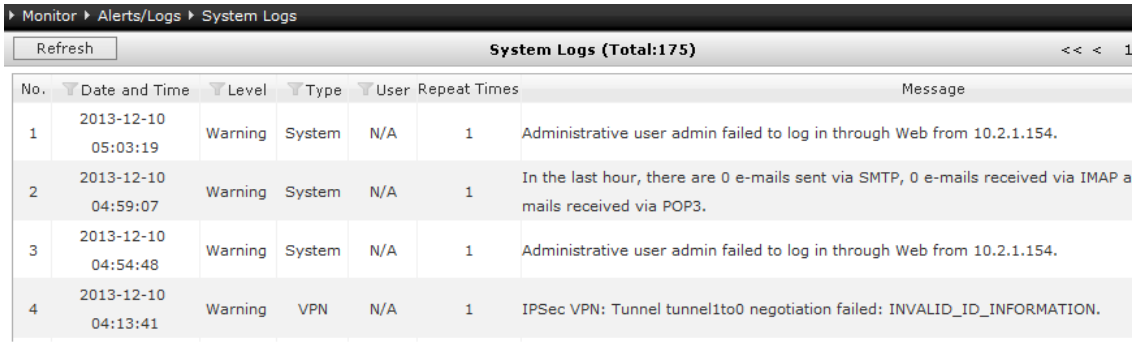


Table 295 Parameters of System Logs

Parameter	Description
Date and Time	Date and time a system log was generated.
Level	Security levels of system logs, Emergency, Alert, Critical, Error, Warning, Notice, Informational, or Debugging.
Type	Sources of system logs, Management, Session, NAT, FW, VPN, IPS, Anti-Virus, Anti-Spam, URL-Filtering, or Application Control.
User	User involved in the log message.
Repeat Times	Number of logs merged into a single log. FGX can merge duplicate system logs within a set period and inform users by showing the repeat times.
Message	Body of a system log. A message describes events that occurred and includes parameters related to the events.

14.16.2 Anti-Virus Alerts

Choose **Monitor** > **Alerts/Logs** > **Anti-Virus Alerts**. Click **Refresh** to get the most recent anti-virus alerts. Click to edit filter conditions.

Table 296 Parameters of Anti-Virus Alerts

Parameter	Description
Date and Time	Date and time a file was quarantined.
Profile	Profile used by the anti-virus policy that a quarantined file matches.
Filename	Quarantined file name.
File Type	Quarantined file types.
Virus	Name of the virus detected.
Service	Application layer protocols used for sending a file, HTTP, FTP, SMTP, POP3, or IMAP.
Src IP	IP address from which a quarantined file was sent.
Status	The reason a file was quarantined.
Message	Details about a quarantined file.
Action	Actions for processing a quarantined file, Pass or Block.

14.16.3 Anti-Spam Alerts

Choose **Monitor** > **Alerts/Logs** > **Anti-Spam Alerts**. Click **Refresh** to get the most recent anti-spam alerts. Click to edit filter conditions.

Table 297 Parameters of Anti-Spam Alerts

Parameter	Description
Date and Time	Date and time an e-mail message was quarantined.
Profile	Profile used by the anti-spam policy that a quarantined e-mail message matches.
Service	Application layer protocols used for sending an e-mail message, SMTP or POP3.
Src IP	IP address from which a quarantined e-mail message was sent.
Sender	Sender of a quarantined e-mail message.
Subject	Subject of a quarantined e-mail message.

Table 297 Parameters of Anti-Spam Alerts (*continued*)

Parameter	Description
Attachment	Attachments of a quarantined e-mail message.
Status	The reason an e-mail message was quarantined.
Message	Details about a quarantined-mail message.
Recipient	Recipient of a quarantined e-mail message.
Action	Actions for processing a quarantined e-mail message, Block, Allow, or Tag.

14.16.4 URL Filtering Alerts

Choose **Monitor** > **Alerts/Logs** > **URL Filtering Alerts**. Click **Refresh** to get the most recent URL filtering alerts. Click to edit filter conditions.

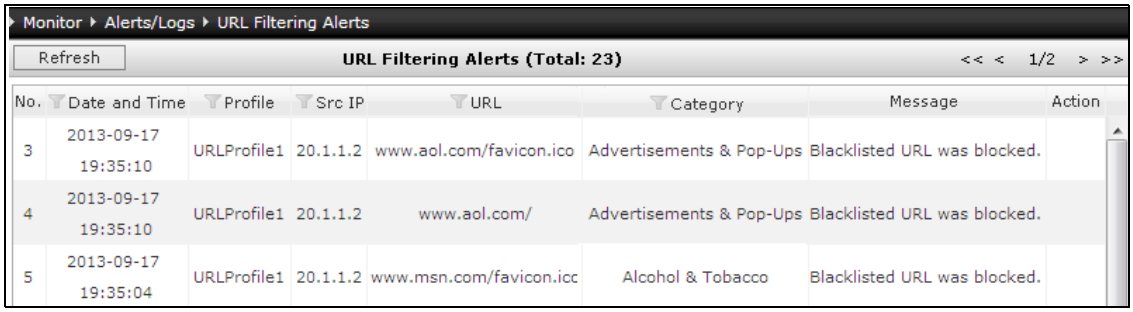


Table 298 Parameters of URL Filtering Alerts

Parameter	Description
Date and Time	Date and time a URL was logged for URL filtering.
Src IP	Source IP address of an HTTP request.
URL	The URL from which traffic is blocked or allowed.
Category	Category a URL belongs to.
Message	Details about why a URL is blocked or allowed.
Action	Actions for processing a URL that matches a URL filtering policy, Allow or Block.

14.16.5 IPS Alerts

Choose **Monitor** > **Alerts/Logs** > **IPS Alerts**. Click **Refresh** to get the most recent IPS alerts. Click . to edit filter conditions.

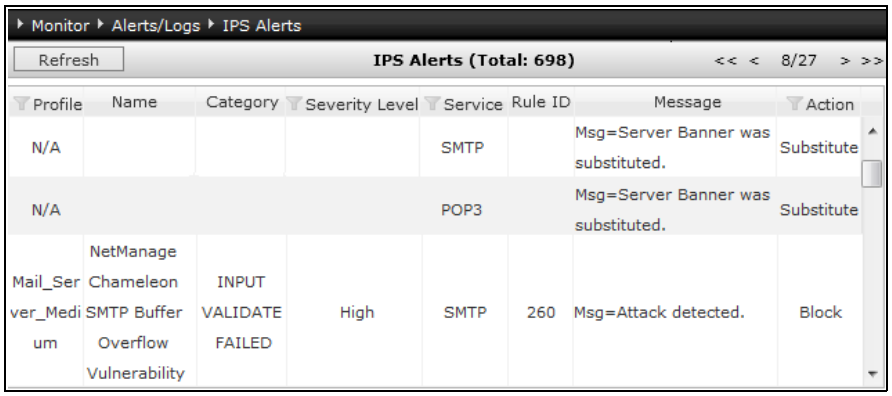


Table 299 Parameters of IPS Alerts

Parameter	Description
Date and Time	Date and time an attack signature rule was matched and a log was generated.
Profile	Profile used by the attack signature rule that a packet matches.
Src IP	Source IP address of the packets which match an attack signature rule.
Src Port	Source port of the packets which match an attack signature rule.
Dst IP	Destination IP address of the packets which match an attack signature rule.
Dst Port	Destination port of the packets which match an attack signature rule.
Name	Name of a matched attack signature rule.
Category	Category of a matched attack signature rule.
Severity Level	Severity levels of attacks that match a signature rule, High (Critical), Medium (Error), Low (Warning), or Info (Notification).
Service	Service used by the packets which match an attack signature rule.
Rule ID	IPS rule of an attack signature which was matched.
Message	Details about an IPS alert.
Action	Actions for processing packets which match an attack signature rule, Allow, Block, or Reject.

14.16.6 Application Control Alerts

Choose **Monitor** > **Alerts/Logs** > **Application Control Alerts**. Click **Refresh** to get the most recent application control alerts. Click to edit filter conditions.

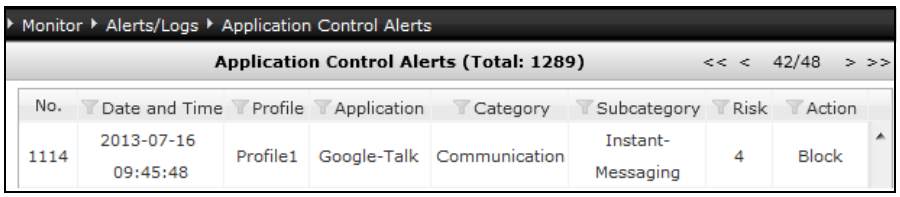


Table 300 Parameters of Application Control Alerts

Parameter	Description
Date and Time	Date and time an application was matched and log was generated.
Profile	Profile used by the application control policy that an application matches.
Src IP	Source IP address of the application which matches a rule.
Src Port	Source port of the application which matches a rule.
Dst IP	Destination IP address of the application which matches a rule.
Dst Port	Destination port of the application which matches a rule.
Protocol Type	Types of protocol used by the application which matches a rule, such as DNS, HTTP, SMTP, POP3, IMAP, and FTP.
Application	Application which matches an application control rule.
Category	Application categories, Business, Communication, General-Internet, Multi-Media, or Networking.
Subcategory	Subcategories of the application, such as Auth-Service and Database.
Risk	Potential risk to the system.
Action	Actions for processing an application, Pass or Block.

15 Reporting

This chapter explains the reporting feature, comprising:

- 15.1 Overview. Describes reporting concepts and functions.
- 15.2 Basic Configuration Steps. Describes basic configuration steps and the UI dialogs. Your scenario will not require all of these steps.
- 15.3 Parameter Reference. Describes in detail all parameters.

15.1 Overview

Reporting is a WebUI-based application. It shows data recorded by the system. This section describes:

- 15.1.1 Recorded Content
- 15.1.2 Report Content / Format
- 15.1.3 Scheduled Report Generation
- 15.1.4 View / Download / Email Reports
- 15.1.5 Retaining Old Reports

15.1.1 Recorded Content

Content of the following categories can be recorded:

- System
- Traffic
- Web security
- Mail security
- Anti-virus
- Attack
- Application
- User

15.1.2 Report Content / Format

- A report includes cover page, table of contents, and statistics (displayed in line graphs, bar charts, pie charts, and tables).
- Open **Monitor** > **Reports** > **Schedules** (under "**Content Settings**") to optionally specify report content.
- Display the cover page default or imported logo (.jpg).
- Language can be English or Chinese.
- Format can be PDF and/or HTML.

15.1.3 Scheduled Report Generation

You can make up to 10 report schedules in each Vsys. Reports will be generated automatically as specified.

A calendar shows different types of report schedules (daily, weekly, and monthly).

15.1.4 View / Download / Email Reports

You can

- View reports.
- Download reports to your local computer.
- Email: You can configure SMTP server and e-mail information to send reports by e-mail. For information about email senders and recipients, see 15.3 Parameter Reference.

15.1.5 Retaining Old Reports

Specify the number of reports to save (5-20, 10 by default). (**Monitor** > **Reports** > **General Settings**, under "**Executive Report Settings**.")

15.2 Basic Configuration Steps

This section describes the basic configuration procedure:

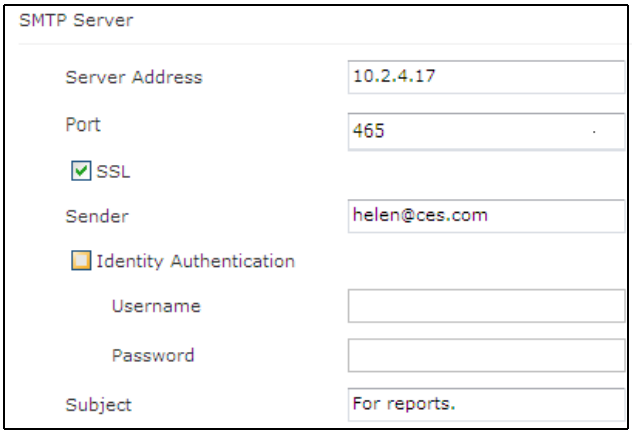
- 15.2.1 Configure General Settings
- 15.2.2 Create a Report Schedule
- 15.2.3 Manage Report Results

15.2.1 Configure General Settings

Choose **Monitor** > **Reports** > **General Settings**.

