FortiGate™
Version 3.0 MR5

Visit http://support.fortinet.com to register your FortiGate product. By registering you can receive product updates, technical support, and FortiGuard services.

www.fortinet.com
Contents

Introduction ...................................................................................... 19

What’s new in this release.............................................................................. 19

Introducing the FortiGate units................................................................. 20
  FortiGate-5000 series chassis ................................................................. 20
  About the FortiGate-5000 series modules ............................................. 21
  FortiGate-AMC modules ....................................................................... 22
  FortiGate-3810A..................................................................................... 22
  FortiGate-3600A..................................................................................... 23
  FortiGate-3600...................................................................................... 23
  FortiGate-3000...................................................................................... 23
  FortiGate-1000A..................................................................................... 24
  FortiGate-1000AFA2 ............................................................................. 24
  FortiGate-1000...................................................................................... 24
  FortiGate-800...................................................................................... 24
  FortiGate-800F...................................................................................... 25
  FortiGate-500A..................................................................................... 25
  FortiGate-500...................................................................................... 25
  FortiGate-400A..................................................................................... 25
  FortiGate-400...................................................................................... 25
  FortiGate-300A..................................................................................... 26
  FortiGate-300...................................................................................... 26
  FortiGate-224B..................................................................................... 26
  FortiGate-200A..................................................................................... 27
  FortiGate-200...................................................................................... 27
  FortiGate-100A..................................................................................... 27
  FortiGate-100...................................................................................... 27
  FortiGate-60B...................................................................................... 27
  FortiWiFi-60B ...................................................................................... 28
  FortiGate-60/60M/ADSL ................................................................. 28
  FortiWiFi-60/60A/60AM ................................................................. 28
  FortiGate-50B..................................................................................... 28
  FortiGate-50A..................................................................................... 29

Fortinet family of products ..................................................................... 29
  FortiGuard Subscription Services ......................................................... 29
  FortiAnalyzer ........................................................................................ 29
  FortiClient............................................................................................ 29
  FortiManager ........................................................................................ 30
  FortiBridge .......................................................................................... 30
  FortiMail ............................................................................................. 30

About this document .............................................................................. 30
  Document conventions ........................................................................ 32
FortiGate documentation ............................................................................... 33
Fortinet Tools and Documentation CD ....................................................... 34
Fortinet Knowledge Center ........................................................................ 34
Comments on Fortinet technical documentation ....................................... 34
Customer service and technical support ................................................... 35
Register your Fortinet product .................................................................... 35

Web-based manager ...................................................................................... 37
Button bar features ...................................................................................... 38
Contact Customer Support ......................................................................... 38
Backup your FortiGate configuration ......................................................... 38
Using the Online Help ............................................................................... 39
Logout ........................................................................................................ 41

Web-based manager pages ......................................................................... 42
Web-based manager menu .......................................................................... 42
Lists ........................................................................................................... 43
Adding filters to web-based manager lists .................................................. 43
Icons .......................................................................................................... 46

System Status .............................................................................................. 49
Status page .................................................................................................. 49
Viewing system status ............................................................................. 49
Changing system information .................................................................. 58
Configuring system time .......................................................................... 58
Changing the FortiGate unit host name .................................................... 59
Changing the FortiGate firmware .............................................................. 59
Upgrading to a new firmware version ....................................................... 59
Reverting to a previous firmware version ................................................. 60
Viewing operational history ...................................................................... 61
Manually updating FortiGuard definitions ................................................ 62
Viewing Statistics ...................................................................................... 63
Viewing the session list ........................................................................... 63
Viewing the Content Archive information ............................................... 64
Viewing the Attack Log ........................................................................... 65

Topology viewer ........................................................................................ 67
The Topology Viewer window ................................................................ 67
Adding a subnet object ............................................................................ 69
Customizing the topology diagram ......................................................... 70

Using virtual domains ................................................................................. 71
Virtual domains ......................................................................................... 71
VDOM configuration settings ................................................................. 72
Global configuration settings ................................................................. 73
### System Network

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>79</td>
</tr>
<tr>
<td>Switch Mode</td>
<td>82</td>
</tr>
<tr>
<td>Interface settings</td>
<td>83</td>
</tr>
<tr>
<td>Configuring an ADSL interface</td>
<td>85</td>
</tr>
<tr>
<td>Creating an 802.3ad aggregate interface</td>
<td>86</td>
</tr>
<tr>
<td>Creating a redundant interface</td>
<td>87</td>
</tr>
<tr>
<td>Configuring DHCP on an interface</td>
<td>88</td>
</tr>
<tr>
<td>Configuring an interface for PPPoE or PPPoA</td>
<td>90</td>
</tr>
<tr>
<td>Configuring Dynamic DNS service for an interface</td>
<td>91</td>
</tr>
<tr>
<td>Configuring a virtual IPSec interface</td>
<td>92</td>
</tr>
<tr>
<td>Interfaces only configurable with CLI commands</td>
<td>93</td>
</tr>
<tr>
<td>Additional configuration for interfaces</td>
<td>94</td>
</tr>
<tr>
<td>Zone</td>
<td>98</td>
</tr>
<tr>
<td>Zone settings</td>
<td>98</td>
</tr>
<tr>
<td>Network Options</td>
<td>99</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>100</td>
</tr>
<tr>
<td>Dead gateway detection</td>
<td>100</td>
</tr>
<tr>
<td>Routing table (Transparent Mode)</td>
<td>101</td>
</tr>
<tr>
<td>Transparent mode route settings</td>
<td>101</td>
</tr>
<tr>
<td>Configuring the modem interface</td>
<td>101</td>
</tr>
<tr>
<td>Configuring modem settings</td>
<td>102</td>
</tr>
<tr>
<td>Redundant mode configuration</td>
<td>104</td>
</tr>
<tr>
<td>Standalone mode configuration</td>
<td>105</td>
</tr>
<tr>
<td>Adding firewall policies for modem connections</td>
<td>106</td>
</tr>
<tr>
<td>Connecting and disconnecting the modem</td>
<td>106</td>
</tr>
<tr>
<td>Checking modem status</td>
<td>106</td>
</tr>
<tr>
<td>VLAN overview</td>
<td>107</td>
</tr>
<tr>
<td>FortiGate units and VLANs</td>
<td>107</td>
</tr>
<tr>
<td>VLANS in NAT/Route mode</td>
<td>108</td>
</tr>
<tr>
<td>Rules for VLAN IDs</td>
<td>108</td>
</tr>
<tr>
<td>Rules for VLAN IP addresses</td>
<td>108</td>
</tr>
<tr>
<td>Adding VLAN subinterfaces</td>
<td>109</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANs in Transparent mode</td>
<td>110</td>
</tr>
<tr>
<td>Rules for VLAN IDs</td>
<td>112</td>
</tr>
<tr>
<td>Transparent mode virtual domains and VLANs</td>
<td>112</td>
</tr>
<tr>
<td>Troubleshooting ARP Issues</td>
<td>115</td>
</tr>
<tr>
<td>FortiGate IPv6 support</td>
<td>115</td>
</tr>
<tr>
<td><strong>System Wireless</strong></td>
<td>117</td>
</tr>
<tr>
<td>About FortiWiFi-50B power over ethernet (POE)</td>
<td>117</td>
</tr>
<tr>
<td>FortiWiFi wireless interfaces</td>
<td>117</td>
</tr>
<tr>
<td>Channel assignments</td>
<td>118</td>
</tr>
<tr>
<td>IEEE 802.11a channel numbers</td>
<td>118</td>
</tr>
<tr>
<td>IEEE 802.11b channel numbers</td>
<td>119</td>
</tr>
<tr>
<td>IEEE 802.11g channel numbers</td>
<td>119</td>
</tr>
<tr>
<td>FortiWiFi-50B, 60A, 60AM, and 60B system wireless settings</td>
<td>120</td>
</tr>
<tr>
<td>Adding a wireless interface to a FortiWiFi-50B, 60A, 60AM, and 60B unit</td>
<td>122</td>
</tr>
<tr>
<td>FortiWiFi-60 System wireless settings</td>
<td>124</td>
</tr>
<tr>
<td>Wireless MAC Filter</td>
<td>125</td>
</tr>
<tr>
<td>FortiWiFi-50B, 60A, 60AM, and 60B Wireless MAC Filter list</td>
<td>125</td>
</tr>
<tr>
<td>FortiWiFi-60 Wireless MAC Filter</td>
<td>126</td>
</tr>
<tr>
<td>Wireless Monitor</td>
<td>127</td>
</tr>
<tr>
<td><strong>System DHCP</strong></td>
<td>129</td>
</tr>
<tr>
<td>FortiGate DHCP servers and relays</td>
<td>129</td>
</tr>
<tr>
<td>Configuring DHCP services</td>
<td>130</td>
</tr>
<tr>
<td>Configuring an interface as a DHCP relay agent</td>
<td>131</td>
</tr>
<tr>
<td>Configuring a DHCP server</td>
<td>131</td>
</tr>
<tr>
<td>Viewing address leases</td>
<td>132</td>
</tr>
<tr>
<td>Reserving IP addresses for specific clients</td>
<td>133</td>
</tr>
<tr>
<td><strong>System Config</strong></td>
<td>135</td>
</tr>
<tr>
<td>HA</td>
<td>135</td>
</tr>
<tr>
<td>HA options</td>
<td>135</td>
</tr>
<tr>
<td>Cluster members list</td>
<td>139</td>
</tr>
<tr>
<td>Viewing HA statistics</td>
<td>141</td>
</tr>
<tr>
<td>Changing subordinate unit host name and device priority</td>
<td>142</td>
</tr>
<tr>
<td>Disconnecting a cluster unit from a cluster</td>
<td>142</td>
</tr>
<tr>
<td><strong>SNMP</strong></td>
<td>143</td>
</tr>
<tr>
<td>Configuring SNMP</td>
<td>143</td>
</tr>
<tr>
<td>Configuring an SNMP community</td>
<td>144</td>
</tr>
<tr>
<td>Fortinet MIBs</td>
<td>146</td>
</tr>
<tr>
<td>FortiGate traps</td>
<td>147</td>
</tr>
<tr>
<td>Fortinet MIB fields</td>
<td>149</td>
</tr>
</tbody>
</table>
Contents

Replacement messages ................................................................. 153
Replacement messages list ......................................................... 153
Changing replacement messages ................................................. 154
Changing the authentication login page ..................................... 156
Changing the FortiGuard web filtering block override page ........ 157
Changing the SSL-VPN login message ....................................... 157
Changing the authentication disclaimer page ......................... 157
Changing the Host Check pages (FortiGate-224B unit only) ....... 157

Operation mode and VDOM management access .................... 158
Changing operation mode ......................................................... 159
Management access ................................................................ 160

System Administrators ............................................................. 161
Administrators ......................................................................... 161
Configuring RADIUS authentication for administrators ............ 163
Configuring PKI certificate authentication for administrators .... 164
Viewing the administrators list ............................................... 165
Configuring an administrator account ..................................... 166

Access profiles ........................................................................... 169
Viewing the access profiles list ............................................... 171
Configuring an access profile .................................................. 172

Central Management ............................................................... 173

Settings ...................................................................................... 175

Monitoring administrators ......................................................... 177

System Maintenance ................................................................. 179
Maintenance System Configuration ........................................... 179
Backup and Restore ................................................................. 181
Firmware ................................................................................... 183
FortiClient .................................................................................. 183
Firmware Upgrade ................................................................. 184
Advanced ................................................................................. 184

Revision Control ....................................................................... 185

FortiGuard Center ................................................................. 186
FortiGuard Distribution Network ............................................. 186
FortiGuard Services ............................................................... 187
Configuring the FortiGate unit for FDN and FortiGuard services 188
Troubleshooting FDN connectivity ......................................... 193
Updating antivirus and attack definitions .............................. 193
Enabling push updates .......................................................... 195

License ....................................................................................... 199
| Contents |
|---------------------------------|----------------|
| System Chassis (FortiGate-5000 series) | 201 |
| SMC (shelf manager card) | 201 |
| Blades (FortiGate-5000 chassis slots) | 202 |
| Chassis monitoring event log messages | 204 |
| Switch (FortiGate-224B only) | 207 |
| Overview | 207 |
| Enabling switch view | 208 |
| Viewing WAN ports and WAN VLAN interfaces | 208 |
| Viewing switch-LAN ports | 209 |
| Configuring a switch-LAN interface | 210 |
| Viewing switch VLANs | 211 |
| Configuring a switch VLAN | 212 |
| Configuring port monitoring | 213 |
| Using Spanning-Tree Protocol | 214 |
| Configuring Spanning-Tree settings | 214 |
| Configuring Spanning-Tree VLAN settings | 216 |
| Viewing Spanning-Tree VLAN information | 217 |
| Configuring Spanning-Tree VLAN port settings | 218 |
| Configuring IGMP snooping | 218 |
| Configuring QoS | 218 |
| Configuring QoS settings | 218 |
| Configuring CoS-Map settings | 219 |
| Configuring DSCP-Map settings | 219 |
| Viewing QoS rate limits | 219 |
| Adding a QoS rate limit | 220 |
| Configuring port quarantine | 220 |
| Viewing client profiles | 221 |
| Configuring a client profile | 221 |
| Viewing access policies | 222 |
| Configuring an access policy | 223 |
| Configuring dynamic policies | 224 |
| Viewing quarantine policies | 224 |
| Configuring a dynamic policy | 224 |
| Configuring 802.1X authentication | 226 |
| Viewing switch status | 227 |
| Monitoring access results | 227 |
| Viewing quarantine port information | 227 |
| Viewing the MAC table | 228 |
| Creating a MAC table entry | 228 |
| Viewing statistics | 229 |
Router Static ................................................................. 231
Routing concepts .......................................................... 231
How the routing table is built ........................................... 232
How routing decisions are made ...................................... 232
Multipath routing and determining the best route ............. 232
How route sequence affects route priority ....................... 233
Equal Cost Multipath (ECMP) Routes .............................. 234
Blackhole Routing ......................................................... 234
Static Route ..................................................................... 235
Working with static routes .............................................. 235
Default route and default gateway ................................. 236
Adding a static route to the routing table ......................... 238
Policy Route ................................................................... 239
Adding a route policy ..................................................... 240
Moving a route policy ..................................................... 241
Router Dynamic ............................................................ 243
RIP .............................................................................. 244
How RIP works ........................................................... 244
Viewing and editing basic RIP settings ........................... 244
Selecting advanced RIP options ..................................... 246
Overriding the RIP operating parameters on an interface ... 247
OSPF .......................................................................... 248
OSPF autonomous systems ........................................... 248
Defining an OSPF AS .................................................... 249
Viewing and editing basic OSPF settings ......................... 250
Selecting advanced OSPF options ................................. 252
Defining OSPF areas .................................................... 253
Specifying OSPF networks ........................................... 254
Selecting operating parameters for an OSPF interface ...... 255
BGP ........................................................................... 256
How BGP works .......................................................... 256
Viewing and editing BGP settings ................................. 257
Multicast ....................................................................... 258
Viewing and editing multicast settings ......................... 258
Overriding the multicast settings on an interface .......... 260
Multicast destination NAT ........................................... 260
Bi-directional Forwarding Detection (BFD) ...................... 261
How it works .............................................................. 261
Configuring BFD ......................................................... 261
Router Monitor ............................................................. 263
Displaying routing information ...................................... 263
Searching the FortiGate routing table ............................. 265
Contents

Firewall Policy ................................................................. 267
  About firewall policies ...................................................... 267
  Multicast policies .......................................................... 268
  How policy matching works ............................................. 268
Viewing the firewall policy list ........................................... 268
  Adding a firewall policy .................................................. 270
  Moving a policy to a different position in the policy list ............. 270
Configuring firewall policies ............................................. 271
  Firewall policy options ................................................... 272
  Configuring intra-VLAN firewall policies (FortiGate-224B only) ........ 275
  Adding authentication to firewall policies ............................ 276
  Adding traffic shaping to firewall policies ........................... 278
  IPSec firewall policy options .......................................... 280
  SSL-VPN firewall policy options ...................................... 281
  Options to check FortiClient on hosts ................................. 282
Firewall policy examples .................................................. 282
  Scenario one: SOHO sized business .................................. 282
  Scenario two: enterprise sized business ............................. 285
Firewall Address .............................................................. 289
  About firewall addresses .................................................. 289
Viewing the firewall address list ........................................ 290
Configuring addresses .......................................................... 291
Viewing the address group list ........................................... 291
Configuring address groups .................................................. 292
Firewall Service ................................................................. 293
  Viewing the predefined service list ....................................... 293
  Viewing the custom service list ......................................... 297
  Configuring custom services ............................................ 297
  Viewing the service group list ............................................ 299
  Configuring service groups .............................................. 300
Firewall Schedule ............................................................. 301
  Viewing the one-time schedule list ..................................... 301
  Configuring one-time schedules ....................................... 302
  Viewing the recurring schedule list .................................... 302
  Configuring recurring schedules ....................................... 303
Firewall Virtual IP ................................................................. 305
  Virtual IPs ................................................................................ 305
    How virtual IPs map connections through the FortiGate unit .... 305
  Viewing the virtual IP list ..................................................... 308
  Configuring virtual IPs .......................................................... 309
    Adding a static NAT virtual IP for a single IP address ... 310
    Adding a static NAT virtual IP for an IP address range ... 312
    Adding static NAT port forwarding for a single IP address
      and a single port .............................................................. 314
    Adding static NAT port forwarding for an IP address range
      and a port range ............................................................ 315
    Adding a server load balance virtual IP ......................... 317
    Adding a server load balance port forwarding virtual IP ... 319
    Adding dynamic virtual IPs .............................................. 321
    Adding a virtual IP with port translation only ............... 322

Virtual IP Groups ................................................................. 322
  Viewing the VIP group list ............................................... 322
  Configuring VIP groups .................................................... 323

IP pools ..................................................................................... 324
  IP pools and dynamic NAT ................................................ 324
  IP Pools for firewall policies that use fixed ports .............. 325
  Source IP address and IP pool address matching .......... 325
  Viewing the IP pool list ...................................................... 326
  Configuring IP Pools .......................................................... 327

Firewall Protection Profile .................................................. 329
  What is a protection profile? .............................................. 329
  Default protection profiles .............................................. 330
  Viewing the protection profile list ................................... 330
  Configuring a protection profile ...................................... 331
    Antivirus options ............................................................ 332
    Web filtering options .................................................... 333
    FortiGuard Web Filtering options ................................... 334
    Spam filtering options .................................................. 336
    IPS options ................................................................. 338
    Content archive options .............................................. 338
    IM and P2P options ..................................................... 339
    VoIP options ............................................................... 340
    Logging options .......................................................... 341
  Adding a protection profile to a policy ......................... 342
  Protection profile CLI configuration .............................. 342
Contents

VPN IPSEC...................................................................................... 343
  Overview of IPSec interface mode............................................................. 343
  Auto Key........................................................................................................... 345
    Creating a new phase 1 configuration...................................................... 345
    Defining phase 1 advanced settings......................................................... 348
    Creating a new phase 2 configuration...................................................... 350
    Defining phase 2 advanced settings......................................................... 351
    Internet browsing configuration............................................................... 353
  Manual Key...................................................................................................... 354
    Creating a new manual key configuration................................................ 355
  Concentrator.................................................................................................... 357
    Defining concentrator options................................................................. 357
  Monitor.............................................................................................................. 358

VPN PPTP ....................................................................................... 361
  PPTP Range................................................................................................. 361

VPN SSL.......................................................................................... 363
  Configuring SSL VPN.................................................................................... 363
  Monitoring SSL VPN sessions................................................................. 365
  SSL VPN bookmarks..................................................................................... 365
  Viewing the SSL VPN bookmark list............................................................ 366
  Configuring SSL VPN bookmarks.............................................................. 366
  Viewing the SSL VPN Bookmark Groups list................................................. 367
  Configuring SSL VPN bookmark groups...................................................... 368

VPN Certificates ............................................................................. 369
  Local Certificates ........................................................................................ 369
    Generating a certificate request............................................................... 370
    Downloading and submitting a certificate request.................................... 372
    Importing a signed server certificate....................................................... 373
    Importing an exported server certificate and private key.......................... 373
    Importing separate server certificate and private key files....................... 374
  Remote Certificates..................................................................................... 374
    Importing Remote (OCSP) certificates..................................................... 375
  CA Certificates............................................................................................ 375
    Importing CA certificates......................................................................... 376
  CRL.................................................................................................................. 377
    Importing a certificate revocation list....................................................... 377
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>379</td>
</tr>
<tr>
<td>Configuring user authentication</td>
<td>379</td>
</tr>
<tr>
<td>Local user accounts</td>
<td>380</td>
</tr>
<tr>
<td>Configuring a user account</td>
<td>380</td>
</tr>
<tr>
<td>RADIUS servers</td>
<td>381</td>
</tr>
<tr>
<td>Configuring a RADIUS server</td>
<td>381</td>
</tr>
<tr>
<td>LDAP servers</td>
<td>382</td>
</tr>
<tr>
<td>Configuring an LDAP server</td>
<td>383</td>
</tr>
<tr>
<td>PKI authentication</td>
<td>384</td>
</tr>
<tr>
<td>Configuring PKI users</td>
<td>385</td>
</tr>
<tr>
<td>Windows AD servers</td>
<td>385</td>
</tr>
<tr>
<td>Configuring a Windows AD server</td>
<td>386</td>
</tr>
<tr>
<td>User groups</td>
<td>386</td>
</tr>
<tr>
<td>User group types</td>
<td>387</td>
</tr>
<tr>
<td>User group list</td>
<td>389</td>
</tr>
<tr>
<td>Configuring a user group</td>
<td>389</td>
</tr>
<tr>
<td>Configuring FortiGuard override options for a user group</td>
<td>391</td>
</tr>
<tr>
<td>Configuring SSL VPN user group options</td>
<td>392</td>
</tr>
<tr>
<td>Authentication peers and peer groups</td>
<td>394</td>
</tr>
<tr>
<td>Configuring peers and peer groups</td>
<td>394</td>
</tr>
<tr>
<td>AntiVirus</td>
<td>397</td>
</tr>
<tr>
<td>Order of operations</td>
<td>397</td>
</tr>
<tr>
<td>Antivirus elements</td>
<td>397</td>
</tr>
<tr>
<td>FortiGuard antivirus</td>
<td>398</td>
</tr>
<tr>
<td>Antivirus settings and controls</td>
<td>399</td>
</tr>
<tr>
<td>File pattern</td>
<td>400</td>
</tr>
<tr>
<td>Viewing the file pattern list catalog</td>
<td>400</td>
</tr>
<tr>
<td>Creating a new file pattern list</td>
<td>401</td>
</tr>
<tr>
<td>Viewing the file pattern list</td>
<td>401</td>
</tr>
<tr>
<td>Configuring the file pattern list</td>
<td>402</td>
</tr>
<tr>
<td>Quarantine</td>
<td>402</td>
</tr>
<tr>
<td>Viewing the Quarantined Files list</td>
<td>403</td>
</tr>
<tr>
<td>Viewing the AutoSubmit list</td>
<td>404</td>
</tr>
<tr>
<td>Configuring the AutoSubmit list</td>
<td>404</td>
</tr>
<tr>
<td>Configuring quarantine options</td>
<td>405</td>
</tr>
<tr>
<td>Config</td>
<td>407</td>
</tr>
<tr>
<td>Viewing the virus list</td>
<td>407</td>
</tr>
<tr>
<td>Viewing the grayware list</td>
<td>407</td>
</tr>
</tbody>
</table>
### Antivirus CLI configuration
- system global optimize
- config antivirus heuristic
- config antivirus quarantine
- config antivirus service <service_name>

### Intrusion Protection
#### About intrusion protection
- IPS settings and controls
- When to use IPS

#### Predefined signatures
- Viewing the predefined signature list
- Using display filters
- Configuring predefined signatures
- Fine tuning IPS predefined signatures for enhanced system performance

#### Custom signatures
- Viewing the custom signature list
- Creating custom signatures

#### Protocol Decoders
- Viewing the protocol decoder list
- Configuring IPS protocol decoders
- Upgrading IPS protocol decoder list

#### Anomalies
- Viewing the traffic anomaly list
- Configuring IPS traffic anomalies

#### IPS CLI configuration
- system autoupdate ips
- ips global fail-open
- ips global ip_protocol
- ips global socket-size
- (config ips anomaly) config limit

### Web Filter
#### Order of web filtering
#### How web filtering works
#### Web filter controls
Contents

Content block

Viewing the web content block list catalog .................................................. 426
Creating a new web content block list ....................................................... 427
Viewing the web content block list ............................................................ 427
Configuring the web content block list ....................................................... 428
Viewing the web content exempt list catalog ............................................ 429
Creating a new web content exempt list ................................................... 429
Viewing the web content exempt list ......................................................... 430
Configuring the web content exempt list ................................................... 431

URL filter

Viewing the URL filter list catalog .............................................................. 431
Creating a new URL filter list .................................................................. 432
Viewing the URL filter list .......................................................................... 432
Configuring the URL filter list .................................................................... 433
Moving URLs in the URL filter list ............................................................. 435

FortiGuard - Web Filter

Configuring FortiGuard Web Filtering ....................................................... 436
Viewing the override list ............................................................................ 436
Configuring override rules ......................................................................... 437
Creating local categories ........................................................................... 439
Viewing the local ratings list ...................................................................... 439
Configuring local ratings ............................................................................ 440
Category block CLI configuration .............................................................. 441
FortiGuard Web Filtering reports ............................................................... 441

Antispam

Order of Spam Filtering ............................................................................ 443
Anti-spam filter controls ............................................................................ 444

Banned word

Viewing the antispam banned word list catalog ......................................... 446
Creating a new antispam banned word list ................................................. 447
Viewing the antispam banned word list .................................................... 447
Configuring the antispam banned word list ............................................. 448