1. Enable functions for recording specific types of statistics.

2. Configure SMTP server and e-mail information.



3. Set a maximum number of report results to keep.

4. Use the default logo. You can also click **Import** to upload a different logo. The uploaded logo is shown in the **Preview** area.

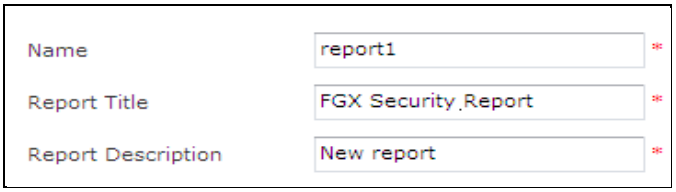
The imported logo must be less than 100 K with a resolution of at least 96 dpi. Importing a logo overwrites the existing log.

5. Click **OK**.

15.2.2 Create a Report Schedule

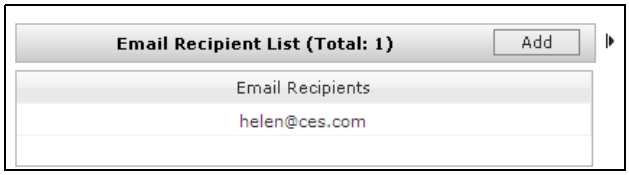
Choose **Monitor** > **Reports** > **Schedules** > **New**.

1. Configure the following basic report information.

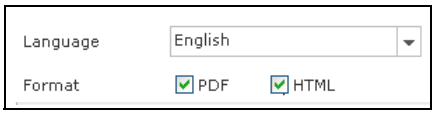


2. Set a report schedule.

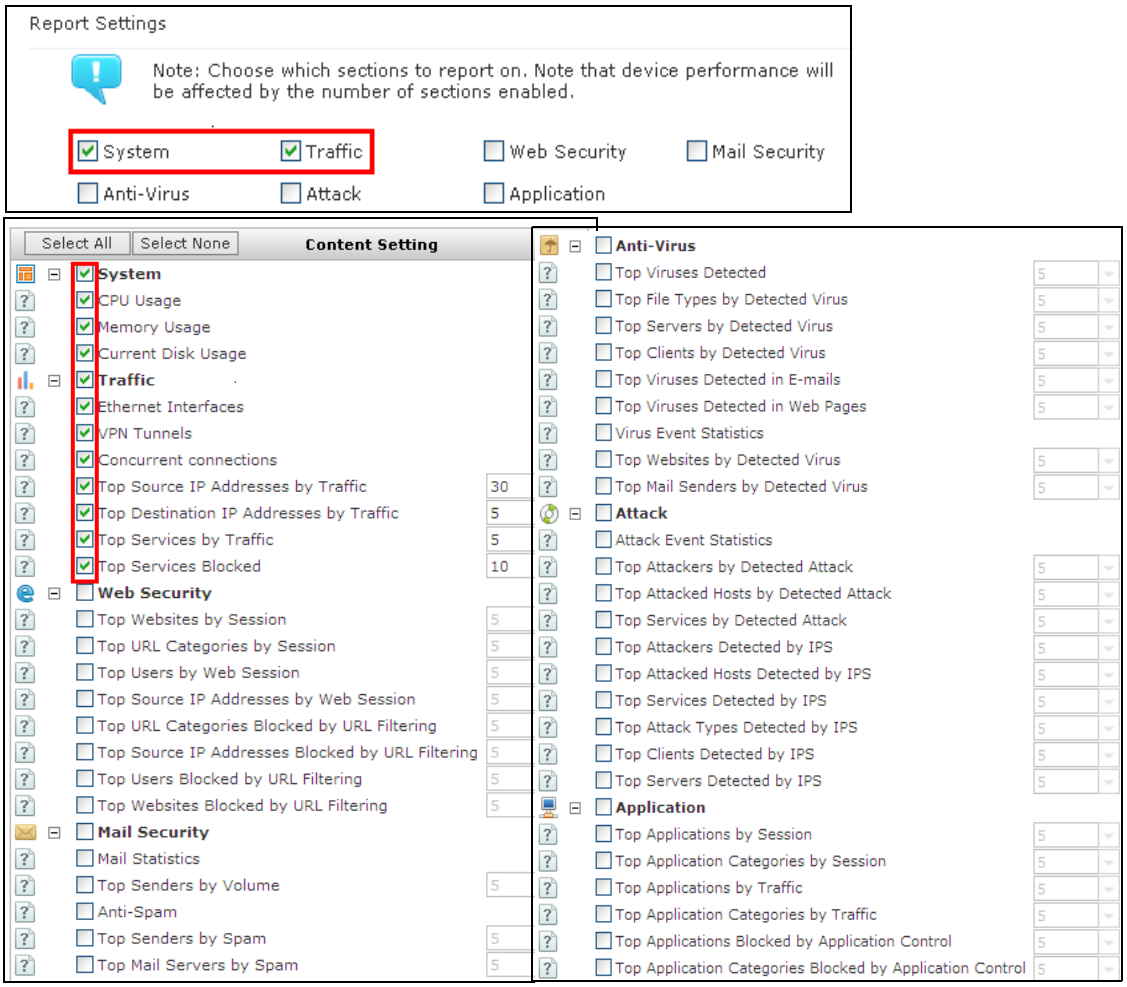
3. Create a report recipient.



4. Set report language and format.



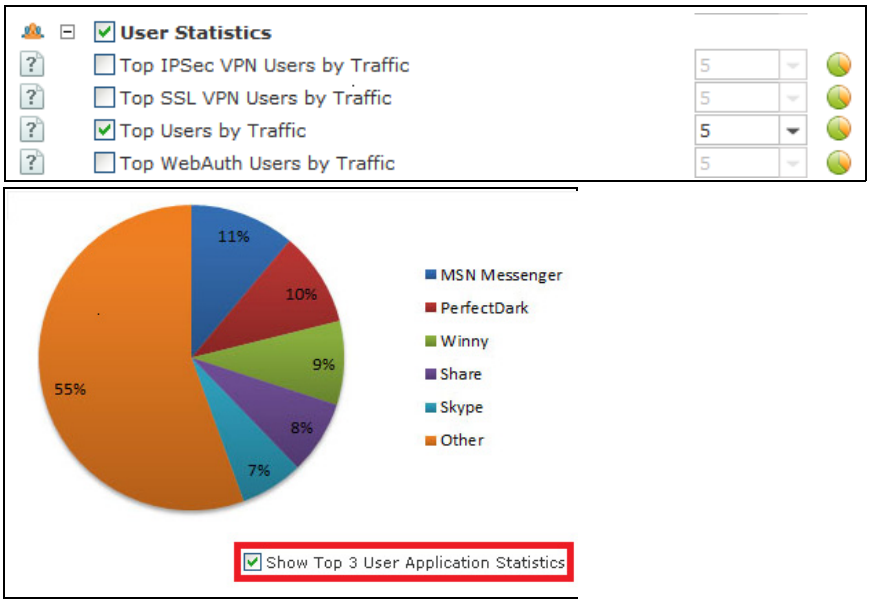
5. Choose content to be recorded in the **Content Setting** section.



Note: When you choose content in the **Content Setting** section, make sure that you enable the corresponding recording function in the **General Settings** > **Report Settings** section. Otherwise, the corresponding statistics will not be shown in the report.

6. Choose user content to record.

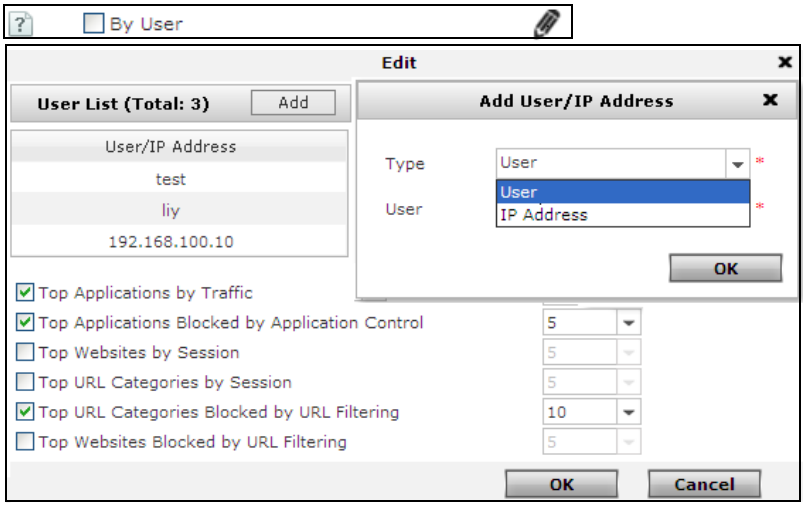
Click to view a pie chart showing top 5 applications of each of the top 3 users.



Note: To choose user content in the **Content Setting** section, you need to enable the recording function of **Traffic** in the **General Settings** > **Report Settings** section.

7. Add specific users or IP addresses.

FGX can record statistics about specified users. To add a specific user or IP address (up to 5 entries), click following By User.



Note: You can only choose users that already exist in the system.

8. View samples.

Click ? to view sample statistics of a certain category. Click **View Sample Report** at bottom of the Schedules page to view a sample report. You can also save the sample report to local.

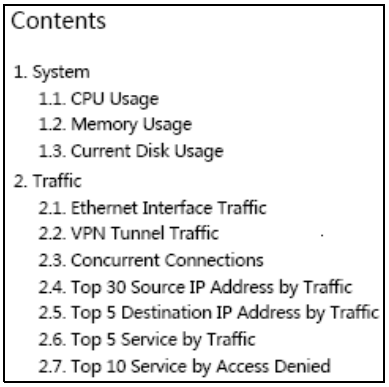
15.2.3 Manage Report Results

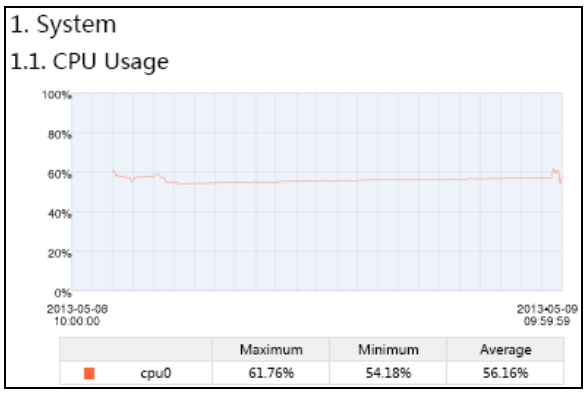
Choose **Monitor** > **Reports** > **Results**.

1. Delete report results or download them to local.

2. View report results.

   For details about report results, see 15.3.4 Global Content Parameters and 15.3.5 Per-User Content Parameters.





15.3 Parameter Reference

This section describes parameters used when configuring reporting function:

- 15.3.1 SMTP Server Parameters
- 15.3.2 Schedule Parameters
- 15.3.3 Report Result Parameters
- 15.3.4 Global Content Parameters
- 15.3.5 Per-User Content Parameters

15.3.1 SMTP Server Parameters

You can configure the system to send reports by e-mail.

Table 301 SMTP Server & Sender Information

Parameter	Description
Server Address	SMTP server address. A domain name or an IP address.
Port	SMTP server port number. 1-65535.
SSL	Used to enable or disable SSL encryption. It is disabled by default. When it is enabled, the server port number should be 465.
Sender	Sender e-mail address. 5-255 characters.
Identity Authentication	Used to enable or disable identity authentication. It is disabled by default. If the SMTP server requires identify authentication, you must enable it and configure: • **Username—**report sender user name. 1-63 UTF-8 characters except spaces and ? , ” ' \ < > & #. • **Password—**report sender password. 0-255 ASCII characters. Only ASCII 33-62 and 64-126 allowed.
Subject	E-mail subject. 0-64 UTF-8 characters except ? ' \.