Black/White List

Viewing the antispam IP address list catalog ............................................ 449
Creating a new antispam IP address list .................................................... 450
Viewing the antispam IP address list ......................................................... 450
Configuring the antispam IP address list ................................................ 451
Viewing the antispam email address list catalog .................................... 451
Creating a new antispam email address list ............................................. 452
Viewing the antispam email address list ................................................... 452
Configuring the antispam email address list ............................................ 453
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced antispam configuration</td>
<td>454</td>
</tr>
<tr>
<td>config spamfilter mheader</td>
<td>454</td>
</tr>
<tr>
<td>config spamfilter dnsbl</td>
<td>454</td>
</tr>
<tr>
<td>Using Perl regular expressions</td>
<td>455</td>
</tr>
<tr>
<td>Regular expression vs. wildcard match pattern</td>
<td>455</td>
</tr>
<tr>
<td>Word boundary</td>
<td>455</td>
</tr>
<tr>
<td>Case sensitivity</td>
<td>456</td>
</tr>
<tr>
<td>Perl regular expression formats</td>
<td>456</td>
</tr>
<tr>
<td>Example regular expressions</td>
<td>457</td>
</tr>
<tr>
<td>IM, P2P &amp; VoIP</td>
<td>459</td>
</tr>
<tr>
<td>Overview</td>
<td>459</td>
</tr>
<tr>
<td>Configuring IM/P2P protocols</td>
<td>461</td>
</tr>
<tr>
<td>How to enable and disable IM/P2P options</td>
<td>461</td>
</tr>
<tr>
<td>How to configure IM/P2P/VoIP options</td>
<td>462</td>
</tr>
<tr>
<td>How to configure IM/P2P applications</td>
<td>462</td>
</tr>
<tr>
<td>How to configure protocols that are not supported</td>
<td>462</td>
</tr>
<tr>
<td>Statistics</td>
<td>463</td>
</tr>
<tr>
<td>Viewing overview statistics</td>
<td>463</td>
</tr>
<tr>
<td>Viewing statistics by protocol</td>
<td>464</td>
</tr>
<tr>
<td>User</td>
<td>465</td>
</tr>
<tr>
<td>Viewing the Current Users list</td>
<td>465</td>
</tr>
<tr>
<td>Viewing the User List</td>
<td>466</td>
</tr>
<tr>
<td>Adding a new user to the User List</td>
<td>466</td>
</tr>
<tr>
<td>Configuring a policy for unknown IM users</td>
<td>467</td>
</tr>
<tr>
<td>Log&amp;Report</td>
<td>469</td>
</tr>
<tr>
<td>FortiGate Logging</td>
<td>469</td>
</tr>
<tr>
<td>FortiGuard Analysis Service</td>
<td>470</td>
</tr>
<tr>
<td>FortiGuard Analysis Service portal website</td>
<td>471</td>
</tr>
<tr>
<td>Log severity levels</td>
<td>471</td>
</tr>
<tr>
<td>High Availability cluster logging</td>
<td>472</td>
</tr>
<tr>
<td>Storing Logs</td>
<td>472</td>
</tr>
<tr>
<td>Logging to a FortiAnalyzer unit</td>
<td>472</td>
</tr>
<tr>
<td>Connecting to FortiAnalyzer using Automatic Discovery</td>
<td>473</td>
</tr>
<tr>
<td>Testing the FortiAnalyzer configuration</td>
<td>474</td>
</tr>
<tr>
<td>Logging to memory</td>
<td>475</td>
</tr>
<tr>
<td>Logging to a Syslog server</td>
<td>476</td>
</tr>
<tr>
<td>Logging to WebTrends</td>
<td>477</td>
</tr>
</tbody>
</table>
Configuring FortiGuard Analysis Service ................................................... 477
   Registering an account ............................................................................. 478
   Logging to a FortiGuard Analysis server ................................................... 479
   Accessing logs on the FortiGuard Analysis server .................................... 479
   FortiGuard Analysis reports ................................................................. 480

Log types ........................................................................................................ 481
   Traffic log ............................................................................................... 481
   Event log ............................................................................................... 482
   Antivirus log ........................................................................................... 483
   Web filter log .......................................................................................... 483
   Attack log ............................................................................................... 484
   Spam filter log ....................................................................................... 484
   IM and P2P log ...................................................................................... 484
   VoIP log ................................................................................................. 485

Accessing Logs ............................................................................................... 485
   Accessing log messages stored in memory .............................................. 486
   Accessing log message stored on the hard disk ....................................... 486
   Accessing logs stored on the FortiAnalyzer unit ....................................... 487
   Accessing logs stored on the FortiGuard Analysis server ......................... 487

Viewing log information ................................................................................ 488

Customizing the display of log messages ..................................................... 488
   Column settings ....................................................................................... 489
   Filtering log messages ............................................................................. 490

Content Archive ............................................................................................. 491
   Configuring content archiving ............................................................... 491
   Viewing content archives ....................................................................... 492

Alert Email ...................................................................................................... 493
   Configuring Alert Email ........................................................................ 493

Reports ............................................................................................................ 494
   Basic traffic reports ............................................................................... 494
   FortiAnalyzer reports ............................................................................. 496
   Configuring a FortiAnalyzer report .......................................................... 496
   Viewing FortiAnalyzer reports from a FortiGate unit ................................ 503
   Viewing parts of a FortiAnalyzer report ..................................................... 503
   Editing FortiAnalyzer reports ................................................................. 504
   Printing your FortiAnalyzer report .......................................................... 504

Index .............................................................................................................. 505
Introduction

Welcome and thank you for selecting Fortinet products for your real-time network protection.

FortiGate™ ASIC-accelerated multi-threat security systems improve network security, reduce network misuse and abuse, and help you use communications resources more efficiently without compromising the performance of your network. FortiGate Systems are ICSA-certified for Antivirus, Firewall, IPSec, SSL-TLS, IPS, Intrusion detection, and AntiSpyware services.

FortiGate Systems are dedicated, easily managed security device that delivers a full suite of capabilities including:

• Application-level services such as virus protection, intrusion protection, spam filtering, web content filtering, IM, P2P, and VoIP filtering
• Network-level services such as firewall, intrusion detection, IPSec and SSL VPN, and traffic shaping
• Management services such as user authentication, logging, reporting with FortiAnalyzer, administration profiles, secure web and CLI administrative access, and SNMP

The FortiGate security system uses Fortinet's Dynamic Threat Prevention System (DTPS™) technology, which leverages breakthroughs in chip design, networking, security and content analysis. The unique ASIC-accelerated architecture analyzes content and behavior in real-time, enabling key applications to be deployed right at the network edge where they are most effective at protecting your networks.

This chapter contains the following sections:

• What’s new in this release
• Introducing the FortiGate units
• Fortinet family of products
• About this document
• FortiGate documentation
• Customer service and technical support
• Register your Fortinet product

What’s new in this release

This section lists and describes some of the new features in FortiOS v3.0 MR5. For more information about new features in FortiOS v3.0 MR5 see the FortiOS v3.0 Upgrade Guide.

• FortiGate-224B – The FortiGate-224B operates two views or modes (switch and firewall) and supports VLAN trunking. See “Switch (FortiGate-224B only)” on page 207 for information about switch view.
• FortiGuard Management Services – This new service provides remote managing of firmware upgrades and backup of configuration files. See “FortiGuard Center” on page 186 for more information.
Introducing the FortiGate units

All FortiGate Unified Threat Management Systems deliver similar SOHO or enterprise-class network-based antivirus, content filtering, firewall, VPN, and network-based intrusion detection/prevention features.

FortiGate-5000 series chassis

The FortiGate-5000 series Security Systems are chassis-based systems that MSSPs and large enterprises can use to provide subscriber security services such as firewall, VPN, antivirus protection, spam filtering, web filtering and intrusion prevention (IPS). The wide variety of system configurations available with FortiGate-5000 series provide flexibility to meet the changing needs of growing high performance networks. The FortiGate-5000 series chassis support multiple hot-swappable FortiGate-5000 series modules and power supplies. This modular approach provides a scalable, high-performance and failure-proof solution.
Introduction

Introducing the FortiGate units

FortiGate-5140 chassis

You can install up to 14 FortiGate-5000 series modules in the 14 slots of the FortiGate-5140 ATCA chassis. The FortiGate-5140 is a 12U chassis that contains two redundant hot swappable DC power entry modules that connect to -48 VDC Data Center DC power. The FortiGate-5140 chassis also includes three hot swappable cooling fan trays.

FortiGate-5050 chassis

You can install up to five FortiGate-5000 series modules in the five slots of the FortiGate-5050 ATCA chassis. The FortiGate-5050 is a 5U chassis that contains two redundant DC power connections that connect to -48 VDC Data Center DC power. The FortiGate-5050 chassis also includes a hot swappable cooling fan tray.

FortiGate-5020 chassis

You can install one or two FortiGate-5000 series modules in the two slots of the FortiGate-5020 ATCA chassis. The FortiGate-5020 is a 4U chassis that contains two redundant AC to DC power supplies that connect to AC power. The FortiGate-5020 chassis also includes an internal cooling fan tray.

About the FortiGate-5000 series modules

Each FortiGate-5000 series module is a standalone security system that can also function as part of an HA cluster. All FortiGate-5000 series modules are also hot swappable. All FortiGate-5000 series units are high capacity security systems with multiple gigabit interfaces, multiple virtual domain capacity, and other high end FortiGate features. FortiOS Carrier runs on FortiGate-5000 series modules.
FortiGate-5005FA2 module
The FortiGate-5001SX module is an independent high-performance security system with eight Gigabit ethernet interfaces; two of which include Fortinet technology to accelerate small packet performance. The FortiGate-5005FA2 module also supports high-end features including 802.1Q VLANs, multiple virtual domains and specialized FortiGate-5000 series features such as base and fabric backplane switching and FortiOS Carrier MMS content processing and GTP protection.

FortiGate-5001SX module
The FortiGate-5001SX module is an independent high-performance security system with eight Gigabit ethernet interfaces. The FortiGate-5001SX module supports high-end features including 802.1Q VLANs and multiple virtual domains and specialized FortiGate-5000 series features such as base and fabric backplane switching and FortiOS Carrier MMS content processing and GTP protection.

FortiGate-5001FA2 module
The FortiGate-5001FA2 module is an independent high-performance security system with six Gigabit ethernet interfaces. The FortiGate-5001FA2 module is similar to the FortiGate-5001SX module except that two of the FortiGate-5001FA2 interfaces include Fortinet technology to accelerate small packet performance.

FortiGate-5002FB2 module
The FortiGate-5002FB2 module is an independent high-performance FortiGate security system with a total of 6 Gigabit ethernet interfaces. Two of the FortiGate-5002FB2 interfaces include Fortinet technology to accelerate small packet performance.

FortiGate-AMC modules
The FortiGate-AMC modules (including the FortiGate-ADM-XB2, FortiGate-ASM-FB4, and the FortiGate-ASM-SO8) add additional capabilities such as accelerated interfaces, hard disk space and so on to FortiGate units, such as the FortiGate-3600A unit and the FortiGate-3810 unit that contain AMC slots.

FortiGate-3810A
The FortiGate-3810A unit provides carrier-class levels of performance and reliability demanded by large enterprises and service providers. The unit uses multiple CPUs and FortiASIC chips to deliver throughput of up to 26 Gbps, meeting the needs of the most demanding applications. The FortiGate-3810A unit includes eight 10/100/1000 network interfaces, two SFP interfaces and also includes two dual-width and two single width ASM expansion modules.
FortiGate-3600A

The FortiGate-3600A unit provides carrier-class levels of performance and reliability demanded by large enterprises and service providers. The unit uses multiple CPUs and FortiASIC chips to deliver throughput of 4Gbps, meeting the needs of the most demanding applications. The FortiGate-3600A unit includes redundant power supplies, which minimize single-point failures, and supports load-balanced operation. The high-capacity, reliability and easy management makes the FortiGate-3600A a natural choice for managed service offerings.

FortiGate-3600

The FortiGate-3600 unit provides carrier-class levels of performance and reliability demanded by large enterprises and service providers. The unit uses multiple CPUs and FortiASIC chips to deliver throughput of 4Gbps, meeting the needs of the most demanding applications. The FortiGate-3600 unit includes redundant power supplies, which minimize single-point failures, and supports load-balanced operation. The high-capacity, reliability and easy management makes the FortiGate-3600 a natural choice for managed service offerings.

FortiGate-3000

The FortiGate-3000 unit provides the carrier-class levels of performance and reliability demanded by large enterprises and service providers. The unit uses multiple CPUs and FortiASIC chips to deliver a throughput of 3Gbps, meeting the needs of the most demanding applications. The FortiGate-3000 unit includes redundant power supplies to minimize single-point failures, including load-balanced operation and redundant failover with no interruption in service. The high capacity, reliability, and easy management of the FortiGate-3000 makes it a natural choice for managed service offerings.
Introducing the FortiGate units

FortiGate-1000A

The FortiGate-1000A Security System is a high-performance solution for the most demanding large enterprise and service providers. The FortiGate-1000A automatically keeps up to date information on Fortinet’s FortiGuard Subscription Services by the FortiGuard Distribution Network, ensuring around-the-clock protection against the latest viruses, worms, trojans and other threats. The FortiGate-1000A has flexible architecture to quickly adapt to emerging technologies such as IM, P2P or VOIP including identity theft methods such as spyware, phishing and pharming attacks.

FortiGate-1000AFA2

The FortiGate-1000AFA2 Security System is a high-performance solution for the most demanding large enterprise and service providers. The FortiGate-1000AFA2 features two extra optical fiber ports with Fortinet's FortiAccel™ technology, enhancing small packet performance. The FortiGate-1000AFA2 also delivers critical security functions in a hardened security platform, tuned for reliability, usability, rapid deployment, low operational costs and most importantly a superior detection rate against known and unknown anomalies.

FortiGate-1000

The FortiGate-1000 unit is designed for larger enterprises. The FortiGate-1000 meets the needs of the most demanding applications, using multiple CPUs and FortiASIC chips to deliver a throughput of 2Gps. The FortiGate-1000 unit includes support for redundant power supplies to minimize single-port failures, load-balanced operation, and redundant failover with no interruption in service.