15.3.2 Schedule Parameters

Table 302 Schedule Parameters

Parameter	Description
Name	Report name. 1-63 UTF-8 characters except spaces and ? , ” ' \ < > & #. Report names must be unique within a Vsys.
Report Title	1-63 UTF-8 characters. The default report title is FGX Security Report.
Report Description	Description about a report. 0-255 UTF-8 characters except spaces and ? , ” ' \ < > &.
Schedule	Used to set report generation schedules. A report can be generated daily, weekly, or monthly. By default, a report is generated daily at 01:00. • A weekly report is generated at 01:00 every Monday. • A monthly report is generated at 01:00 on the first day of every month.
Email Recipient List	E-mail addresses of recipients whom FGX will send reports to. You can set up to 32 e-mail addresses.
Language	Report languages, English and simplified Chinese. English by default.
Format	Report output formats, PDF and HTML. You can choose either format or both.
Content Setting	Sets content to be recorded about system, traffic statistics, Web security, mail security, anti-virus, attack, application, and user statistics. All are disabled by default. For information about each category, see 15.3.4 Global Content Parameters and 15.3.5 Per-User Content Parameters.

15.3.3 Report Result Parameters

Table 303 Result Parameters

Parameter	Description
Time	Date and time when a report is generated.
Name	Report name that is set in a report schedule.
Status	Indicates whether a report is generated successfully. Status can be Fail, Success, and Generating.
Information	Information about report generation: • Failed to connect SMTP server. • Failed to create report. A hyphen (-) indicates that a report has been generated successfully or is being generated.
Report File	Provides links for you to download a generated report, in PDF or HTML.

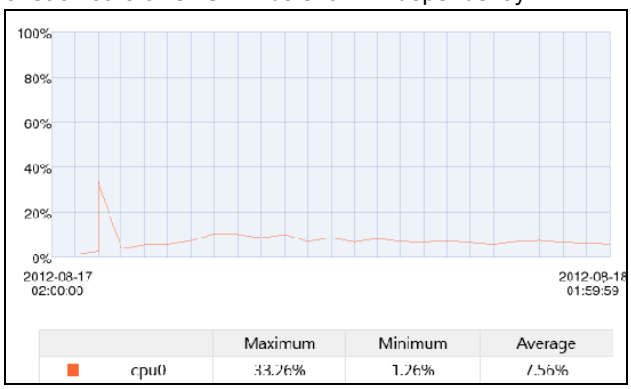
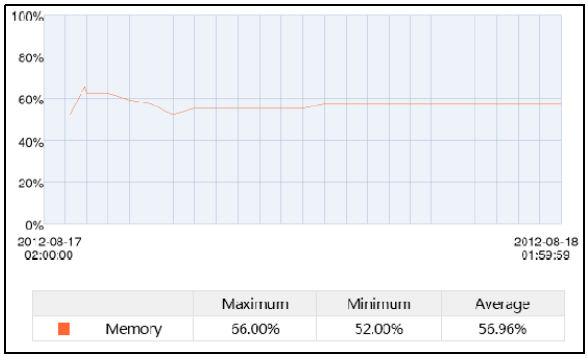
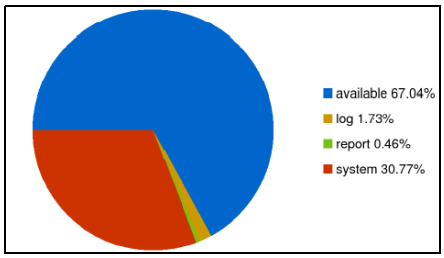
15.3.4 Global Content Parameters

This section explains specific information to be shown in a report and gives report samples. Content of the following categories can be recorded:

- 15.3.4.1 System
- 15.3.4.2 Traffic
- 15.3.4.3 Web Security
- 15.3.4.4 Mail Security
- 15.3.4.5 Anti-Virus
- 15.3.4.6 Attack
- 15.3.4.7 Application
- 15.3.4.8 User Statistics

15.3.4.1 System

Table 304 System Information

Type	Description
CPU Usage	The system generates statistics about CPU usage every 5 minutes. Information of each core or CPU will be shown independently.  The y-axis in the graph represents CPU utilization percentage. Each point represents the average value within 5 minutes.
Memory Usage	The system generates statistics about memory usage every 5 minutes.  The y-axis in the graph represents memory utilization percentage. Each point represents the average value within 5 minutes.
Current Disk Usage	The system generates statistics about current disk usage when a report is generated. 

15.3.4.2 Traffic

Table 305 Traffic Information

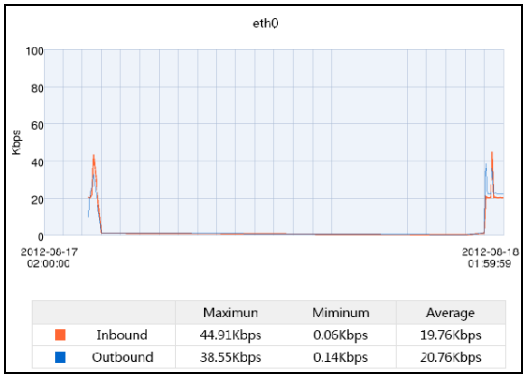
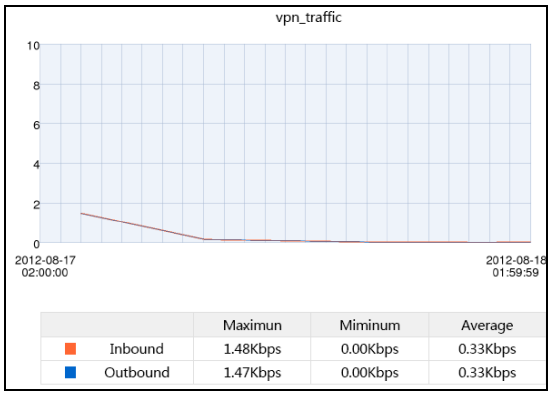
Type	Description
Ethernet Interfaces	The system generates statistics about inbound and outbound traffic of Ethernet interfaces every 5 minutes.  Each point in the graph represents the average value within 5 minutes.
VPN Tunnels	The system generates statistics about inbound and outbound traffic of VPN tunnels every 5 minutes. Reports display data for only the latest 10 enabled site-to-site auto IKE VPN tunnels.  Each point in the line graph represents in the average value within 5 minutes.

Table 305 Traffic Information (*continued*)

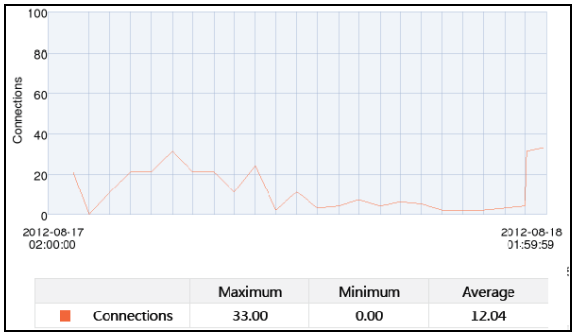
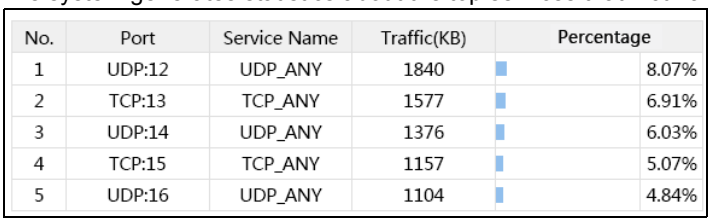
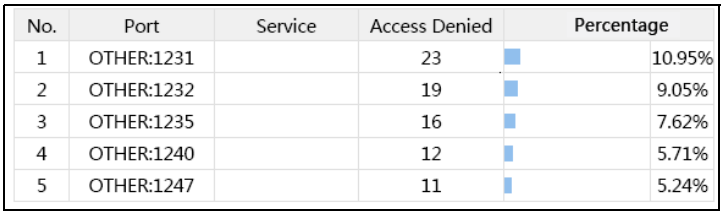
Type	Description
Concurrent Connections	The system generates statistics about total number of concurrent connections every 5 minutes.  Each point in the line graph represents the total number within 5 minutes.
Top Source IP Addresses by Traffic	The system generates statistics about the top source IP addresses with maximum traffic. No. | Source IP | Traffic(KB) | Percentage 1 | 192.168.111.2 | 1902 | 8.34% 2 | 192.168.111.3 | 1706 | 7.48% 3 | 192.168.111.4 | 1560 | 6.84% 4 | 192.168.111.5 | 1329 | 5.83% 5 | 192.168.111.6 | 1290 | 5.66% • Traffic (KB): Total traffic from a source IP address. • Percentage: Percentage of total traffic from a source IP address, out of the total traffic.
Top Destination IP Addresses by Traffic	The system generates statistics about the top destination IP addresses with maximum traffic. No. | Dst IP | Traffic(KB) | Percentage 1 | 192.168.101.2 | 1902 | 8.34% 2 | 192.168.101.3 | 1706 | 7.48% 3 | 192.168.101.4 | 1560 | 6.84% 4 | 192.168.101.5 | 1329 | 5.83% 5 | 192.168.101.6 | 1290 | 5.66% • Traffic (KB): Total traffic sent to a destination IP address. • Percentage: Percentage of total traffic sent to a destination IP address, out of the total traffic.

Table 305 Traffic Information (*continued*)

Type	Description
Top Services by Traffic	The system generates statistics about the top services that incur a maximum traffic.  • Port: Destination port number. If there is no port number, protocol number will be shown; for example, Other: 44. • Service Name: Name of service object using a certain destination port number. • Traffic (KB): Total traffic sent to a destination port number. • Percentage: Percentage of total traffic sent to a destination port number, out of the total traffic.
Top Services Blocked	The system generates statistics about the top services that are most blocked by access policies.  • Access Denied: Total number of times that a destination port number is blocked by access policies. • Percentage: Percentage of total number of times that a destination port number is blocked by access policies, out of the total number of times that all port numbers are blocked by access policies.

15.3.4.3 Web Security

Table 306 Web Security Information

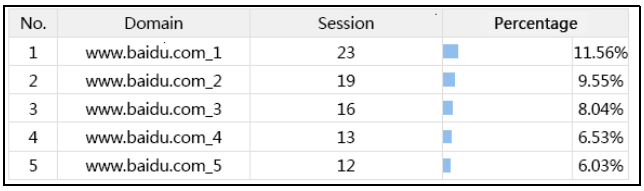
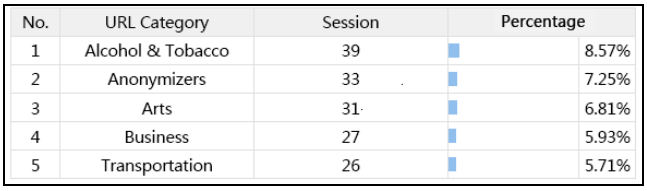
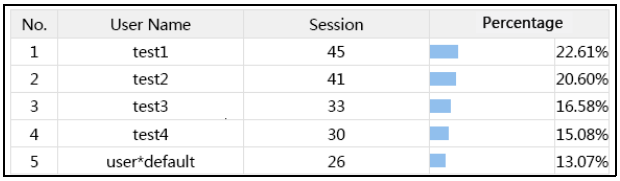
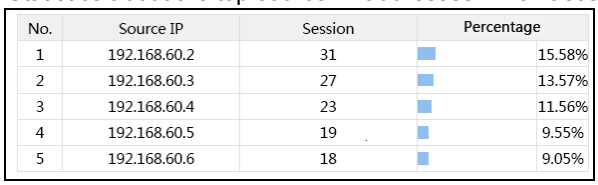
Type	Description
Top Websites by Session	Statistics about the top Websites that are most accessed.  No. / Domain / Session / Percentage 1 / www.baidu.com_1 / 23 / 11.56% 2 / www.baidu.com_2 / 19 / 9.55% 3 / www.baidu.com_3 / 16 / 8.04% 4 / www.baidu.com_4 / 13 / 6.53% 5 / www.baidu.com_5 / 12 / 6.03% • Session: Total number of times that a Website is accessed. • Percentage: Percentage of total number of times that a Website is accessed, out of the total number of times that all Websites are accessed.
Top URL Categories by Session	Statistics about the top URL categories that are most accessed.  No. / URL Category / Session / Percentage 1 / Alcohol & Tobacco / 39 / 8.57% 2 / Anonymizers / 33 / 7.25% 3 / Arts / 31 / 6.81% 4 / Business / 27 / 5.93% 5 / Transportation / 26 / 5.71%
Top Users by Web Session	Statistics about the top users who access Websites most.  No. / User Name / Session / Percentage 1 / test1 / 45 / 22.61% 2 / test2 / 41 / 20.60% 3 / test3 / 33 / 16.58% 4 / test4 / 30 / 15.08% 5 / user*default / 26 / 13.07% Percentage: Percentage of total number of times that a user accesses Websites, out of the total number of times that all users access Websites.
Top Source IP Addresses by Web Session	Statistics about the top source IP addresses which access the Web.  No. / Source IP / Session / Percentage 1 / 192.168.60.2 / 31 / 15.58% 2 / 192.168.60.3 / 27 / 13.57% 3 / 192.168.60.4 / 23 / 11.56% 4 / 192.168.60.5 / 19 / 9.55% 5 / 192.168.60.6 / 18 / 9.05% Percentage: Percentage of total number of times that an IP address accesses the Web, out of the total number of Web access times.

Table 306 Web Security Information (*continued*)

Type	Description
Top URL Categories Blocked by URL Filtering	Statistics about the top URL categories that are most blocked by URL filtering. No. / URL Category / URL Filtering Blocked / Percentage 1 / Alcohol & Tobacco / 39 / 8.57% 2 / Anonymizers / 33 / 7.25% 3 / Arts / 31 / 6.81% 4 / Business / 27 / 5.93% 5 / Transportation / 26 / 5.71% • URL Filtering Blocked: Total number of times that a URL category is blocked by URL filtering. • Percentage: Percentage of total number of times that a URL category is blocked by URL filtering, out of the total number of times that all URL categories are blocked by URL filtering.
Top Source IP Addresses Blocked by URL Filtering	Statistics about the top source IP addresses that are most blocked by URL filtering. No. / Source IP / URL Filtering Blocked / Percentage 1 / 192.168.60.2 / 58 / 12.75% 2 / 192.168.60.3 / 52 / 11.43% 3 / 192.168.60.4 / 50 / 10.99% 4 / 192.168.60.5 / 46 / 10.11% 5 / 192.168.60.6 / 45 / 9.89%
Top Users Blocked by URL Filtering	Statistics about the top users who are most blocked by URL filtering. No. / User Name / URL Filtering Blocked / Percentage 1 / test1 / 90 / 19.78% 2 / test2 / 84 / 18.46% 3 / test3 / 76 / 16.70% 4 / test4 / 71 / 15.60% 5 / user*default / 68 / 14.95%
Top Websites Blocked by URL Filtering	Statistics about the top Websites that are most blocked by URL filtering. No. / Domain / URL Filtering Blocked / Percentage 1 / www.baidu.com_1 / 24 / 5.27% 2 / www.baidu.com_2 / 18 / 3.96% 3 / www.baidu.com_3 / 16 / 3.52% 4 / www.baidu.com_4 / 13 / 2.86% 5 / www.baidu.com_5 / 12 / 2.64%

15.3.4.4 Mail Security

Table 307 Mail Security Information

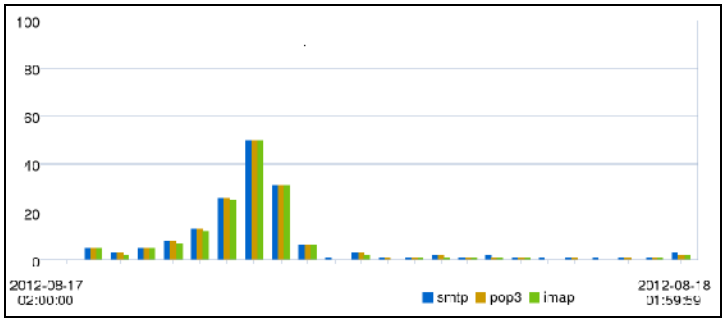
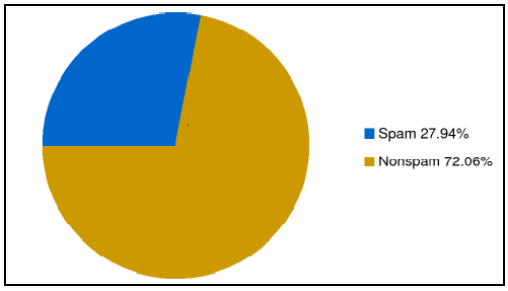
Type	Description
Mail Statistics	The system generates statistics about total number of e-mails using SMTP, POP3, and IMAP every 1 hour for daily reports, every 6 hours for weekly reports, and every 24 hours for monthly reports.  The bar chart above is a daily report sample. The y-axis represents the number of received and sent e-mails for a daily report. Each point represents the total number of e-mails within 1 hour.
Top Senders by Volume	Statistics about the top e-mail senders who send e-mails most. No. | Sender | Mails | Percentage 1 | bbbb_1@hmail.com | 30 | 17.96% 2 | bbbb_5@hmail.com | 18 | 10.78% 3 | bbbb_9@hmail.com | 15 | 8.98% 4 | bbbb_13@hmail.com | 13 | 7.78% 5 | bbbb_17@hmail.com | 13 | 7.78% • Mails: Total number of e-mails that a sender sends. • Percentage: Percentage of total number of e-mails that a sender sends, out of the total number of e-mails.
Anti-Spam	Percentage of spam out of the total number of e-mails. 

Table 307 Mail Security Information (*continued*)

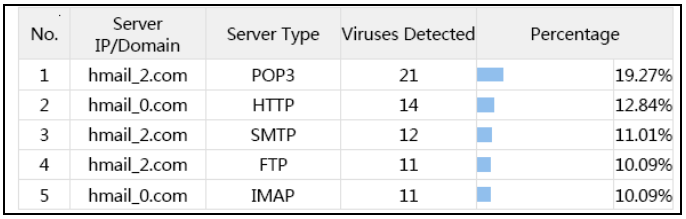
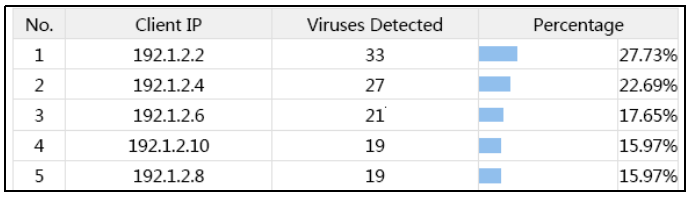
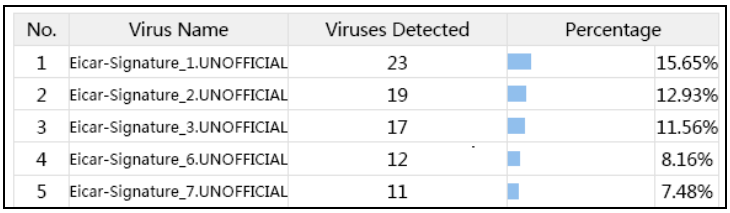
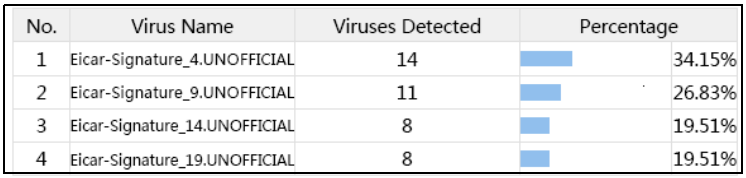
Type	Description
Top Senders by Spam	Statistics about the top senders who send spam most. No. | Sender | Spam Mails | Percentage 1 | bbbb_1@hmail_1.com | 24 | 13.64% 2 | bbbb_2@hmail_2.com | 16 | 9.09% 3 | bbbb_3@hmail_3.com | 13 | 7.39% 4 | bbbb_4@hmail_0.com | 11 | 6.25% 5 | bbbb_5@hmail_1.com | 11 | 6.25%
Top Mail Servers by Spam	Statistics about the top mail servers that send spam most. No. | Mail Server Domain | Spam Mails | Percentage 1 | hmail_1.com | 57 | 32.39% 2 | hmail_2.com | 48 | 27.27% 3 | hmail_3.com | 37 | 21.02% 4 | hmail_0.com | 34 | 19.32%

15.3.4.5 Anti-Virus

Table 308 Anti-Virus Information

Type	Description
Top Viruses Detected	Statistics about the top viruses that are most detected. No. | Virus Name | Viruses Detected | Percentage 1 | Eicar-Signature_1.UNOFFICIAL | 23 | 10.09% 2 | Eicar-Signature_2.UNOFFICIAL | 19 | 8.33% 3 | Eicar-Signature_3.UNOFFICIAL | 17 | 7.46% 4 | Eicar-Signature_4.UNOFFICIAL | 14 | 6.14% 5 | Eicar-Signature_5.UNOFFICIAL | 13 | 5.70% • Viruses Detected: Total number of times that a virus is detected. • Percentage: Percentage of total number of times that a virus is detected, out of the total number of times that viruses are detected.
Top File Types by Detected Virus	Statistics about the top file types in which viruses are most detected. No. | File Type | Viruses Detected | Percentage 1 | rar | 50 | 21.93% 2 | zip | 46 | 20.18% 3 | txt | 38 | 16.67% 4 | dat | 35 | 15.35% 5 | jpg | 31 | 13.60%

Table 308 Anti-Virus Information (*continued*)

Type	Description
Top Servers by Detected Virus	Statistics about the top servers in which server protection detects viruses most times.  • Viruses Detected: Total number of times that server protection detects viruses in a server. • Percentage: Percentage of total number of times that server protection detects viruses in a server, out of the total number of times that server protection detects viruses.
Top Clients by Detected Virus	Statistics about the top clients in which client protection detects viruses most times.  • Viruses Detected: Total number of times that client protection detects viruses in a client. • Percentage: Percentage of total number of times that client protection detects viruses in a client, out of the total number of times that client protection detects viruses.
Top Viruses Detected in E-mails	Statistics about the top viruses that are most detected in e-mails. 
Top Viruses Detected in Web Pages	Statistics about the top viruses that are detected most times in Web pages. 