FortiGate-800

The FortiGate-800 provides high throughput, a total of eight network connections, (four of which are user-defined), VLAN support, and virtual domains. The FortiGate-800 also provides stateful failover HA, when you are configuring a cluster of FortiGate units. The FortiGate-800 is a natural choice for large enterprises, who demand top network security performance.
FortiGate-800F
The FortiGate-800F provides the same features as the FortiGate-800, using four fibre-optic Internal, External, DMZ and HA interfaces. The FortiGate-800F also provides stateful failover HA, and support for the RIP and OSPF routing protocols. The FortiGate-800F provides the flexibility, reliability and easy management large enterprises are looking for.

FortiGate-500A
The FortiGate-500A unit provides the carrier-class levels of performance and reliability demanded by large enterprises and service providers. With a total of 10 network connections, (including a 4-port LAN switch), and high-availability features with automatic failover with no session loss, the FortiGate-500A is the choice for mission critical applications. The flexibility, reliability, and easy management of the FortiGate-500A makes it a natural choice for managed service offerings.

FortiGate-500
The FortiGate-500 unit is designed for larger enterprises. The flexibility, reliability, and easy management makes the FortiGate-500 a natural choice for managed service offerings. The FortiGate-500 supports high availability (HA).

FortiGate-400A
The FortiGate-400A unit meets enterprise-class requirements for performance, availability, and reliability. The FortiGate-400A also supports high availability (HA) and features automatic failover with no session loss, making it the choice for mission critical applications.

FortiGate-400
The FortiGate-400 unit is designed for larger enterprises. The FortiGate-400 unit is capable of throughput up to 500Mbps and supports high availability (HA), which includes automatic failover with no session loss.
Introducing the FortiGate units

FortiGate-300A

The FortiGate-300A unit meets enterprise-class requirements for performance, availability, and reliability. The FortiGate-300A also supports high availability (HA) and includes automatic failover with no session loss, making the FortiGate-300A a good choice for mission-critical applications.

FortiGate-300

The FortiGate-300 unit is designed for larger enterprises. The FortiGate-300 unit features high availability (HA), which includes automatic failover with no session loss. This feature makes the FortiGate-300 an excellent choice for mission-critical applications.

FortiGate-224B

The FortiGate-224B unit provides both layer-2 and layer-3 security features. It provides protection between external networks or the Internet and your internal networks, as well as providing protection between different segments of your internal network.

The FortiGate-224B features:

- firewall view - the unit is the same as other FortiGate models, except that in firewall view the FortiGate-224B has 28 network interfaces. This is the default mode.
- switch mode - port1 through port26 are switch ports on the swlan interface. The web-based manager Switch menu is available, providing access to enhanced security features. HA is not supported. See “Switch (FortiGate-224B only)” on page 207 for information about switch view.
- Access control to enforce software security requirements for client workstations. You can apply this at the port level or at the inter-VLAN level. Non-compliant clients are restricted to a quarantine VLAN. See “Configuring intra-VLAN firewall policies (FortiGate-224B only)” on page 275.
- Route and port-based VLANs.
- Firewall protection between internal networks and the Internet.
- Firewall protection between secure switch ports.
- Firewall-like security policies to control communication between switch ports.
FortiGate-200A
The FortiGate-200A unit is an easy-to-deploy and easy-to-administer solution that delivers exceptional value and performance for small office, home office and branch office applications.

FortiGate-200
The FortiGate-200 unit is designed for small businesses, home offices or even branch office applications. The FortiGate-200 unit is an easy-to-deploy and easy-to-administer solution. The FortiGate-200 also supports high availability (HA).

FortiGate-100A
The FortiGate-100A unit is designed to be an easy-to-administer solution for small offices, home offices, and branch office applications.

The FortiGate-100A supports advanced features such as 802.1Q VLAN, virtual domains, and the RIP and OSPF routing protocols.

FortiGate-100
The FortiGate-100 unit is designed for SOHO, SMB and branch office applications.

The FortiGate-100 supports advanced features such as 802.1Q VLAN, virtual domains, high availability (HA), and the RIP and OSPF routing protocols.

FortiGate-60B
The FortiGate-60B is designed for telecommuters and small remote offices with ten or fewer employees. The FortiGate-60B provides complete real-time network protection through a combination of network-based antivirus, web and email content filtering, firewall, VPN, network-based intrusion detection and prevention, and traffic shaping. The FortiGate-60B integrates a PC (also called PCMCIA) card for additional expansion including a Type II PC Card based 3G wireless broadband and MiniPCI Card based IEEE802.11b/g WiFi broadband. This will enable organizations to establish secure 3G/WiFi wireless broadband network access instantly without the need for a fixed internet connection. FortiGate-60B also integrates a 2-port FXO VOIP Card. This enables the organizations to use the low-cost VOIP communication.
FortiWiFi-60B

The FortiWiFi-60B is designed for telecommuters and small remote offices with ten or fewer employees. The FortiWiFi-60B provides complete real-time network protection through a combination of network-based antivirus, web and email content filtering, firewall, VPN, network-based intrusion detection and prevention, and traffic shaping. The FortiWiFi-60B supports wireless 802.11a/b/g standards and integrates PCMCIA card slot for feature expansion such as a 2-port FXO VOIP Card. This enables the organizations to use the low-cost VOIP communication.

FortiGate-60/60M/ADSL

The FortiGate-60 unit is designed for telecommuters remote offices, and retail stores. The FortiGate-60 unit includes an external modem port that can be used as a backup or stand alone connection to the Internet while the FortiGate-60M unit includes an internal modem that can also be used either as a backup or a standalone connection to the Internet. The FortiGate-60ADSL includes an internal ADSL modem.

FortiWiFi-60/60A/60AM

The FortiWiFi-60 model provides a secure, wireless LAN solution for wireless connections. It combines mobility and flexibility with FortiWiFi Antivirus Firewall features, and can be upgraded to future radio technologies. The FortiWiFi-60 serves as the connection point between wireless and wired networks or the center-point of a standalone wireless network.

FortiGate-50B

The FortiGate-50B is designed for telecommuters and small remote offices with 10 to 50 employees. The FortiGate-50B unit includes two WAN interfaces for redundant connections to the Internet. The FortiGate-50B unit also features a 3-port switch for internal network connections and supports HA configurations with other FortiGate-50B units.
FortiGate-50A

The FortiGate-50A unit is designed for telecommuters and small remote offices with 10 or fewer employees. The FortiGate-50 unit includes an external modem port that can be used as a backup or stand alone connection to the Internet.

Fortinet family of products

Fortinet offers a family of products that includes both software and hardware appliances for a complete network security solution including mail, logging, reporting, network management, and security along with FortiGate Unified Threat Manager Systems. For more information on the Fortinet product family, go to www.fortinet.com/products.

FortiGuard Subscription Services

FortiGuard Subscription Services are security services created, updated and managed by a global team of Fortinet security professionals. They ensure the latest attacks are detected and blocked before harming your corporate resources or infecting your end-user computing devices. These services are created with the latest security technology and designed to operate with the lowest possible operational costs.

For more information about FortiGuard services, go to the FortiGuard Center at www.fortiguard.com.

FortiAnalyzer

FortiAnalyzer™ provides network administrators with the information they need to enable the best protection and security for their networks against attacks and vulnerabilities. FortiAnalyzer features include:

• collects logs from FortiGate devices and syslog devices and FortiClient
• creates hundreds of reports using collected log data
• scans and reports vulnerabilities
• stores files quarantined from a FortiGate unit

The FortiAnalyzer unit can also be configured as a network analyzer to capture real-time traffic on areas of your network where firewalls are not employed. You can also use the unit as a storage device where users can access and share files, including the reports and logs that are saved on the FortiAnalyzer hard disk.

FortiClient

FortiClient™ Host Security software provides a secure computing environment for both desktop and laptop users running the most popular Microsoft Windows operating systems. FortiClient offers many features including:

• creating VPN connections to remote networks
• configuring real-time protection against viruses
• guarding against modification of the Windows registry
About this document

This FortiGate Version 3.0 MR5 Administration Guide provides detailed information about FortiGate™ web-based manager options and how to use them. This guide also contains some information about the FortiGate CLI.

This administration guide describes web-based manager functions in the same order as the web-based manager menu. The document begins with a general description of the FortiGate web-based manager and a description of FortiGate virtual domains. Following these chapters, each item in the System menu, Router menu, Firewall menu, and VPN menu gets a separate chapter. Then User, AntiVirus, Intrusion Protection, Web Filter, AntiSpam, IM/P2P, and Log & Report are all described in single chapters. The document concludes with a detailed index.

The most recent version of this document is available from the FortiGate page of the Fortinet Technical Documentation web site. The information in this document is also available in a slightly different form as FortiGate web-based manager online help.

FortiClient also offers a silent installation feature, enabling an administrator to efficiently distribute FortiClient to several users’ computers with preconfigured settings.

FortiManager

FortiManager™ meets the needs of large enterprises (including managed security service providers) responsible for establishing and maintaining security policies across many dispersed FortiGate installations. With FortiManager you can configure multiple FortiGate devices and monitor their status. You can also view real-time and historical logs for FortiGate devices. FortiManager emphasizes ease of use, including easy integration with third party systems.

FortiBridge

FortiBridge™ products are designed to provide enterprise organizations operating FortiGate units in Transparent mode with continuous network traffic flow in the event of a power outage or a FortiGate system failure. The FortiBridge unit bypasses the FortiGate unit to make sure that the network can continue processing traffic. FortiBridge products are easy to use and deploy, including providing customizable actions a FortiBridge unit takes in the event of a power outage or FortiGate system failure.

FortiMail

FortiMail™ provides powerful, flexible heuristic scanning and reporting capabilities to incoming and outgoing email traffic. The FortiMail unit has reliable, high performance features for detecting and blocking malicious attachments and spam, such as FortiGuard Antispam/Antivirus support, heuristic scanning, greylisting, and Bayesian scanning. Built on Fortinet’s award winning FortiOS and FortiASIC technology, FortiMail antivirus technology extends full content inspection capabilities to detect the most advanced email threats.
You can find more information about FortiOS v3.0 from the FortiGate page of the Fortinet Technical Documentation web site as well as from the Fortinet Knowledge Center.

This administration guide contains the following chapters:

- **Web-based manager** provides an introduction to the features of the FortiGate web-based manager, the button bar, and includes information about how to use the web-based manager online help.
- **System Status** describes the System Status page, the dashboard of your FortiGate unit. At a glance you can view the current system status of the FortiGate unit including serial number, uptime, FortiGuard license information, system resource usage, alert messages and network statistics. This section also describes status changes that you can make, including changing the unit firmware, host name, and system time. Finally this section also describes the topology viewer that is available on all FortiGate models except those with model numbers 50 and 60.
- **Using virtual domains** describes how to use virtual domains to operate your FortiGate unit as multiple virtual FortiGate units, providing separate firewall and routing services to multiple networks.
- **System Network** explains how to configure physical and virtual interfaces and DNS settings on the FortiGate unit.
- **System Wireless** describes how to configure the Wireless LAN interface on a FortiWiFi-60 unit.
- **System DHCP** provides information about how to configure a FortiGate interface as a DHCP server or DHCP relay agent.
- **System Config** contains procedures for configuring HA and virtual clustering, configuring SNMP and replacement messages, and changing the operation mode.
- **System Administrators** guides you through adding and editing administrator accounts, defining access profiles for administrators, configuring central management using the FortiGuard Management Service or FortiManager, defining general administrative settings such as language, timeouts, and web administration ports.
- **System Maintenance** details how to back up and restore the system configuration using a management computer or a USB disk, use revision control, enable FortiGuard services and FortiGuard Distribution Network (FDN) updates, and enter a license key to increase the maximum number of virtual domains.
- **System Chassis (FortiGate-5000 series)** describes information displayed on the system chassis web-based manager pages about all of the hardware components in your FortiGate-5140 or FortiGate-5050 chassis.
- **Switch (FortiGate-224B only)** describes how to configure secure switch features on the FortiGate-224B unit in switch view.
- **Router Static** explains how to define static routes and create route policies. A static route causes packets to be forwarded to a destination other than the factory configured default gateway.
- **Router Dynamic** contains information about how to configure dynamic protocols to route traffic through large or complex networks.
- **Router Monitor** explains how to interpret the Routing Monitor list. The list displays the entries in the FortiGate routing table.
• **Firewall Policy** describes how to add firewall policies to control connections and traffic between FortiGate interfaces, zones, and VLAN subinterfaces.
• **Firewall Address** describes how to configure addresses and address groups for firewall policies.
• **Firewall Service** describes available services and how to configure service groups for firewall policies.
• **Firewall Schedule** describes how to configure one-time and recurring schedules for firewall policies.
• **Firewall Virtual IP** describes how to configure and use virtual IP addresses and IP pools.
• **Firewall Protection Profile** describes how to configure protection profiles for firewall policies.
• **VPN IPSEC** provides information about the tunnel-mode and route-based (interface mode) Internet Protocol Security (IPSec) VPN options available through the web-based manager.
• **VPN PPTP** explains how to use the web-based manager to specify a range of IP addresses for PPTP clients.
• **VPN SSL** provides information about basic SSL VPN settings.
• **VPN Certificates** explains how to manage X.509 security certificates.
• **User** details how to control access to network resources through user authentication.
• **AntiVirus** explains how to enable antivirus options when you create a firewall protection profile.
• **Intrusion Protection** explains how to configure IPS options when a firewall protection profile is created.
• **Web Filter** explains how to configure web filter options when a firewall protection profile is created.
• **Antispam** explains how to configure spam filter options when a firewall protection profile is created.
• **IM, P2P & VoIP** explains how to configure IM, P2P, and VoIP options when a firewall protection profile is created. You can view IM, P2P, and VoIP statistics to gain insight into how the protocols are being used within the network.
• **Log&Report** describes how to enable logging, view log files, and view the basic reports available through the web-based manager.