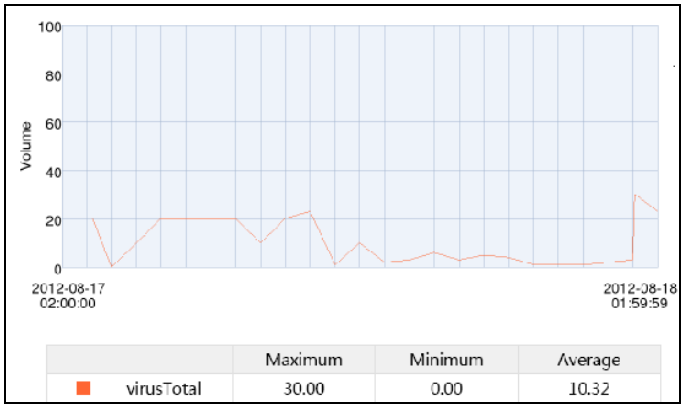
No.	Server IP/Domain	Server Type	Viruses Detected	Percentage
1	hmail_2.com	POP3	21	19.27%
2	hmail_0.com	HTTP	14	12.84%
3	hmail_2.com	SMTP	12	11.01%
4	hmail_2.com	FTP	11	10.09%
5	hmail_0.com	IMAP	11	10.09%

No.	Client IP	Viruses Detected	Percentage
1	192.1.2.2	33	27.73%
2	192.1.2.4	27	22.69%
3	192.1.2.6	21	17.65%
4	192.1.2.10	19	15.97%
5	192.1.2.8	19	15.97%

No.	Virus Name	Viruses Detected	Percentage
1	Eicar-Signature_1.UNOFFICIAL	23	15.65%
2	Eicar-Signature_2.UNOFFICIAL	19	12.93%
3	Eicar-Signature_3.UNOFFICIAL	17	11.56%
4	Eicar-Signature_6.UNOFFICIAL	12	8.16%
5	Eicar-Signature_7.UNOFFICIAL	11	7.48%

No.	Virus Name	Viruses Detected	Percentage
1	Eicar-Signature_4.UNOFFICIAL	14	34.15%
2	Eicar-Signature_9.UNOFFICIAL	11	26.83%
3	Eicar-Signature_14.UNOFFICIAL	8	19.51%
4	Eicar-Signature_19.UNOFFICIAL	8	19.51%

Table 308 Anti-Virus Information (*continued*)

Type	Description
Virus Event Statistics	The system generates statistics about total number of times that viruses are detected every 5 minutes.  Maximum / Minimum / Average virusTotal: 30.00 / 0.00 / 10.32 The y-axis in the line graph above represents the number of times that viruses are detected. Each point represents the total number of times within 5 minutes.
Top Websites by Detected Virus	Statistics about the top Websites in which viruses are detected most times. No. / Web Site / Viruses Detected / Percentage 1 / hmail_0.com / 14 / 34.15% 2 / hmail_1.com / 11 / 26.83% 3 / hmail_2.com / 8 / 19.51% 4 / hmail_3.com / 8 / 19.51%
Top Mail Senders by Detected Virus	Statistics about the top senders in whose e-mails viruses are detected most times. No. / Sender / Viruses Detected / Percentage 1 / bbbb_1@hmail_1.com / 23 / 15.65% 2 / bbbb_2@hmail_2.com / 19 / 12.93% 3 / bbbb_3@hmail_3.com / 17 / 11.56% 4 / bbbb_6@hmail_2.com / 12 / 8.16% 5 / bbbb_7@hmail_3.com / 11 / 7.48%

15.3.4.6 Attack

Table 309 Attack Information

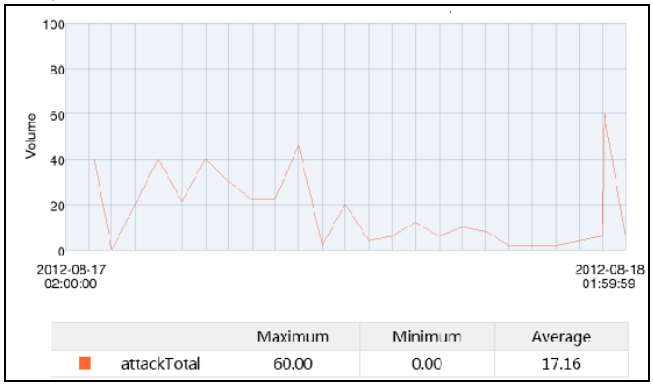
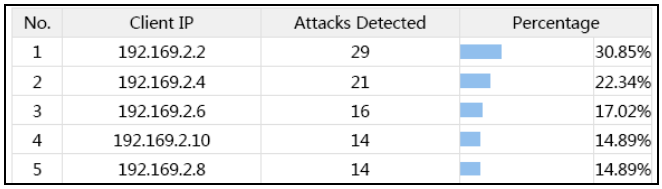
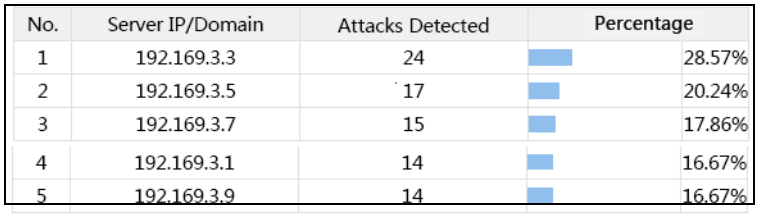
Type	Description
Attack Event Statistics	The system generates statistics about total number of times that attacks occur every 5 minutes.  The y-axis in the line graph above represents the number of times that attacks occur. Each point represents the total number of times within 5 minutes.
Top Attackers by Detected Attack	Statistics about the top attackers who launch attacks most. No. / Attacker / Attacks Detected / Percentage 1 / 10.168.1.2 / 31 / 8.40% 2 / 192.169.3.2 / 29 / 7.86% 3 / 10.168.1.3 / 27 / 7.32% 4 / 192.169.2.3 / 24 / 6.50% 5 / 10.168.1.4 / 22 / 5.96% • Attacker: Attacker IP address. • Attacks Detected: Total number of attacks that an attacker launches. • Percentage: Percentage of total number of attacks that an attacker launches, out of the total number of attacks detected.
Top Attacked Hosts by Detected Attack	Statistics about the top hosts that are most attacked. No. / Attacked Host / Attacks Detected / Percentage 1 / 10.2.1.2 / 31 / 8.40% 2 / 192.169.2.2 / 29 / 7.86% 3 / 10.2.1.3 / 27 / 7.32% 4 / 192.169.3.3 / 24 / 6.50% 5 / 10.2.1.4 / 22 / 5.96%

Table 309 Attack Information (*continued*)

Type	Description
Top Services by Detected Attack	Statistics about the top services that are most attacked. No. | Port | Service | Attacks Detected | Percentage 1 | TCP:280 | TCP_ANY | 23 | 8.42% 2 | OTHER:1231 | | 23 | 8.42% 3 | OTHER:1232 | | 19 | 6.96% 4 | UDP:281 | UDP_ANY | 18 | 6.59% 5 | OTHER:1235 | | 15 | 5.49% • Port: Destination port number. If there is no port number, protocol number will be shown; for example, Other: 44. • Service: Name of service object using a certain destination port number.
Top Attackers Detected by IPS	Statistics about the top attackers who launch attacks most times, detected by IPS. No. | Attacker | Attacks Detected | Percentage 1 | 192.169.3.2 | 29 | 16.29% 2 | 192.169.2.3 | 24 | 13.48% 3 | 192.169.3.4 | 21 | 11.80% 4 | 192.169.2.5 | 17 | 9.55% 5 | 192.169.3.6 | 16 | 8.99% • Attacks Detected: Total number of times that an attacker launches attacks, detected by IPS. • Percentage: Percentage of total number of times that an attacker launches attacks, detected by IPS, out of the total number of times that attacks are detected by IPS.
Top Attacked Hosts Detected by IPS	Statistics about the top hosts that are most attacked, detected by IPS. No. | Attacked Host | Attacks Detected | Percentage 1 | 192.169.2.2 | 29 | 16.29% 2 | 192.169.3.3 | 24 | 13.48% 3 | 192.169.2.4 | 21 | 11.80% 4 | 192.169.3.5 | 17 | 9.55% 5 | 192.169.2.6 | 16 | 8.99%
Top Services Detected by IPS	Statistics about the top services that are most attacked, detected by IPS and attack defense. No. | Port | Service | Attacks Detected | Percentage 1 | TCP:280 | TCP_ANY | 23 | 28.05% 2 | UDP:281 | UDP_ANY | 18 | 21.95% 3 | TCP:285 | TCP_ANY | 10 | 12.20% 4 | UDP:286 | UDP_ANY | 9 | 10.98% 5 | TCP:290 | TCP_ANY | 5 | 6.10%
Top Attack Types Detected by IPS	Statistics about the top types of attacks that occur most, detected by IPS. No. | Attack Type | Attacks Detected | Percentage 1 | UNKNOWN | 104 | 58.43% 2 | INPUT VALIDATE FAILED | 44 | 24.72% 3 | CROSS-SITE SCRIPTING | 30 | 16.85%

Table 309 Attack Information (*continued*)

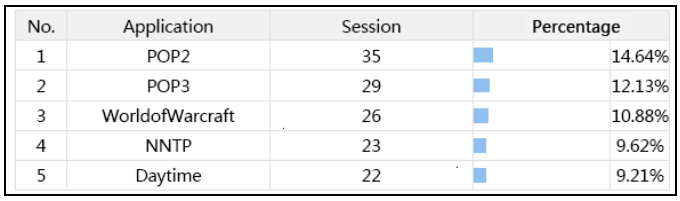
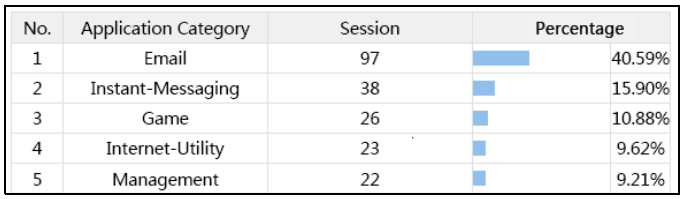
Type	Description
Top Clients Detected by IPS	Statistics about the top clients that are most attacked, detected by IPS in client protection.  • Attacks Detected: Total number of times that a client is attacked, detected by IPS in client protection. • Percentage: Percentage of total number of times that a client is attacked, detected by IPS in client protection, out of the total number of times that attacks are detected by IPS in client protection.
Top Servers Detected by IPS	Statistics about the top servers that are most attacked, detected by IPS in server protection.  • Attacks Detected: Total number of times that a server is attacked, detected by IPS in server protection. • Percentage: Percentage of total number of times that a server is attacked, detected by IPS in server protection, out of the total number of times that attacks are detected by IPS in server protection.

15.3.4.7 Application

Table 310 Application Information

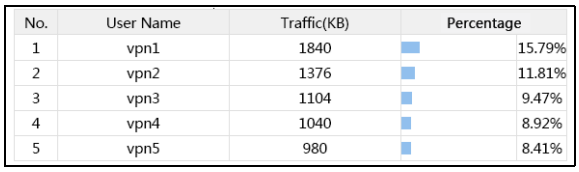
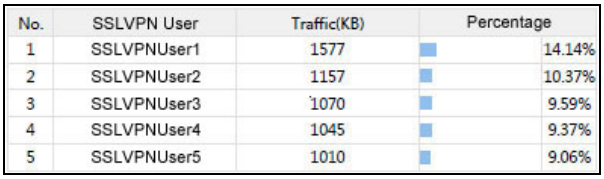
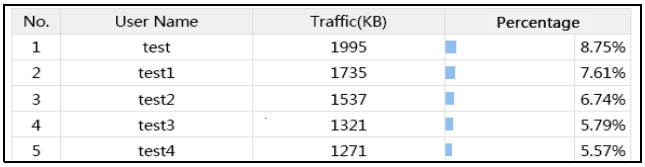
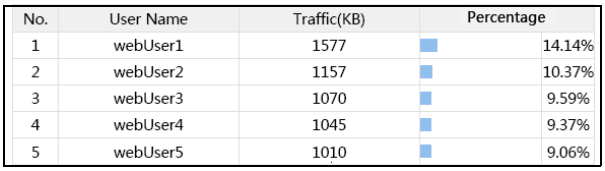
Type	Description
Top Applications by Session	Statistics about the top applications that have most sessions. No. | Application | Session | Percentage 1 | WorldofWarcraft | 23 | 10.04% 2 | NNTP | 19 | 8.30% 3 | Daytime | 16 | 6.99% 4 | IMAP | 13 | 5.68% 5 | MSN | 12 | 5.24% • Application: Application name. • Session: Total number of sessions that an application has. • Percentage: Percentage of total number of sessions that an application has, out of the total number of all application sessions.
Top Application Categories by Session	Statistics about the top application categories that have most sessions. No. | Application Category | Session | Percentage 1 | Instant-Messaging | 39 | 17.03% 2 | Game | 30 | 13.10% 3 | Management | 30 | 13.10% 4 | Internet-Utility | 27 | 11.79% 5 | Email | 23 | 10.04%
Top Applications by Traffic	Statistics about the top applications that incur most traffic. No. | Application | Traffic(KB) | Percentage 1 | POP2 | 2923 | 12.82% 2 | POP3 | 2538 | 11.13% 3 | WorldofWarcraft | 2361 | 10.35% 4 | NNTP | 2166 | 9.50% 5 | Daytime | 2137 | 9.37% • Traffic (KB): Total traffic that an application incurs. • Percentage: Percentage of total traffic that an application incurs, out of the total application traffic.
Top Application Categories by Traffic	Statistics about the top application categories that incur most traffic. No. | Application Category | Traffic(KB) | Percentage 1 | Email | 8619 | 37.79% 2 | Instant-Messaging | 4176 | 18.31% 3 | Game | 2361 | 10.35% 4 | Internet-Utility | 2166 | 9.50% 5 | Management | 2137 | 9.37%

Table 310 Application Information (*continued*)

Type	Description
Top Applications Blocked by Application Control	Statistics about the top applications whose sessions are most blocked by application control.  • Session: Total number of sessions of an application, blocked by application control. • Percentage: Percentage of total number of sessions of an application, blocked by application control, out of the total number of all application sessions that are blocked by application control.
Top Application Categories Blocked by Application Control	Statistics about the top application categories whose sessions are most blocked by application control. 

15.3.4.8 User Statistics

Table 311 User Information

Type	Information
Top IPSec VPN Users by Traffic	Statistics about the top IPSec VPN users with maximum traffic.  No. / User Name / Traffic(KB) / Percentage 1 / vpn1 / 1840 / 15.79% 2 / vpn2 / 1376 / 11.81% 3 / vpn3 / 1104 / 9.47% 4 / vpn4 / 1040 / 8.92% 5 / vpn5 / 980 / 8.41% • Traffic (KB): Total traffic that an IPSec VPN user incurs. • Percentage: Percentage of total traffic that an IPSec VPN user incurs, out of the total IPSec VPN user traffic.
Top SSL VPN Users by Traffic	Statistics about the top SSL VPN users with maximum traffic.  No. / SSLVPN User / Traffic(KB) / Percentage 1 / SSLVPNUser1 / 1577 / 14.14% 2 / SSLVPNUser2 / 1157 / 10.37% 3 / SSLVPNUser3 / 1070 / 9.59% 4 / SSLVPNUser4 / 1045 / 9.37% 5 / SSLVPNUser5 / 1010 / 9.06% • Traffic (KB): Total traffic that an SSL VPN user incurs. • Percentage: Percentage of total traffic that an SSL VPN user incurs, out of the total SSL VPN user traffic.
Top Users by Traffic	Statistics about the top VPN users and WebAuth users with maximum traffic.  No. / User Name / Traffic(KB) / Percentage 1 / test / 1995 / 8.75% 2 / test1 / 1735 / 7.61% 3 / test2 / 1537 / 6.74% 4 / test3 / 1321 / 5.79% 5 / test4 / 1271 / 5.57% • Traffic (KB): Total traffic that a user incurs. • Percentage: Percentage of total traffic that a user incurs, out of the total user traffic.
Top WebAuth Users by Traffic	Statistics about the top WebAuth users with maximum traffic.  No. / User Name / Traffic(KB) / Percentage 1 / webUser1 / 1577 / 14.14% 2 / webUser2 / 1157 / 10.37% 3 / webUser3 / 1070 / 9.59% 4 / webUser4 / 1045 / 9.37% 5 / webUser5 / 1010 / 9.06% • Traffic (KB): Total traffic that a WebAuth user incurs. • Percentage: Percentage of total traffic that a WebAuth user incurs, out of the total WebAuth user traffic.

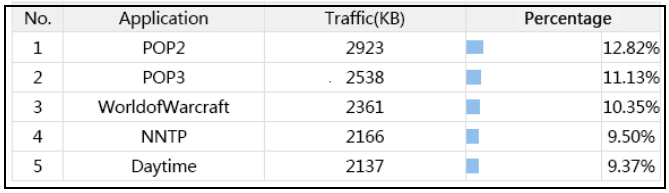
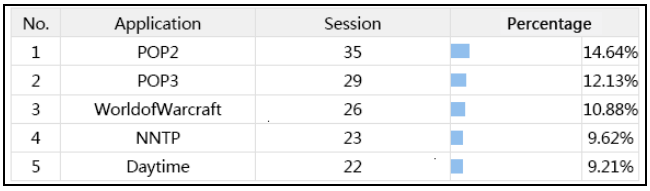
15.3.5 Per-User Content Parameters

You can choose the following content for specified users or IP addresses:

- 15.3.5.1 Application
- 15.3.5.2 Web Security

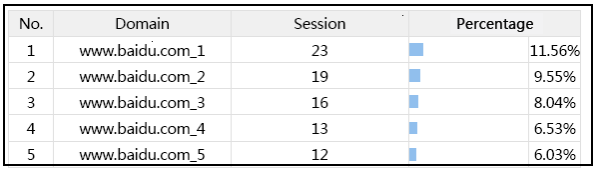
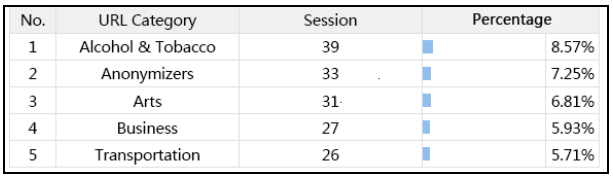
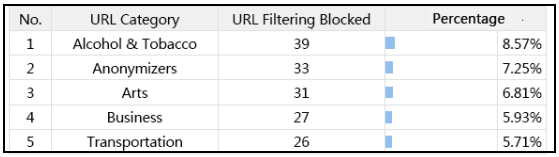
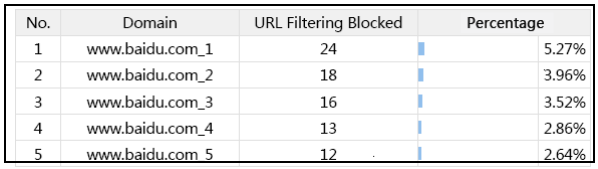
15.3.5.1 Application

Table 312 Application Information of Specific Users or IP Addresses

Type	Description
Top Applications by Traffic	Statistics about the top applications that are accessed by a specific user or IP address and incur most traffic.  • Traffic (KB): Total traffic of an application. • Percentage: Percentage of total traffic of an application, out of the total application traffic of the user or IP address.
Top Applications Blocked by Application Control	Statistics about the top applications that are accessed by a specific user or IP address and are most blocked by application control.  • Session: Total number of sessions of an application blocked by application control. • Percentage: Percentage of total number of sessions of an application blocked by application control, out of the total number of the user or IP address's all application sessions that are blocked by application control.

15.3.5.2 Web Security

Table 313 Web Security Information of Specific Users

Type	Description
Top Websites by Session	Statistics about the top Websites that are most accessed by a specific user or IP address.  • Session: Total number of times that a Website is accessed. • Percentage: Percentage of total number of times that a Website is accessed, out of the total number of times that all Websites are accessed by the user or IP address.
Top URL Categories by Session	Statistics about the top URL categories that are most accessed by a specific user or IP address.  • Session: Total number of times that a URL category is accessed. • Percentage: Percentage of total number of times that a URL category is accessed, out of the total number of times that all URL categories are accessed by the user or IP address.
Top URL Categories Blocked by URL Filtering	Statistics about the top URL categories that are accessed by a specific user or IP address and are most blocked by URL filtering.  • URL Filtering Blocked: Total number of times that a URL category is blocked by URL filtering. • Percentage: Percentage of total number of times that a URL category is blocked by URL filtering, out of the total number of times that all URL categories accessed by the user or IP address are blocked by URL filtering.
Top Websites Blocked by URL Filtering	Statistics about the top Websites that are accessed by a specific user or IP address and are most blocked by URL filtering.  Percentage: Percentage of total number of times that a Website is blocked by URL filtering, out of the total number of times that all Websites accessed by the user or IP address are blocked by URL filtering.

No.	Domain	Session	Percentage
1	www.baidu.com_1	23	11.56%
2	www.baidu.com_2	19	9.55%
3	www.baidu.com_3	16	8.04%
4	www.baidu.com_4	13	6.53%
5	www.baidu.com_5	12	6.03%

No.	URL Category	Session	Percentage
1	Alcohol & Tobacco	39	8.57%
2	Anonymizers	33	7.25%
3	Arts	31	6.81%
4	Business	27	5.93%
5	Transportation	26	5.71%

No.	URL Category	URL Filtering Blocked	Percentage
1	Alcohol & Tobacco	39	8.57%
2	Anonymizers	33	7.25%
3	Arts	31	6.81%
4	Business	27	5.93%
5	Transportation	26	5.71%

No.	Domain	URL Filtering Blocked	Percentage
1	www.baidu.com_1	24	5.27%
2	www.baidu.com_2	18	3.96%
3	www.baidu.com_3	16	3.52%
4	www.baidu.com_4	13	2.86%
5	www.baidu.com_5	12	2.64%

A MIBs

The following table lists private MIBs.

Table 314 Private MIBs

	1. fwSystemInfoGroup	
1	fwProductName	Name of the product
2	fwProductVer	Version of the product
3	fwRegMsg	Registration message
4	fwName	Name of the system
	2. fwRunningStatGroup	
5	fwCpuUsage	Utilization of CPU
6	fwMemUsage	Utilization of the memory
	3. fwChannelGroup	
	fwChannelTable /fwChannelEntry	
7	fwChannelIndex	Index of the channel
8	fwChannelName	Name of the channel
9	fwChannelStat	Status of the channel
10	fwChannelMode	Mode of the channel
11	fwChannelNativeVlan	Default VLAN of the channel
12	fwChannelIncludePorts	Ports included in the channel
13	fwChannelBelowInterfaces	Interfaces the channel belongs to
	4. fwVlanGroup	
	fwVlanTable / fwVlanEntry	
14	fwVlanIndex	Index of the VLAN
15	fwVlanName	Name of the VLAN
16	fwVlanStat	Status of the VLAN
17	fwVlanMTU	MTU of the VLAN
18	fwVlanMAC	MAC address of the VLAN
19	fwVlanIP	IP address of the VLAN

Table 314 Private MIBs

20	fwVlanBelowVsys	Vsys the VLAN belongs to
21	fwVlanIncludePorts	Ports included in the VLAN
22	fwVlanTXPackets	Number of packets sent in the VLAN
23	fwVlanRXPackets	Number of packets received in the VLAN
24	fwVlanTXBytes	Bytes sent in the VLAN
25	fwVlanRXBytes	Bytes received in the VLAN
	5. fwVsysGroup	
	fwVsysTable/fwVsysEntry	
26	fwVsysIndex	Index of the Vsys
27	fwVsysName	Name of the Vsys
28	fwVsysStat	Status of the Vsys
29	fwVsysResourcePercent	Percentage of the Vsys resource
30	fwIncludeVlans	Number of VLANs included in the Vsys
	6. fwSecureZoneGroup	
	fwSecureZoneTable/fwSecureZoneEntry	
31	fwSecureZoneIndex	Index of the zone
32	fwSecureZoneName	Name of the zone
33	fwSecureZoneInternalRule	Intra-zone policy of the zone
34	fwSecureZoneIncludeInterfaces	Interfaces included in the zone
35	fwSecureZoneIncludePorts	Ports included in the zone
	7. fwUserGroup	
	fwUserTable/fwUserEntry	
36	fwUserIndex	Index of the user
37	fwUserName	Name of the user
38	fwUserBelowVsys	Vsys the user belongs to
	8. fwVPNTunnelGroup	
	8.1. fwVPNAutoTunnelTable/fwVPNAutoTunnelEntry	
39	fwVPNAutoTunnelIndex	Index of the VPN automatic tunnel
40	fwVPNAutoTunnelName	Name of the VPN automatic tunnel
41	fwVPNAutoTunnelState	Status of the VPN automatic tunnel
42	fwVPNAutoTunnelRemoteType	Auto remote peer type: Dynamic IP, Static IP, Dial-Up User, or Dial-Up User Group
43	fwVPNAutoTunnelRemoteInfo	Auto remote peer information. It can be a dynamic IP, a static IP, a dial-up user, or a dial-up user group.
	8.2. fwVPNManualTunnelTable/fwVPNManualTunnelEntry	
44	fwVPNManualTunnelIndex	Index of the VPN manual tunnel