**Document conventions**

The following document conventions are used in this guide:

• In the examples, private IP addresses are used for both private and public IP addresses.
• Notes and Cautions are used to provide important information:

  **Note:** Highlights useful additional information.

  **Caution:** Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.
Typographic conventions

Fortinet documentation uses the following typographical conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu commands</td>
<td>Go to VPN &gt; IPSEC &gt; Phase 1 and select Create New.</td>
</tr>
<tr>
<td>Keyboard input</td>
<td>In the Gateway Name field, type a name for the remote VPN peer or client (for example, Central_Office_1).</td>
</tr>
</tbody>
</table>
| Code examples           | config sys global
                          | set ips-open enable
                          | end                      |
| CLI command syntax      | config firewall policy
                          | edit id_integer
                          | set http_retry_count <retry_integer>
                          | set natip <address_ipv4mask>
                          | end                      |
| Document names          | FortiGate Administration Guide                                         |
| File content            | <HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>
                          | <BODY><H4>You must authenticate to use this service.</H4>              |
| Program output          | Welcome!                                                               |
| Variables               | <address_ipv4>                                                         |

FortiGate documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at http://docs.forticare.com.

The following FortiGate product documentation is available:

- *FortiGate QuickStart Guide*
  Provides basic information about connecting and installing a FortiGate unit.

- *FortiGate Installation Guide*
  Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.

- *FortiGate Administration Guide*
  Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.

- *FortiGate online help*
  Provides a context-sensitive and searchable version of the Administration Guide in HTML format. You can access online help from the web-based manager as you work.
• **FortiGate CLI Reference**
  Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.

• **FortiGate Log Message Reference**
  Available exclusively from the Fortinet Knowledge Center, the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.

• **FortiGate High Availability Overview and FortiGate High Availability User Guide**
  These documents contain in-depth information about the FortiGate High Availability (HA) feature and the FortiGate clustering protocol.

• **FortiGate IPS User Guide**
  Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.

• **FortiGate IPSec VPN User Guide**
  Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.

• **FortiGate SSL VPN User Guide**
  Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.

• **FortiGate PPTP VPN User Guide**
  Explains how to configure a PPTP VPN using the web-based manager.

• **FortiGate Certificate Management User Guide**
  Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.

• **FortiGate VLANs and VDOMs User Guide**
  Describes how to configure VLANs and VDOMs in both NAT/Route and Transparent mode. Includes detailed examples.

**Fortinet Tools and Documentation CD**

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current for your product at shipping time. For the latest versions of all Fortinet documentation see the Fortinet Technical Documentation web site at [http://docs.forticare.com](http://docs.forticare.com).

**Fortinet Knowledge Center**

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at [http://kc.forticare.com](http://kc.forticare.com).

**Comments on Fortinet technical documentation**

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.
Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

Register your Fortinet product

Register your Fortinet product to receive Fortinet customer services such as product updates and technical support. You must also register your product for FortiGuard services such as FortiGuard Antivirus and Intrusion Prevention updates and for FortiGuard Web Filtering and AntiSpam.

Register your product by visiting http://support.fortinet.com and selecting Product Registration.

To register, enter your contact information and the serial numbers of the Fortinet products that you or your organization have purchased. You can register multiple Fortinet products in a single session without re-entering your contact information.
Web-based manager

This section describes the features of the user-friendly web-based manager administrative interface of your FortiGate unit.

Using HTTP or a secure HTTPS connection from any computer running a web browser, you can configure and manage the FortiGate unit. The web-based manager supports multiple languages. You can configure the FortiGate unit for HTTP and HTTPS administration from any FortiGate interface.

Figure 2: Example FortiGate-5001SX Web-based manager dashboard

You can use the web-based manager to configure most FortiGate settings and to monitor the status of the FortiGate unit. Configuration changes made using the web-based manager are effective immediately without resetting the firewall or interrupting service. Once you are satisfied with a configuration, you can back it up. The saved configuration can be restored at any time.

For information about connecting to the web-based manager, see “Connecting to the web-based manager” in the Installation Guide for your unit.
This section describes:

- Button bar features
- Web-based manager pages

**Button bar features**

The button bar in the upper right corner of the web-based manager provides access to several important FortiGate features.

![Figure 3: Web-based manager button bar](image)

**Contact Customer Support**

The Contact Customer Support button opens the Fortinet Support web page in a new browser window. From this page you can:

- Access the Fortinet Knowledge Center.
- Log into Customer Support (Support Login).
- Register your FortiGate unit (Product Registration).
- Find out about Fortinet Training and Certification.
- Visit the FortiGuard Center.

To register your FortiGate unit, go to Product Registration and follow the instructions. You must register your FortiGate unit to receive product updates, technical support, and FortiGuard services.

**Backup your FortiGate configuration**

Select the Backup Configuration button to backup your FortiGate configuration. You can backup your FortiGate configuration to:

- The local PC that you are using to manage the FortiGate unit.
- A management station. This can be a FortiManager unit or the FortiGuard Management Service; as configured from **System > Admin > Central Management**. See “Central Management” on page 173.
- A USB disk if your FortiGate has a USB port and you have connected a USB disk to it.

For more information about backing up and restoring your FortiGate configuration, see “Backup and Restore” on page 181.
Using the Online Help

The Online Help button displays online help for the current web-based manager page. The online help page that is displayed contains information and procedures related to the controls on the current web-based manager page. Most help pages also contains hyperlinks to related topics. The online help system also includes a number of controls that you can use to find additional information.

Figure 5: Viewing system status online help page

Open the online help navigation pane. From the navigation pane you can use the online help table of contents, index, and search to access all of the information in the online help. The online help is organized in the same way as the FortiGate web-based manager and the FortiGate Administration Guide.

Previous

Display the previous page in the online help.

Next

Display the next page in the online help.

Email

Send an email to Fortinet Technical Documentation at techdoc@fortinet.com. You can use this email address to let us know if you have a comment about or correction for the online help or any other Fortinet technical documentation product.

Print

Print the current online help page.

Bookmark

Add an entry for this online help page to your browser bookmarks or favorites list. Use this button to make it easier to find helpful online help pages. You cannot use the Bookmark icon to add an entry to your favorites list if you are viewing online help from Internet Explorer running on a management PC with Windows XP and service pack 2 installed.

Select Show Navigation to display the online help navigation pane.
About searching the online help

Using the online help search, you can search for one word or multiple words in the full text of the FortiGate online help system. Please note the following about the search:

- If you search for multiple words, the search finds help pages that contain all of the words that you entered. The search does not find help pages that only contain one of the words that you entered.

- The help pages found by the search are ranked in order of relevance. The higher the ranking, the more likely the help page includes useful or detailed information about the word or words that you are searching for. Help pages with one or more of the search words in the help page title are ranked highest.

- You can use the asterisk (*) as a search wildcard character that is replaced by any number of characters. For example, if you search for auth* the search finds help pages containing auth, authenticate, authentication, authenticates, and so on.

- In some cases the search only finds exact matches. For example if you search for windows the search may not find pages containing the word window. You can work around this using the * wildcard (for example by searching for window*).

To search in the help system

1. From any web-based manager page, select the online help button.
2. Select Show Navigation to display the online help navigation pane.
3. Select Search.
4. Type one or more words to search for in the search field and then press enter or select Go.

The search pane lists the names of all the online help pages that contain the word or words that you entered. Select a name from the list to display that help page.

**Using the keyboard to navigate in the online help**

You can use the keyboard shortcuts listed in Table 1 to display and find information in the online help.

<table>
<thead>
<tr>
<th>Key</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alt+1</td>
<td>Display the table of contents.</td>
</tr>
<tr>
<td>Alt+2</td>
<td>Display the index.</td>
</tr>
<tr>
<td>Alt+3</td>
<td>Display the Search tab.</td>
</tr>
<tr>
<td>Alt+4</td>
<td>Go to the previous page.</td>
</tr>
<tr>
<td>Alt+5</td>
<td>Go to the next page.</td>
</tr>
<tr>
<td>Alt+7</td>
<td>Send an email to Fortinet Technical Documentation at <a href="mailto:techdoc@fortinet.com">techdoc@fortinet.com</a>. You can use this email address to let us know if you have a comment about or correction for the online help or any other Fortinet technical documentation product.</td>
</tr>
<tr>
<td>Alt+8</td>
<td>Print the current online help page.</td>
</tr>
<tr>
<td>Alt+9</td>
<td>Add an entry for this online help page to your browser bookmarks or favorites list. Use this button to make it easier to find helpful online help pages.</td>
</tr>
</tbody>
</table>

**Logout**

The Logout button immediately logs you out of the web-based manager. Log out before you close the browser window. If you simply close the browser or leave the web-based manager, you remain logged-in until the idle timeout (default 5 minutes) expires.
Web-based manager pages

The web-based manager interface consists of a menu and pages, many of which have multiple tabs. When you select a menu item, such as System, it expands to reveal a submenu. When you select one of the submenu items, the associated page opens at its first tab. To view a different tab, select the tab.

The procedures in this manual direct you to a page by specifying the menu item, the submenu item and the tab, like this:

1. Go to **System > Network > Interface**.

Figure 7: Parts of the web-based manager (shown for the FortiGate-50B)

- Web-based manager menu
- Lists
- Adding filters to web-based manager lists
- Icons
- Button bar features

Web-based manager menu

The menu provides access to configuration options for all major features of the FortiGate unit.

**System**
Configure system facilities, such as network interfaces, virtual domains, DHCP services, High Availability (HA), system time and set system options.

**Switch**
This applies only to the FortiGate-224B unit in switch view. Configure secure switch features, including switch-VLANs, port quarantine, spanning-tree protocol, QoS settings, IGMP snooping and 802.1X authentication.

**Router**
Configure FortiGate static and dynamic routing.
Lists

Many of the web-based manager pages are lists. There are lists of network interfaces, firewall policies, administrators, users, and so on.

Figure 8: Example of a web-based manager list

The list shows some information about each item and the icons in the right-most column enable you to take action on the item. In this example, you can select Delete to remove the item or select Edit to modify the item.

To add another item to the list, you select Create New. This opens a dialog box in which you define the new item. The dialog box for creating a new item is similar to the one for editing an existing item.

Adding filters to web-based manager lists

On the following web-based manager pages that contain complex lists, you can add filters to control the information that is displayed by the list.

- Session list (see “Viewing the session list” on page 63)
- Firewall policy list (see “Viewing the firewall policy list” on page 268)
- IPSec VPN Monitor (see “Monitor” on page 358)
- Intrusion protection predefined signatures list (see “Viewing the predefined signature list” on page 413)
- Log and report log access list (see “Accessing Logs” on page 485)

Filters are useful for reducing the number of entries that are displayed on a list so that you can focus on the information that is important to you. For example, you can go to System > Status and in the Statistics section, select Details on the Sessions line to view the communications sessions currently being processed by the FortiGate unit. A busy FortiGate unit may be processing hundreds or
thousands of communications sessions. If you are looking for specific communications sessions, you can add filters to make it easier to find them. For example, you might be looking for all communications sessions being accepted by a specific firewall policy. You can add a Policy ID filter to display only the sessions for a particular Policy ID or range of Policy IDs.

You add filters for a web-based manager list by selecting any filter icon to display the Edit Filters window. From the Edit Filters window you can select any column name to filter and configure the filter for that column. You can add filters for one column or for multiple columns. You can configure multiple columns and then select OK. The filter icon remains grey for unfiltered columns and changes to green for filtered columns.

The filter configuration is retained after leaving the web-based manager page and even after logging out of the web-based manager or rebooting the FortiGate unit.

Different filter styles are available depending on the type of information displayed in individual columns. In all cases you configure filters by specifying what to filter on and whether to display information that matches the filter or you can select NOT to display information that does not match the filter.

**Filters for columns that contain numbers**

If the column includes numbers (for example, IP addresses or firewall policy IDs) you can filter by a single number or a range of numbers.
Filters for columns containing text strings

If the column includes text strings (for example, names) you can filter by a text string. You can also filter information that is an exact match for the text string (equals), that contains the text string, or that does not equal or does not contain the text string. You can also specify whether to match the capitalization (case) of the text string.

Figure 11: Example firewall policy list filter to display all policies that do not include a source address with a name that contains the string “My_Address”

Filters for columns that can only contain specific items

For columns that can only contain specific items (for example, a log message severity or a pre-defined signature action) you can select a single item from a list. In this case you can only filter on a single selected item.

Figure 12: Example IPS predefined signature list filter to display all signatures with Action set to reset
Custom filters

Other custom filters are also available. You can filter log messages according to date range and time range. You can also set the level log message filter to display log message with multiple severity levels.

Figure 13: Example log access filter to display all log messages with level of alert, critical, error, or warning

Icons

The web-based manager has icons in addition to buttons to enable you to interact with the system. There are tooltips to assist you in understanding the function of the icon. Pause the mouse pointer over the icon to view the tooltip. Table 2 describes the icons that are available in the web-based manager.