Table 314 Private MIBs

45	fwVPNManualTunnelName	Name of the VPN manual tunnel
46	fwVPNManualTunnelState	Status of the VPN manual tunnel
47	fwVPNManualTunnelRemoteType	Manual remote peer type: Static IP
48	fwVPNManualTunnelRemoteInfo	Manual remote peer information. It can be a static IP.
	9. fwChassisGroup	
	9.1. fwChassisSerialNumber	
49	fwChassisSerialNumber	Serial number of the chassis
	9.2. fwChassisMBType	
50	fwChassisMBType	Type of the chassis motherboard
	9.3. fwChassisMBRevNumber	
51	fwChassisMBRevNumber	Revision number of the chassis motherboard
	9.4. fwChassisMBSerialNumber	
52	fwChassisMBSerialNumber	Serial number of the chassis motherboard
	9.5. fwCardTable/fwCardEntry	
53	fwCardIndex	Index of the card
54	fwCardOperStatus	Operating status of the card
	10. fwStorageGroup	
	fwSIMMTotal	
55	fwSIMMTotal	Total capacity of SIMM memory
	11. fwProcessGroup	
	11.1. fwProcessorUtilization	
56	fwProcessorUtilization	Utilization of CPU
	11.2. fwProcessTable/fwProcessEntry	
57	fwProcessID	ID of the process
58	fwProcessParentID	Parent ID of the process
59	fwProcessOwner	Owner of the process (user)
60	fwProcessMemory	Memory utilization of the process (Mb)
61	fwProcessPercentCPU	CPU utilization of the process
62	fwProcessName	Name of the process
	12. fwAssetGroup	
	12.1. fwAssetChassisSerialNumber	
63	fwAssetChassisSerialNumber	Serial number of the chassis
	12.2. fwCPUModel	
64	fwCPUModel	Model of the chassis CPU

Table 314 Private MIBs

	12.3. fwCPUMfr	
65	fwCPUMfr	Manufacturer of the chassis CPU
	12.4. fwCPUFreq	
66	fwCPUFreq	Frequency of CPU
	12.5. fwKernMaxMem	
67	fwKernMaxMem	Maximum capacity of the kernel memory
	12.6. fwMotherBoardSerNum	
68	fwMotherBoardSerNum	Serial number of the motherboard
	12.7. fwMotherBoardRev	
69	fwMotherBoardRev	Revision number of the motherboard
	12.8. fwMotherBoardModel	
70	fwMotherBoardModel	Model number of the motherboard
	12.9. fwOSRelease	
71	fwOSRelease	Release number of the current system
	12.10. fwOSVersion	
72	fwOSVersion	Version number of the current system
	12.11. fwProductModel	
73	fwProductModel	Product model number of the current system
	12.12. fwAssetTable/fwAssetEntry	
74	fwPkgIndex	Index of the software installed and operated
75	fwPkgName	Name of the software
76	fwPkgMajorVersion	Major version number of the software
77	fwPkgMinorVersion	Minor version number of the software
	12.13. fwDiskDriveTableModel/fwDiskDriveEntry	
78	fwDiskDriveIndex	Index of the disk
79	fwDiskSysDriveIndex	Index the operating system uses to identify the disk
80	fwDiskDriveModel	Disk type: hard disk, floppy disk, or compact flash card
81	fwDiskDriveCapacity	Capacity of the disk
82	fwDiskDriveLocation	Location of the disk
	12.14. fwBiosVendor	
83	fwBiosVendor	Vendor of BIOS
	12.15. fwBiosVersion	
84	fwBiosVersion	Version of BIOS
	12.16. fwBiosDate	
85	fwBiosDate	Released date of BIOS

Table 314 Private MIBs

13. fwCounterSessionGroup

fwCounterSessionTable/fwCounterSessionEntry

86	fwCounterIndex	Index of the interface
87	fwCounterInterfaceName	Name of the interface
88	fwCounterSessions	Total number of sessions
89	fwCounterMacTblFull	Total number of times that the MAC table has been filled up
90	fwCounterDroppedPkts	Number of packets dropped by the system
91	fwCounterLoggedPkts	Number of packets logged by the system
92	fwCounterRejectedPkts	Number of packets rejected by policies
93	fwCounterRejectedBytes	Total bytes of packets
94	fwCounterDroppedByVlanPkts	Number of packets dropped due to VLAN issues. For example, VLAN headers are missing.
95	fwCounterDroppedNoInBufPkts	Number of packets dropped due to receive buffer underflow
96	fwCounterDroppedNoOutBufPkts	Number of packets dropped due to send buffer underflow
97	fwCounterOutPkts	Number of packets sent by the system
98	fwCounterOutBytes	Total bytes of packets sent by the system
99	fwCounterOutCollErr	Number of conflicting packets sent by the system
100	fwCounterInPkts	Number of packets received by the system
101	fwCounterInBytes	Total bytes of packets received by the system
102	fwCounterInCollErrPkts	Number of conflicting packets received by the system
103	fwCounterInCrcErrPkts	Number of CRC errors in packets received
104	fwCounterInArpReq	Number of ARP requests received by the system
105	fwCounterOutArpReq	Number of ARP requests sent by the system
106	fwCounterInSelfPkts	Number of packets sent to local IP addresses (management IP addresses) of the system
107	fwCounterInVpnPkts	Number of VPN packets received by the system
108	fwCounterInIpPkts	Number of IP packets received by the system
109	fwCounterInIpBytes	Bytes of IP packets received by the system
110	fwCounterInNipPkts	Number of non-IP packets received by the system
111	fwCounterInNipBytes	Bytes of non-IP packets received by the system
112	fwCounterInTcpPkts	Number of TCP packets received by the system
113	fwCounterInTcpBytes	Bytes of TCP packets received by the system
114	fwCounterInUdpPkts	Number of UDP packets received by the system
115	fwCounterInUdpBytes	Bytes of UDP packets received by the system
116	fwCounterInIcmpPkts	Number of ICMP packets received by the system

Table 314 Private MIBs

117	fwCounterInMiscProtoPkts	Number of non-TCP, -UDP, and -ICMP packets received by the system
118	fwCounterInLess64Pkts	Number of packets that are no greater than 64 bytes in length
119	fwCounterInLess256Pkts	Number of packets that are greater than 64 bytes but no greater than 256 bytes in length
120	fwCounterInLess1024Pkts	Number of packets that are greater than 256 bytes but no greater than 1,024 bytes in length
121	fwCounterInBigger1024Pkts	Number of packets that are greater than 1,024 bytes in length
122	fwCounterTcpSynPkts	Number of TCP SYN packets received by the system
123	fwCounterTcpSynAckPkts	Number of TCP SYN/ACK packets received by the system
124	fwCounterTcpAckPkts	Number of TCP ACK packets received by the system
125	fwCounterTcpFinPkts	Number of TCP FIN packets received by the system
126	fwCounterTcpRstPkts	Number of TCP RST packets received by the system
127	fwCounterNipDenyPkts	Number of packets denied by non-IP packet filter policies
128	fwCounterIpMacDenyPkts	Number of packets denied by IP-MAC policies
129	fwCounterRouteDenyPkts	Number of packets denied by routing policies
130	fwCounterSnatDenyPkts	Number of packets denied by SNAT policies
131	fwCounterDnatDenyPkts	Number of packets denied by DNAT policies
132	fwCounterDroppedDtsIpLimit	Number of packets dropped by destination-based session limit policies
133	fwCounterDroppedSrsIpLimit	Number of packets dropped by source-based session limit policies
134	fwCounterDroppedSessionLimit	Number of packets dropped since the maximum session limit has been reached
135	fwCounterDroppedNoNatResPkts	Number of packets dropped since NAT resources have been used up
136	fwCounterDroppedNoGatePkts	Number of packets dropped because there is no available incoming interface
137	fwCounterDroppedIpfilterPkts	Number of packets denied by IP packet filter policies
138	fwCounterPacketsIcmpFlood	Number of ICMP flood attack packets
139	fwCounterPacketsSynFlood	Number of SYN flood attack packets
140	fwCounterPacketsUdpFlood	Number of UDP flood attack packets
141	fwCounterPacketsTcpRstScan	Number of RST scan packets
142	fwCounterPacketsWinnuke	Number of WinNuke attack packets
143	fwCounterPacketsSmurf	Number of Smurf attack packets
144	fwCounterPacketsLand	Number of LAND attack packets
145	fwCounterPacketsPingOfDeath	Number of Ping of Death attack packets
146	fwCounterPacketsTearDrop	Number of Teardrop attack packets
147	fwCounterPacketsFinScan	Number of FIN scan packets
148	fwCounterPacketsXmasScan	Number of XMAS scan packets
149	fwCounterPacketsNullScan	Number of NULL scan packets

Table 314 Private MIBs

150	fwCounterPacketsSynScan	Number of SYN port scan packets
151	fwCounterPacketsIpSweep	Number of IP address sweep packets
152	fwCounterPacketsSynFinSet	Number of TCP packets with SYN and FIN flags set
153	fwCounterPacketsFinWithoutAck	Number of FIN packets without ACK flags
154	fwCounterNonSynFlags	Number of TCP packets without SYN flags set
155	fwCounterIpoptTimeStamp	Number of IP packets with IP timestamp options
156	fwCounterIpoptRecordRoute	Number of IP packets with IP record route options
157	fwCounterIpoptTraceRoute	Number of IP packets with IP traceroute options
158	fwCounterIpoptLooseSourceRoute	Number of IP packets with IP loose source route options
159	fwCounterIpoptStrictSourceRoute	Number of IP packets with IP strict source route options
160	fwCounterIpoptOther	Number of packets with other IP options
161	fwCounterIpSpoofing	Number of IP spoofing attack packets
162	fwCounterIpFrag	Number of IP fragment packets blocked
163	fwCounterIcmpFrag	Number of ICMP fragment packets blocked
164	fwCounterIcmpLargePacket	Number of ICMP packets blocked
165	fwCounterSourceRouteFilter	Number of packets filtered by source route options
166	fwCounterTcpWithoutFlag	Number of TCP packets without control flags
167	fwCounterUnknowProto	Number of unknown protocol packets blocked
168	fwCounterSynFrag	Number of SYN fragment attack packets blocked
169	fwCounterActiveRaTunnels	Number of currently established dial-up VPN tunnels
170	fwCounterActiveTunnels	Number of currently active tunnels
171	fwCounterIkeConcurent	Number of concurrent IKE negotiations
172	fwCounterIkeFailures	Number of failed IKE negotiations in Phase 1
173	fwCounterIkeSuccesses	Number of successful IKE negotiations in Phase 1
174	fwCounterDecPkts	Total number of packets decrypted
175	fwCounterDecBytes	Total number of bytes decrypted
176	fwCounterDecErr	Total number of decryption errors
177	fwCounterEncPkts	Total number of packets encrypted
178	fwCounterEncBytes	Total number of bytes encrypted
179	fwCounterEncErr	Total number of encryption errors
180	fwCounterVpnAccelEncBytes	Total number of bytes encrypted by the acceleration chip
181	fwCounterVpnAccelEncErr	Total number of acceleration chip encryption errors
182	fwCounterVpnAccelDecBytes	Total number of bytes decrypted by the acceleration chip
183	fwCounterVpnAccelDecErr	Total number of acceleration chip decryption errors
184	fwCounterCreatSessionHttp	Total number of sessions established by HTTP