Table 2: web-based manager icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Change Password" /></td>
<td>Change Password</td>
<td>Change the administrator password. This icon appears in the Administrators list if your access profile enables you to give write permission to administrators.</td>
</tr>
<tr>
<td><img src="image" alt="Clear" /></td>
<td>Clear</td>
<td>Clear a log file.</td>
</tr>
<tr>
<td><img src="image" alt="Collapse" /></td>
<td>Collapse</td>
<td>Collapse this section to hide some fields. This icon is used in some dialog boxes and some lists.</td>
</tr>
<tr>
<td><img src="image" alt="Column Settings" /></td>
<td>Column Settings</td>
<td>Select the columns to display. This icon is used in Log Access and firewall Policy lists among others.</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Delete</td>
<td>Delete an item. This icon appears in lists where the item can be deleted and you have edit permission on the page.</td>
</tr>
<tr>
<td><img src="image" alt="Description" /></td>
<td>Description</td>
<td>The tooltip for this icon displays the Description field for this table entry.</td>
</tr>
<tr>
<td><img src="image" alt="Download or Backup" /></td>
<td>Download or Backup</td>
<td>Download a log file or back up a configuration file.</td>
</tr>
<tr>
<td><img src="image" alt="Download" /></td>
<td>Download</td>
<td>Download a Certificate Signing Request.</td>
</tr>
</tbody>
</table>
Table 2: web-based manager icons  (Continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Edit</td>
<td>Edit a configuration. This icon appears in lists where you have write permission on the page.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Expand</td>
<td>Expand this section to reveal more fields. This icon is used in some dialog boxes and some lists. Sometimes called a twistie.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Filter</td>
<td>Set a filter on one or more columns in this table. A dialog opens in which you can specify filters. The icon is green on columns where a filter is active, otherwise it is grey. If you mouse over a green filter icon the web-based manager displays the filter setting.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Go</td>
<td>Run a command. For example, on some lists you can specify a filter for the list and select Go to enable the filter.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Insert Policy</td>
<td>Create a new policy to precede the current one.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Move</td>
<td>Move item in list.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Next page</td>
<td>View the next page of a list.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Previous page</td>
<td>View the previous page of a list.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Refresh</td>
<td>Update the information on this page.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Restore</td>
<td>Restore a configuration from a file.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>View</td>
<td>View a configuration. This icon appears in lists instead of the Edit icon when you do not have write permission to change a setting.</td>
</tr>
</tbody>
</table>
System Status

This section describes the System Status page, the dashboard of your FortiGate unit. At a glance you can view the current system status of the FortiGate unit including serial number, uptime, FortiGuard™ license information, system resource usage, alert messages and network statistics.

Note: Your browser must support Javascript to view the System Status page.

This section describes:
- Status page
- Changing system information
- Changing the FortiGate firmware
- Viewing operational history
- Manually updating FortiGuard definitions
- Viewing Statistics
- Topology viewer

Status page

View the System Status page, also known as the system dashboard, for a snapshot of the current operating status of the FortiGate unit. FortiGate administrators whose access profiles permit read access to system configuration can view system status information.

When the FortiGate unit is part of an HA cluster, the Status page includes basic HA cluster status information including the name of the cluster and the cluster members including their hostnames. To view more complete status information for the cluster, go to System > Config > HA. For more information, see “HA” on page 135. HA is not available on FortiGate models 50A, 50AM, and 224B.

FortiGate administrators whose access profiles permit write access to system configuration can change or update FortiGate unit information. For information on access profiles, see “Access profiles” on page 169.

Viewing system status

The System Status page displays by default when you log in to the web-based manager.

At any time, go to System > Status to view the System Status page.

To view this page, your access profile must permit read access to system configuration. If you also have system configuration write access, you can modify system information and update FortiGuard - AV and FortiGuard - IPS definitions. For information on access profiles, see “Access profiles” on page 169.
The System Status page is completely customizable. You can select which displays to show, where they are located on the page, and if they are minimized or maximized. Each display has an icon associated with it for easy recognition when minimized.

Figure 14: System Status page

Select Add Content to add any of the displays not currently shown on the System Status page. Any displays current on the System Status page will be greyed out as you can only have one of each display on the System Status page. Optionally select Back to default to restore the historic System Status page configuration.

Position your mouse over a display’s titlebar to see your available options for that display. The options vary slightly from display to display.

Figure 15: A minimized display

<table>
<thead>
<tr>
<th>Display Title</th>
<th>Shows the name of the display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twistie arrow</td>
<td>Select to maximize or minimize the display.</td>
</tr>
<tr>
<td>Refresh icon</td>
<td>Select to update the displayed information.</td>
</tr>
<tr>
<td>Close icon</td>
<td>Select to close the display. You will be prompted to confirm the close.</td>
</tr>
</tbody>
</table>
System information

Figure 16: Example FortiGate-5001 System Information

<table>
<thead>
<tr>
<th>System Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
</tr>
<tr>
<td>Uptime</td>
</tr>
<tr>
<td>System Time</td>
</tr>
<tr>
<td>Cluster Name</td>
</tr>
<tr>
<td>Virtual Cluster 1</td>
</tr>
<tr>
<td>Virtual Cluster 2</td>
</tr>
<tr>
<td>Firmware Version</td>
</tr>
<tr>
<td>Virtual Domain</td>
</tr>
<tr>
<td>Current Administrators</td>
</tr>
</tbody>
</table>

Serial Number  The serial number of the current FortiGate unit. The serial number is specific to the FortiGate unit and does not change with firmware upgrades.

Uptime  The time in days, hours, and minutes since the FortiGate unit was last started.

System Time  The current date and time according to the FortiGate unit internal clock.
Select Change to change the time or configure the FortiGate unit to get the time from an NTP server. See “Configuring system time” on page 58.

Host Name  The host name of the current FortiGate unit.
If the FortiGate unit is in HA mode, this field is not displayed.
Select Change to change the host name.
See “Changing the FortiGate unit host name” on page 59.

Cluster Name  The name of the HA cluster for this FortiGate unit. See “HA” on page 135.
The FortiGate unit must be operating in HA mode to display this field.

Cluster Members  The FortiGate units in the HA cluster. Information displayed about each member includes hostname, serial number, and if the unit is a primary (master) or subordinate (slave) unit in the cluster. See “HA” on page 135.
The FortiGate unit must be operating in HA mode with virtual domains not enabled to display this field.

Virtual Cluster 1  The role of each FortiGate unit in virtual cluster 1.
See “HA” on page 135.
The FortiGate unit must be operating in HA mode with virtual domains enabled to display these fields.

Virtual Cluster 2  The role of each FortiGate unit in virtual cluster 2.
See “HA” on page 135.
The FortiGate unit must be operating in HA mode with virtual domains enabled to display these fields.

Firmware Version  The version of the firmware installed on the current FortiGate unit.
Select Update to change the firmware.
See “Upgrading to a new firmware version” on page 59.

FortiClient Version  The currently loaded version of FortiClient. Select Update to upload a new FortiClient software image to this FortiGate unit from your management computer.
This is available only on FortiGate models that provide a portal from which hosts can download FortiClient software.

Operation Mode  The operating mode of the current FortiGate unit. Except for model 224B in switch view, a FortiGate unit can operate in NAT mode or Transparent mode. Select Change to switch between NAT and Transparent mode. See “Changing operation mode” on page 159.
If virtual domains are enabled, this field shows the operating mode of the current virtual domain. A virtual domain can be operating in either NAT mode or Transparent mode.
This field may not be displayed on your model.
Virtual Domain  The status of virtual domains on your FortiGate unit. Select enable or disable to change the status of virtual domains. Multiple VDOM operation is not available on a FortiGate-224B unit in switch view. If you change the state of virtual domains, your session will be terminated and you will need to login. For more information see “Using virtual domains” on page 71.

Current Administrators  The number of administrators currently logged into the FortiGate unit. Select Details to view more information about each administrator that is logged. The additional information includes user name, type of connection, IP address they are connecting from, and when they logged in.

License Information
License information displays the status of your FortiGate support contract, and FortiGuard subscriptions. The FortiGate unit updates the license information status indicators automatically by connecting to the FortiGuard network. FortiGuard subscriptions status indicators are green for OK, grey if the FortiGate unit cannot connect to the FortiGuard network, and yellow if the license has expired.

Selecting any of the Configure options will take you to the maintenance page. For more information, see “System Maintenance” on page 179.

Figure 17: Example License Information

Support Contract  The support contract number and expiry date.
If Not Registered is displayed, select Register to register the unit.
If Renew is visible, you need to renew your support contract. Contact your local reseller.

FortiGuard Subscriptions

AntiVirus  The FortiGuard Antivirus license version, issue date and service status. If your license has expired you can select Renew two renew the license.

AV Definitions  The current installed version of the FortiGuard Antivirus Definitions. To update the definitions manually, select Update. For more information, see “To update FortiGuard AV Definitions manually” on page 62.

Intrusion Protection  The FortiGuard intrusion protection license version, issue date and service status. If your license has expired you can select Renew two renew the license.

IPS Definitions  The current installed version of the Intrusion Prevention System (IPS) attack definitions. To update the definitions manually, select Update. For more information, see “To update FortiGuard IPS Definitions manually” on page 62.
There are commands in FortiOS that are only accessible from the CLI. Generally to use the CLI you connect via telnet or SSH using a 3rd party program.

The System Status page includes a fully functional CLI console. To use the console, click on it and you are automatically logged in as the account you are currently using in the GUI. The CLI console default view cannot be resized or moved. You can cut (CTRL-C) and paste (CTRL-V) text from the CLI console.

**Figure 18: CLI Console**

The two controls on the CLI console window are the customize icon, and the Detach control.

The Detach control moves the CLI console into its own window that is free to resize or be repositioned on your screen. The two controls on the detached CLI console are Customize and Attach. Customize has been explained. Attach simply puts the CLI console back in place on the System Status page.

The edit icon allows you to change the look of the console using fonts and colors for the text and background.
Status page

Figure 19: Customize CLI Console window

Preview  See how your changes will appear on the CLI console.
Text  Select this control, then choose a color from the color matrix to the right to change the color of the text in the CLI console.
Background  Select this control, then choose a color from the color matrix to the right to change the color of the background in the CLI console.
Use external command input box  Select to allow external input.
Console buffer length  Select the number of lines the console buffer keeps in memory. Valid numbers are from 20 to 9999.
Font  Select a font from the list.
Size  Select the size of the font. The default size is 10.
Reset defaults  Select to return to the default settings, discarding any changes.
OK  Select to save your changes and return to the CLI console.
Cancel  Select to discard your change and return to the CLI console.

System Resources

Any System Resources that are not displayed on the status page can be viewed as a graph by selecting the History icon.

Figure 20: Example System Resources

History
**History icon**  View a graphical representation of the last minute of CPU, memory, sessions, and network usage. This page also shows the virus and intrusion detections over the last 20 hours. For more information see "Viewing operational history" on page 61.

**CPU Usage**  The current CPU status displayed as a dial gauge and as a percentage.
The web-based manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.

**Memory Usage**  The current memory status displayed as a dial gauge and as a percentage.
The web-based manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.

**FortiAnalyzer Disk Quota**  The current status of the FortiAnalyzer disk quota used for the FortiGate unit displayed as a pie chart and a percentage.
This is available only if you have configured logging to a FortiAnalyzer unit.

---

### Unit Operation

An illustration of the FortiGate unit front panel shows the status of the unit ethernet network interfaces. If a network interface is shaded green, that interface is connected. Pause the mouse pointer over the interface to view the name, IP address, netmask and current status of the interface.

If you select Reboot or ShutDown a window opens allowing you to enter the reason for the system event. Your reason will be added to the Disk Event Log. Disk logging will need to be enabled in the CLI. Event Logging and Admin Events need to be enabled. For more information on Event Logging, see “Event log” on page 482.

**Figure 21: Example FortiGate-800 interface status (with no FortiAnalyzer)**
INT / EXT / DMZ / HA / 1 / 2 / 3 / 4

The ethernet network interfaces on the FortiGate unit. The names and number of these interfaces vary with your unit. The icon below the interface name indicates its status by its color. Green indicates the interface is connected. Grey indicates there is no connection.

For more information about the configuration and status of an interface, pause the mouse over the icon for that interface. The full name of the interface, the alias if one is configured, the IP address and netmask, the status of the link, the speed of the interface, and the number of sent and received packets is displayed.

If your FortiGate unit supports ASM modules and if you have installed an ASM module containing interfaces (for example, the FortiGate-ASM-FB4 contains 4 interfaces) these interfaces are added to the interface status display. The interfaces are named AMC/1, AMC/2, and so on.

FortiAnalyzer

The icon on the link between the FortiGate unit graphic and the FortiAnalyzer graphic indicates the status of their connection. An ‘X’ on a red icon indicates there is no connection. A check mark on a green icon indicates there is communication between the two units.

Select the FortiAnalyzer graphic to configure FortiAnalyzer logging on your FortiGate unit. See “Log&Report” on page 469.

Reboot

Select to shutdown and restart the FortiGate unit. You will be prompted to enter a reason for the reboot that will be entered into the logs.

Shutdown

Select to shutdown the FortiGate unit. You will be prompted for confirmation, and also prompted to enter a reason for the shutdown that will be entered into the logs.

Reset

Select to reset the FortiGate unit to factory default settings. You will be prompted for confirmation.

Alert Message Console

Alert messages help you track changes to your FortiGate unit. The following types of messages can appear in the Alert Message Console:

**Figure 22: Example Alert Message Console**

<table>
<thead>
<tr>
<th>Alert Message Console</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006-06-10 00:20:15 System restart</td>
<td></td>
</tr>
<tr>
<td>2006-06-15 00:24:00 Firmware upgraded by admin</td>
<td></td>
</tr>
<tr>
<td>2006-06-15 00:25:50 Lost the connection to FortiAnalyzer (FLG4002F0460600001)</td>
<td></td>
</tr>
<tr>
<td>2006-06-14 14:49:38 Found a new FortiAnalyzer (FLo000200460600001)</td>
<td></td>
</tr>
<tr>
<td>2006-06-14 14:49:38 Lost the connection to FortiAnalyzer (FLG4002F0460600001)</td>
<td></td>
</tr>
</tbody>
</table>

**System restart**
The system restarted. The restart could be due to operator action or power off/on cycling.

**Firmware upgraded by**

The named administrator upgraded the firmware to a more recent version on either the active or non-active partition.

**<admin_name>**

**Firmware downgraded by**

The named administrator downgraded the firmware to an older version on either the active or non-active partition.
Each message shows the date and time that it was posted. If there is insufficient space for all of the messages, select All to view the entire list in a new window.

Selecting Edit brings up Custom Alert Display options that offers the following customizations for your alert message display. The options are to not display:

- system restart messages
- firmware upgrade and downgrade messages
- conserve mode messages

To clear alert messages, select All and then select Clear Alert Messages at the top of the new window. This will delete all current alert messages from your FortiGate unit.

**Statistics**

The statistics section of the status page is designed to allow you to see at a glance what is happening on your FortiGate unit with regards to network traffic and protection.

You can quickly see the amount and type of traffic as well as any attack attempts on your system. To investigate an area that draws your attention, simply select Details for a detailed list of the most recent activity.

The information displayed in the statistics section is saved in log files that can be saved to a FortiAnalyzer unit, saved locally or backed up to an external source. You can use this data to see trends in network activity or attacks over time and deal with it accordingly.

In VDOM mode, statistics can only be viewed on the System Status page under Global Configuration. VDOMs do not have System Status pages. Content Archive and Attack Log Statistics on the System Status page only include logs from the root VDOM. Non-root VDOM statistics cannot be viewed on this page.

For detailed procedures involving the statistics list, see “Viewing Statistics” on page 63.

**Figure 23: Example Statistics**

```
<table>
<thead>
<tr>
<th>Sessions</th>
<th>17 current sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Archive</td>
<td></td>
</tr>
<tr>
<td>HTTP 71 URLs visited</td>
<td></td>
</tr>
<tr>
<td>HTTPS 23 URLs visited</td>
<td></td>
</tr>
<tr>
<td>Email 65 emails sent</td>
<td></td>
</tr>
<tr>
<td>32 emails received</td>
<td></td>
</tr>
<tr>
<td>FTP 0 URLs visited</td>
<td></td>
</tr>
<tr>
<td>0 files uploaded</td>
<td></td>
</tr>
<tr>
<td>0 files downloaded</td>
<td></td>
</tr>
<tr>
<td>SSH 0 file transfers</td>
<td></td>
</tr>
<tr>
<td>0 chat sessions</td>
<td></td>
</tr>
<tr>
<td>0 messages</td>
<td></td>
</tr>
<tr>
<td>Attack Log</td>
<td></td>
</tr>
<tr>
<td>AV 0 viruses caught</td>
<td></td>
</tr>
<tr>
<td>IPS 0 attacks blocked</td>
<td></td>
</tr>
<tr>
<td>Spam 0 spam messages detected</td>
<td></td>
</tr>
<tr>
<td>Web 0 URLs blocked</td>
<td></td>
</tr>
</tbody>
</table>

Reset
```
Changing system information

FortiGate administrators whose access profiles permit write access to system configuration can change the system time, host name and the operation mode for the VDOM.

Configuring system time

1. Go to **System > Status**.
2. In the System Information section, select Change on the System Time line.
3. Select the time zone and then either set the date and time manually or configure synchronization with an NTP server.

Figure 24: Time Settings

Since

The date and time when the counts were reset.

Counts are reset when the FortiGate unit reboots or when you select to the reset icon.

Reset Icon

Reset the Archive and Attack Log counts to zero.

Sessions

The number of communications sessions being processed by the FortiGate unit. Select Details for detailed information. See “Viewing the session list” on page 63.

Content Archive

A summary of the HTTP, email, FTP, and IM/P2P traffic that has passed through the FortiGate unit. The Details pages list the last 64 items of the selected type and provide links to the FortiAnalyzer unit where the archived traffic is stored. If logging to a FortiAnalyzer unit is not configured, the Details pages provide a link to the Log & Report > Log Config > Log Settings page.

Attack Log

A summary of viruses, attacks, spam email messages and URLs the unit has intercepted. The Details pages list the most recent 10 items, providing the time, source, destination and other information.
Changing the FortiGate unit host name

The FortiGate host name appears on the Status page and in the FortiGate CLI prompt. The host name is also used as the SNMP system name. For information about SNMP, see “SNMP” on page 143.

The default host name is the FortiGate unit serial number. For example FGT8002805030003 would be a FortiGate-800 unit.

Administrators whose access profiles permit system configuration write access can change the FortiGate unit host name.

To change the FortiGate unit host name

1. Go to System > Status.
2. In the Host Name field of the System Information section, select Change.
3. In the New Name field, type a new host name.
4. Select OK.

The new host name is displayed in the Host Name field, and in the CLI prompt, and is added to the SNMP System Name.

Changing the FortiGate firmware

FortiGate administrators whose access profiles permit maintenance read and write access can change the FortiGate firmware.

Firmware changes either upgrade to a newer version or revert to an earlier version. Follow the appropriate procedure for the firmware change you want to perform:

• Upgrading to a new firmware version
• Reverting to a previous firmware version

Upgrading to a new firmware version

Use the following procedure to upgrade the FortiGate unit to a newer firmware version.

Note: Installing firmware replaces the current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After you install new firmware, use the procedure “To update antivirus and attack definitions” on page 194 to make sure that antivirus and attack definitions are up to date.
Changing the FortiGate firmware

To upgrade the firmware using the web-based manager

1. Copy the firmware image file to your management computer.
2. Log into the web-based manager as the super admin, or an administrator account that has system configuration read and write privileges.
3. Go to **System > Status**.
4. In the System Information section, select Update on the Firmware Version line.
5. Type the path and filename of the firmware image file, or select Browse and locate the file.
6. Select OK.

   The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, closes all sessions, restarts, and displays the FortiGate login. This process takes a few minutes.
7. Log into the web-based manager.
8. Go to **System > Status** and check the Firmware Version to confirm that the firmware upgrade is successfully installed.
9. Update antivirus and attack definitions. For information about updating antivirus and attack definitions, see “FortiGuard Center” on page 186.

Reverting to a previous firmware version

Use the following procedure to revert your FortiGate unit to a previous firmware version. This also reverts the FortiGate unit to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages. Back up your FortiGate unit configuration to preserve this information. For information, see “Maintenance System Configuration” on page 179.

If you are reverting to a previous FortiOS™ version (for example, reverting from FortiOS v3.0 to FortiOS v2.8), you might not be able to restore the previous configuration from the backup configuration file.

**Note:** Installing firmware replaces the current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After you install new firmware, use the procedure “To update antivirus and attack definitions” on page 194 to make sure that antivirus and attack definitions are up to date.

To revert to a previous firmware version using the web-based manager

1. Copy the firmware image file to the management computer.
2. Log into the web-based manager as the super admin, or an administrator account that has system configuration read and write privileges.
3. Go to **System > Status**.
4. In the System Information section, select Update on the Firmware Version line.
5. Type the path and filename of the firmware image file, or select Browse and locate the file.
6. Select OK.

   The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.
7 Log into the web-based manager.
8 Go to **System > Status** and check the Firmware Version to confirm that the firmware is successfully installed.
9 Restore your configuration.
   For information about restoring your configuration, see “Maintenance System Configuration” on page 179.
10 Update antivirus and attack definitions.
   For information about antivirus and attack definitions, see “To update antivirus and attack definitions” on page 194.

**Viewing operational history**

The System Resource History page displays six graphs representing system resources and protection activity.

1 Go to **System > Status**.
2 Select History in the upper right corner of the System Resources section.

**Figure 25: Sample system resources history**

<table>
<thead>
<tr>
<th>Time Interval</th>
<th>Select the time interval that the graphs show.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Usage History</td>
<td>CPU usage for the preceding interval.</td>
</tr>
<tr>
<td>Memory Usage History</td>
<td>Memory usage for the preceding interval.</td>
</tr>
<tr>
<td>Session History</td>
<td>Number of sessions over the preceding interval.</td>
</tr>
<tr>
<td>Network Utilization History</td>
<td>Network utilization for the preceding interval.</td>
</tr>
<tr>
<td>Virus History</td>
<td>Number of Viruses detected over the preceding interval.</td>
</tr>
<tr>
<td>Intrusion History</td>
<td>Number of intrusion attempts detected over the preceding interval.</td>
</tr>
</tbody>
</table>
Manually updating FortiGuard definitions

You can update your FortiGuard - AV and FortiGuard - Intrusion Protection definitions at any time from the License Information section of the System Status page.

**Note:** For information about configuring the FortiGate unit for automatic AV and automatic IPS (attack) definitions updates, see “FortiGuard Center” on page 186.

**To update FortiGuard AV Definitions manually**

1. Download the latest AV definitions update file from Fortinet and copy it to the computer that you use to connect to the web-based manager.
2. Start the web-based manager and go to **System > Status**.
3. In the License Information section, in the AV Definitions field of the FortiGuard Subscriptions, select Update.
   
   The Anti-Virus Definitions Update dialog box appears.
4. In the Update File field, type the path and filename for the AV definitions update file, or select Browse and locate the AV definitions update file.
5. Select OK to copy the AV definitions update file to the FortiGate unit.
   
   The FortiGate unit updates the AV definitions. This takes about 1 minute.
6. Go to **System > Status** to confirm that the FortiGuard - AV Definitions version information has updated.

**To update FortiGuard IPS Definitions manually**

1. Download the latest attack definitions update file from Fortinet and copy it to the computer that you use to connect to the web-based manager.
2. Start the web-based manager and go to **System > Status**.
3. In the License Information section, in the IPS Definitions field of the FortiGuard Subscriptions, select Update.
   
   The Intrusion Prevention System Definitions Update dialog box appears.
4. In the Update File field, type the path and filename for the attack definitions update file, or select Browse and locate the attack definitions update file.
5. Select OK to copy the attack definitions update file to the FortiGate unit.
   
   The FortiGate unit updates the attack definitions. This takes about 1 minute.
6. Go to **System > Status** to confirm that the IPS Definitions version information has updated.
Viewing Statistics

The System Status Statistics provide information about sessions, content archiving and network protection activity.

Viewing the session list

The session list displays information about the current communications sessions on the FortiGate unit.

To view the session list

1. Go to System > Status.
2. In the Statistics section, select Details on the Sessions line.

Figure 26: Session list

<table>
<thead>
<tr>
<th>#</th>
<th>Protocol</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Policy ID</th>
<th>Expiry (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>tcp</td>
<td>172.20.120.16</td>
<td>9966</td>
<td>172.20.120.448</td>
<td>441</td>
<td>3000</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>tcp</td>
<td>172.20.120.48</td>
<td>2000</td>
<td>172.30.10.0.20</td>
<td>178</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>tcp</td>
<td>172.20.120.48</td>
<td>1988</td>
<td>172.20.120.120</td>
<td>514</td>
<td>3995</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>udp</td>
<td>172.0.0.1</td>
<td>1022</td>
<td>172.0.0.1</td>
<td>92</td>
<td>182</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>tcp</td>
<td>172.20.120.48</td>
<td>2000</td>
<td>192.168.20.10</td>
<td>174</td>
<td>104</td>
<td></td>
</tr>
</tbody>
</table>

Virtual Domain Select a virtual domain to list the sessions being processed by that virtual domain. Select All to view sessions being processed by all virtual domains. This is only available if multiple virtual domains are enabled.

Refresh Update the session list.
Page up View previous page in the session list.
Page down View the next page in the session list.
Line Enter the line number of the session to start the displayed session list. For example if there are 5 sessions and you enter 3, only the sessions numbered 3, 4 and 5 will be displayed. The number following the ‘/’ is the number of active sessions on the FortiGate unit.
Clear All Filters Select to reset any display filters that may have been set.
Filter Icon The icon at the top of all columns except #, and Expiry. When selected it brings up the Edit Filter dialog allowing you to set the display filters by column. See “Adding filters to web-based manager lists” on page 43.
Protocol The service protocol of the connection, for example, udp, tcp, or icmp.
Source Address The source IP address of the connection.
Source Port The source port of the connection.
Destination Address The destination IP address of the connection.
Destination Port The destination port of the connection.
Policy ID The number of the firewall policy allowing this session or blank if the session involves only one FortiGate interface (admin session, for example).
Expiry (sec) The time, in seconds, before the connection expires.
Delete icon Stop an active communication session. Your access profile must include read and write access to System Configuration.
Viewing the Content Archive Information

From the Statistics section of the System Status page, you can view statistics about HTTP, email, FTP and IM traffic through the FortiGate unit. You can select the Details link beside each traffic type to view more information.