Table 314 Private MIBs

185	fwCounterCurSessionHttp	Number of current sessions established by HTTP
186	fwCounterCreatSessionSmtp	Total number of sessions established by SMTP
187	fwCounterCurSessionSmtp	Number of current sessions established by SMTP
188	fwCounterCreatSessionPop3	Total number of sessions established by POP3
189	fwCounterCurSessionPop3	Number of current sessions established by POP3
190	fwCounterCreatSessionImap	Total number of sessions established by IMAP
191	fwCounterCurSessionImap	Number of current sessions established by IMAP
192	fwCounterCreatSessionFtp	Total number of sessions established by FTP
193	fwCounterCurSessionFtp	Number of current sessions established by FTP
194	fwCounterCreatSessionTelnet	Total number of sessions established by Telnet
195	fwCounterCurSessionTelnet	Number of current sessions established by Telnet
	14. fwAnti-VirusCounterGroup	
196	fwCounterHttpBlckByFiletype	Number of HTTP files blocked because files of their type are not allowed to be forwarded
197	fwCounterHttpBlckByVirus	Number of HTTP files on which viruses are detected
198	fwCounterHttpScanned	Number of HTTP files on which virus scan is performed
199	fwCounterFtpBlckByFiletype	Number of FTP files blocked because files of their type are not allowed to be forwarded
200	fwCounterFtpBlckByVirus	Number of FTP files on which viruses are detected
201	fwCounterFtpScanned	Number of FTP files on which virus scan is performed
202	fwCounterSmtpBlckByFiletype	Number of SMTP files blocked because files of their type are not allowed to be forwarded
203	fwCounterSmtpBlckByVirus	Number of SMTP files on which viruses are detected
204	fwCounterSmtpScanned	Number of SMTP files on which virus scan is performed
205	fwCounterPop3BlckByFiletype	Number of POP3 files blocked because files of their type are not allowed to be forwarded
206	fwCounterPop3BlckByVirus	Number of POP3 files on which viruses are detected
207	fwCounterPop3Scanned	Number of POP3 files on which virus scan is performed
208	fwCounterImapBlckByFiletype	Number of IMAP files blocked because files of their type are not allowed to be forwarded
209	fwCounterImapBlckByVirus	Number of IMAP files on which viruses are detected
210	fwCounterImapScanned	Number of IMAP files on which virus scan is performed
211	fwCounterTotalBlckByFiletype	Number of protocol files blocked because files of their type are not allowed to be forwarded
212	fwCounterTotalBlckByVirus	Number of protocol files on which viruses are detected
213	fwCounterTotalScanned	Number of protocol files on which virus scan is performed
	15. fwAnti-SpamCounterGroup	

Table 314 Private MIBs

214	fwCounterBlckByIpBlacklist	Number of e-mail messages blocked by the IP block list
215	fwCounterBlckBySenderBlacklist	Number of e-mail messages blocked by the sender block list
216	fwCounterBlckByWordBlacklist	Number of e-mail messages blocked by the spam word list
217	fwCounterBlckByContent	Number of e-mail messages blocked due to invalid contents
218	fwCounterBlckTotal	Total number of e-mail messages blocked
	16. fwWeb-ProtectionCounterGroup	
219	fwCounterNewSessionRateHttp	Number of new HTTP sessions established per second
220	fwCounterWordFilteringHttp	Number of sessions blocked by word filtering
221	fwCounterFormatSizeHttp	Number of sessions on which HTTP format and length anomalies are detected
222	fwCounterMethodsHttp	Number of sessions blocked by request method restriction
223	fwCounterASIIOnlyReqHttp	Number of HTTP request connections containing non-ASCII characters
224	fwCounterHeaderSpoofingHttp	Number of times that header substitution has been performed
225	fwCounterDirectoryListingHttp	Number of times that directory listing detection has been performed
226	fwCounterErrConcealmentHttp	Number of HTTP connections blocked by error concealment
227	fwCounterSQLInjection	Number of HTTP connections blocked by SQL injection detection
228	fwCounterCmdInjection	Number of HTTP connections blocked by command injection detection
229	fwCounterLDAPInjection	Number of HTTP connections blocked by LDAP injection detection
230	fwCounterCrossSiteScripting	Number of cross-site scripting attacks detected
231	fwCounterErrPageHttp	Number of times that error pages have been blocked by URLs
232	fwCounterAttackDefenseHttp	Number of HTTP attacks detected
	17. fwMail-ProtectionCounterGroup	
233	fwCounterNewSessionRateSmtp	Number of new SMTP sessions established per second
234	fwCounterNewSessionRatePop3	Number of new POP3 sessions established per second
235	fwCounterNewSessionRateImap	Number of new IMAP sessions established per second
236	fwCounterFormatSizeSmtp	Number of sessions on which SMTP format and length anomalies are detected
237	fwCounterBlckCmdsSmtp	Number of invalid commands blocked by SMTP
238	fwCounterFormatSizePop3	Number of sessions on which POP3 format and length anomalies are detected
239	fwCounterBlckCmdsPop3	Number of invalid commands blocked by POP3
240	fwCounterFormatSizeImap	Number of sessions on which IMAP format and length anomalies are detected
241	fwCounterBlckCmdsImap	Number of invalid commands blocked by IMAP
242	fwCounterAttackDefenseSmtp	Number of SMTP attacks detected
243	fwCounterAttackDefensePop3	Number of POP3 attacks detected
244	fwCounterAttackDefenseImap	Number of IMAP attacks detected
	18. fwDeep-InspectionCounterGroup	
245	fwCounterNewSessionRateFtp	Number of new FTP sessions established per second

Table 314 Private MIBs

246	fwCounterNewSessionRateTelnet	Number of new Telnet sessions established per second
247	fwCounterBlckbyBlacklistDns	Number of sessions blocked by the domain blacklist
248	fwCounterBlckCmdsTelnet	Number of sessions blocked by Telnet user-defined command detection
249	fwCounterAttackDefenseDI	Total number of DI attacks detected
250	fwCounterBackdoorDI	Number of backdoor attacks detected by DI
	19. fwUrl-FilteringCounterGroup	
251	fwCounterBlckByBlacklist	Number of URLs blocked by URL blacklists
252	fwCounterBlckByAnonymizers	Number of HTTP connections blocked by URLs of the anonymizers category
253	fwCounterBlckByBotnets	Number of HTTP connections blocked by URLs of the botnets category
254	fwCounterBlckByHacking	Number of HTTP connections blocked by URLs of the hacking category
255	fwCounterBlckByMalware	Number of URLs blocked by URLs of the malware category
256	fwCounterBlckByNetworkErrors	Number of URLs blocked by URLs of the network errors category
257	fwCounterBlckByParkedDomains	Number of URLs blocked by URLs of the parked domains category
258	fwCounterBlckByPhishingFraud	Number of URLs blocked by URLs of the phishing & fraud category
259	fwCounterBlckBySpamSites	Number of URLs blocked by URLs of the spam sites category
260	fwCounterBlckByTranslators	Number of URLs blocked by URLs of the translators category
261	fwCounterBlckByAdvertisementsPop-Ups	Number of URLs blocked by URLs of the advertisements & pop-ups category
262	fwCounterBlckByAlcoholTobacco	Number of URLs blocked by URLs of the alcohol & tobacco category
263	fwCounterBlckByArts	Number of URLs blocked by URLs of the arts category
264	fwCounterBlckByBusiness	Number of URLs blocked by URLs of the business category
265	fwCounterBlckByChat	Number of URLs blocked by URLs of the chat category
266	fwCounterBlckByChildAbuseImages	Number of URLs blocked by URLs of the child abuse images category
267	fwCounterBlckByCompromised	Number of URLs blocked by URLs of the compromised category
268	fwCounterBlckByComputersTechnology	Number of URLs blocked by URLs of the computers & technology category
269	fwCounterBlckByCriminalActivity	Number of URLs blocked by URLs of the criminal activity category
270	fwCounterBlckByCults	Number of URLs blocked by URLs of the cults category
271	fwCounterBlckByDatingPersonals	Number of URLs blocked by URLs of the dating & personals category
272	fwCounterBlckByDownloadSites	Number of URLs blocked by URLs of the download sites category
273	fwCounterBlckByEducation	Number of URLs blocked by URLs of the education category
274	fwCounterBlckByEntertainment	Number of URLs blocked by URLs of the entertainment category
275	fwCounterBlckByFashionBeauty	Number of URLs blocked by URLs of the fashion & beauty category
276	fwCounterBlckByFinance	Number of URLs blocked by URLs of the finance category
277	fwCounterBlckByForumsNewsgroups	Number of URLs blocked by URLs of the forums & newsgroups category
278	fwCounterBlckByGambling	Number of URLs blocked by URLs of the gambling category

Table 314 Private MIBs

279	fwCounterBlckByGames	Number of URLs blocked by URLs of the games category
280	fwCounterBlckByGeneral	Number of URLs blocked by URLs of the general category
281	fwCounterBlckByGovernment	Number of URLs blocked by URLs of the government category
282	fwCounterBlckByGreetingCards	Number of URLs blocked by URLs of the greeting cards category
283	fwCounterBlckByHateIntolerance	Number of URLs blocked by URLs of the hate & intolerance category
284	fwCounterBlckByHealthMedicine	Number of URLs blocked by URLs of the health & medicine category
285	fwCounterBlckByIllegalDrugs	Number of URLs blocked by URLs of the illegal drugs category
286	fwCounterBlckByIllegalSoftware	Number of URLs blocked by URLs of the illegal software category
287	fwCounterBlckByImageSharing	Number of URLs blocked by URLs of the image sharing category
288	fwCounterBlckByInformationSecurity	Number of URLs blocked by URLs of the information security category
289	fwCounterBlckByInstantMessaging	Number of URLs blocked by URLs of the instant messaging category
290	fwCounterBlckByJobSearch	Number of URLs blocked by URLs of the job search category
291	fwCounterBlckByLeisureRecreation	Number of URLs blocked by URLs of the leisure & recreation category
292	fwCounterBlckByNews	Number of URLs blocked by URLs of the news category
293	fwCounterBlckByNon-profitsNGOs	Number of URLs blocked by URLs of the non-profits & NGOs category
294	fwCounterBlckByNudity	Number of URLs blocked by URLs of the nudity category
295	fwCounterBlckByPeertoPeer	Number of URLs blocked by URLs of the peer-to-peer category
296	fwCounterBlckByPersonalSites	Number of URLs blocked by URLs of the personal sites category
297	fwCounterBlckByPolitics	Number of URLs blocked by URLs of the politics category
298	fwCounterBlckByPornographtOrSexually ExpliclI	Number of URLs blocked by URLs of the pornography/sexually explicit category
299	fwCounterBlckByPrivateIPAddresses	Number of URLs blocked by URLs of the private IP addresses category
300	fwCounterBlckByRealEstate	Number of URLs blocked by URLs of the real estate category
301	fwCounterBlckByReligion	Number of URLs blocked by URLs of the religion category
302	fwCounterBlckByRestaurantsDining	Number of URLs blocked by URLs of the restaurants & dining category
303	fwCounterBlckBySchoolCheating	Number of URLs blocked by URLs of the school cheating category
304	fwCounterBlckBySearchEnginesPortals	Number of URLs blocked by URLs of the search engines & portals category
305	fwCounterBlckBySexEducation	Number of URLs blocked by URLs of the sex education category
306	fwCounterBlckByShopping	Number of URLs blocked by URLs of the shopping category
307	fwCounterBlckBySocialNetworking	Number of URLs blocked by URLs of the social networking category
308	fwCounterBlckBySports	Number of URLs blocked by URLs of the sports category
309	fwCounterBlckByStreamingMedia Downloads	Number of URLs blocked by URLs of the streaming media & downloads category
310	fwCounterBlckByTasteless	Number of URLs blocked by URLs of the tasteless category
311	fwCounterBlckByTransportation	Number of URLs blocked by URLs of the transportation category

Table 314 Private MIBs

312	fwCounterBlckByTravel	Number of URLs blocked by URLs of the travel category
313	fwCounterBlckByViolence	Number of URLs blocked by URLs of the violence category
314	fwCounterBlckByWeapons	Number of URLs blocked by URLs of the weapons category
315	fwCounterBlckByWebBasedEmail	Number of URLs blocked by URLs of the web-based e-mail category
316	fwCounterBlckTotal	Total number of connections blocked by URLs

1.