You can select Reset on the header of the Statistics section to clear the content archive and attack log information and reset the counts to zero.

Viewing archived HTTP content information

1. Go to System > Status.
2. In the Content Archive section, select Details for HTTP.

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>From</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005-04-07 02:06:05</td>
<td>172.20.320.51</td>
<td>10.10.10.10/doc-lab/</td>
</tr>
<tr>
<td>2005-04-07 02:06:06</td>
<td>172.20.320.51</td>
<td>10.10.10.10/doc-lab/content1.html</td>
</tr>
<tr>
<td>2005-04-07 02:06:06</td>
<td>172.20.320.51</td>
<td>10.10.10.10/doc-lab/oftware.html</td>
</tr>
<tr>
<td>2005-04-07 02:06:06</td>
<td>172.20.320.51</td>
<td>10.10.10.10/yavision.doc</td>
</tr>
<tr>
<td>2005-04-07 02:06:09</td>
<td>172.20.320.51</td>
<td>10.10.10.10/doc-lab/HCOPD.html</td>
</tr>
<tr>
<td>2005-04-07 02:06:10</td>
<td>172.20.320.51</td>
<td>10.10.10.10/doc-lab/NADUS.html</td>
</tr>
<tr>
<td>2005-04-07 02:06:11</td>
<td>172.20.320.51</td>
<td>10.10.10.10/doc-lab/ference.html</td>
</tr>
<tr>
<td>2005-04-07 02:06:16</td>
<td>172.20.320.51</td>
<td>10.10.10.10/doc-lab/FO-defect-connet.html</td>
</tr>
<tr>
<td>2005-04-07 02:06:14</td>
<td>172.20.320.51</td>
<td>10.10.10.10/doc-lab/simplenet.html</td>
</tr>
<tr>
<td>2005-04-07 02:06:14</td>
<td>172.20.320.51</td>
<td>10.10.10.10/doc-lab/passert-4.html</td>
</tr>
</tbody>
</table>

Long-term archival of content information is available from the FortiLog GUI.

Viewing archived Email content information

1. Go to System > Status.
2. In the Content Archive section, select Details for Email.

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>From</th>
<th>To</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005-06-03 10:03:08</td>
<td><a href="mailto:juser@example.com">juser@example.com</a></td>
<td><a href="mailto:techdoc@fortinet.com">techdoc@fortinet.com</a></td>
<td>Great documentation, great!</td>
</tr>
<tr>
<td>2005-04-07 10:30:06</td>
<td><a href="mailto:techdoc@fortinet.com">techdoc@fortinet.com</a></td>
<td><a href="mailto:juser@example.com">juser@example.com</a></td>
<td>Thanks for the feedback</td>
</tr>
</tbody>
</table>

Long-term archival of content information is available from the FortiLog GUI.

Date and Time: The time when the email was accessed.
From: The IP address from which the URL was accessed.
URL: The URL that was accessed.

Viewing archived IM content information

1. Go to System > Status.
2. In the Content Archive section, select Details for IM.

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>From</th>
<th>To</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005-08-07 10:10:10</td>
<td><a href="mailto:juser@example.com">juser@example.com</a></td>
<td><a href="mailto:juser@example.com">juser@example.com</a></td>
<td>Hello, this is a test message!</td>
</tr>
</tbody>
</table>

Long-term archival of content information is available from the FortiLog GUI.

Date and Time: The time when the email was accessed.
From: The sender’s email address.
To: The recipient’s email address.
Subject: The subject line of the email.
Viewing archived FTP content information

1  Go to System > Status.
2  In the Content Archive section, select Details for FTP.

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Destination</th>
<th>User</th>
<th>Downloads</th>
<th>Uploads</th>
</tr>
</thead>
<tbody>
<tr>
<td>2065-04-07 01:19:19</td>
<td>10.10.10.10</td>
<td>techdec</td>
<td>root/bin/shell/www/wall/ policy / example.png</td>
<td>net/ftplog_policy_example.png</td>
</tr>
<tr>
<td>2065-04-07 01:19:19</td>
<td>10.10.10.10</td>
<td>techdec</td>
<td>net/ftplog_policy_example.png</td>
<td>net/ftplog_policy_example.png</td>
</tr>
<tr>
<td>2065-04-07 01:19:19</td>
<td>10.10.10.10</td>
<td>techdec</td>
<td>net/ftplog_policy_example.png</td>
<td>net/ftplog_policy_example.png</td>
</tr>
</tbody>
</table>

Viewing archived IM content information

1  Go to System > Status.
2  In the Content Archive section, select Details for IM.

<table>
<thead>
<tr>
<th>Date / Time</th>
<th>Protocol</th>
<th>Kind</th>
<th>Local</th>
<th>Remote</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>2065-04-07 01:19:19</td>
<td>IM</td>
<td>IM</td>
<td>IM</td>
<td>IM</td>
<td>IM</td>
</tr>
</tbody>
</table>

Viewing the Attack Log

From the Statistics section of the System Status page, you can view statistics about the network attacks that the FortiGate unit has stopped. You can select the Details link beside each attack type to view more information.

You can select Reset on the header of the Statistics section to clear the content archive and attack log information and reset the counts to zero.

Viewing viruses caught

1  Go to System > Status.
2  In the Attack Log section, select Details for AV.

<table>
<thead>
<tr>
<th>Date and Time</th>
<th>From</th>
</tr>
</thead>
<tbody>
<tr>
<td>The time when the virus was detected.</td>
<td>The sender's email address or IP address.</td>
</tr>
</tbody>
</table>
Viewing Statistics

Viewing attacks blocked

1. Go to **System > Status**.
2. In the Attack Log section, select Details for IPS.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and Time</td>
<td>The time that the attack was detected.</td>
</tr>
<tr>
<td>From</td>
<td>The source of the attack.</td>
</tr>
<tr>
<td>To</td>
<td>The target host of the attack.</td>
</tr>
<tr>
<td>Service</td>
<td>The service type.</td>
</tr>
<tr>
<td>Attack</td>
<td>The type of attack that was detected and prevented.</td>
</tr>
</tbody>
</table>

Viewing spam email detected

1. Go to **System > Status**.
2. In the Attack Log section, select Details for Spam.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and Time</td>
<td>The time that the spam was detected.</td>
</tr>
<tr>
<td>From-&gt;To IP</td>
<td>The sender and intended recipient IP addresses.</td>
</tr>
<tr>
<td>From-&gt;To Email Accounts</td>
<td>The sender and intended recipient email addresses.</td>
</tr>
<tr>
<td>Service</td>
<td>The service type, such as SMTP, POP or IMAP.</td>
</tr>
<tr>
<td>SPAM Type</td>
<td>The type of spam that was detected.</td>
</tr>
</tbody>
</table>

Viewing URLs blocked

1. Go to **System > Status**.
2. In the Attack Log section, select Details for Web.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and Time</td>
<td>The time that the attempt to access the URL was detected.</td>
</tr>
<tr>
<td>From</td>
<td>The host that attempted to view the URL.</td>
</tr>
<tr>
<td>URL Blocked</td>
<td>The URL that was blocked.</td>
</tr>
</tbody>
</table>
**Topology viewer**

The Topology viewer provides a way to diagram and document the networks connected to your FortiGate unit. It is available on all FortiGate units except models numbered 50 and 60.

**The Topology Viewer window**

The Topology window consists of a large “canvas” upon which you can draw a network topology diagram for your FortiGate installation.

**Figure 27: Topology viewer**

```
View/edit controls  Text object  Subnet object
```

```
Default route to Internet
```

```
Office
```

```
Servers
```

```
Main viewport
```

```
Viewport control
```

**Main viewport and viewport control**

The main viewport is a portion of the total drawing area. It corresponds to the dark rectangle in the viewport control. You can drag the main viewport rectangle within the viewport control to determine which part of the drawing area the main viewport displays. The “+” and “-” buttons in the viewport control have the same function as the Zoom in and Zoom out edit controls.

The FortiGate unit is a permanent part of the topology diagram. You can move it, but not delete it.
View and edit controls

The toolbar at the top left of the Topology page shows controls for viewing and editing topology diagrams.

Table 3: View/Edit controls for Topology Viewer

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Refresh]</td>
<td>Refresh the displayed diagram.</td>
</tr>
<tr>
<td>![Zoom In]</td>
<td>Zoom in. Select to show a smaller portion of the drawing area in the main viewport, making objects appear larger.</td>
</tr>
<tr>
<td>![Zoom Out]</td>
<td>Zoom out. Select to show a larger portion of the drawing area in the main viewport, making objects appear smaller.</td>
</tr>
<tr>
<td>![Edit]</td>
<td>Edit. Select this button to begin editing the diagram. The toolbar expands to show the editing controls described below:</td>
</tr>
<tr>
<td>![Save]</td>
<td>Save any changes made to the diagram. You need to save changes before you switch to any other page in the web-based manager.</td>
</tr>
<tr>
<td>![Add Subnet]</td>
<td>Add a subnet object to the diagram. The subnet object is based on the firewall address you select and is connected by a line to the interface associated with that address. See “Adding a subnet object” on page 69.</td>
</tr>
<tr>
<td>![Insert Text]</td>
<td>Insert Text. Select this control and then click on the diagram where you want to place the text object. Type the text and then click outside the text box.</td>
</tr>
<tr>
<td>![Delete]</td>
<td>Delete. Select the object to delete and then select this control or press the Delete key.</td>
</tr>
<tr>
<td>![Customize]</td>
<td>Customize. Select to change the colors and the thickness of lines used in the drawing. See “Customizing the topology diagram” on page 70.</td>
</tr>
<tr>
<td>![Drag]</td>
<td>Drag. Select this control and then drag objects in the diagram to arrange them as needed.</td>
</tr>
<tr>
<td>![Scroll]</td>
<td>Scroll. Select this control and then drag the drawing background to move the main viewport within the drawing area. This has the same effect as moving the main viewport rectangle in the viewport control.</td>
</tr>
<tr>
<td>![Select]</td>
<td>Select. Select this control and then drag the mouse pointer to create a selection rectangle. Objects in the rectangle are selected when you release the mouse button.</td>
</tr>
<tr>
<td>![Exit]</td>
<td>Exit. Select this button to finish editing the diagram. The toolbar contracts to show only the Refresh and Zoom controls.</td>
</tr>
</tbody>
</table>
Adding a subnet object

While editing the topology diagram, you can select the Add Subnet control to define a subnet object. The object is drawn and connected by a line to the interface associated with the address.

**Figure 28: Adding an existing subnet to the topology diagram**

```
<table>
<thead>
<tr>
<th>System Topology Add Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select from existing address/group</td>
</tr>
<tr>
<td>Address Name: ----------------- Addresses: --Please Choose--</td>
</tr>
<tr>
<td>Connect to interface: --Please Choose--</td>
</tr>
<tr>
<td>New addresses</td>
</tr>
</tbody>
</table>

```

**Figure 29: Adding a new subnet to the topology diagram**

```
<table>
<thead>
<tr>
<th>System Topology Add Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select from existing address/group</td>
</tr>
<tr>
<td>New addresses</td>
</tr>
<tr>
<td>Address Name:</td>
</tr>
<tr>
<td>Subnet/IP Range: 0.0.0.0/0.0.0.0</td>
</tr>
<tr>
<td>Connect to interface: --Please Choose--</td>
</tr>
</tbody>
</table>

```

**Select from existing address/group**

Create a subnet object based on an existing firewall address. The object has the name of the firewall address and is connected by a line to the interface associated with that address. For more information about firewall addresses, see "Firewall Address" on page 289.

**Address Name**

Enter a name to identify the firewall address. Addresses, address groups, and virtual IPs must have unique names to avoid confusion in firewall policies.

**Connect to interface**

If the field displays "Please choose", select the interface or zone to associate with this address. If the field already displays a name, changing the setting will change the interface or zone associated with this existing address.

**New addresses**

Create a new firewall address and add a subnet object based on that address to the topology diagram. The address is associated with the interface you choose.

**Address Name**

Enter a name to identify the firewall address. Addresses, address groups, and virtual IPs must have unique names to avoid confusion in firewall policies.

**Type**

Select the type of address: Subnet/IP Range or FQDN.

**Subnet / IP Range**

If Type is Subnet/IP Range, enter firewall IP address, forward slash, subnet mask, or enter IP start address, hyphen, IP end address.

**FQDN**

If Type is FQDN, enter the fully qualified domain name.

**Connect to interface**

Select the interface or zone to associate with this address.
Customizing the topology diagram

Select the Customize button to open the Topology Customization window. Modify the settings as needed and select OK when you are finished.

Figure 30: Topology Customization window

- **Preview**: A simulated topology diagram showing the effect of the selected appearance options.
- **Canvas Size**: The size of the drawing in pixels.
- **Resize to Image**: If you selected an image as Background, resize the diagram to fit within the image.
- **Background**: One of:
  - Solid - a solid color selected in Background Color
  - U.S. Map - a map of the United States.
  - World Map - a map of the world.
  - Upload My Image - upload the image from Image Path.
- **Background Color**: Select the color of the diagram background.
- **Image path**: If you selected Upload My Image for Background, enter the path to your image, or use the Browse button to find it.
- **Exterior Color**: Select the color of the border region outside your diagram.
- **Line Color**: Select the color of connecting lines between subnet objects and interfaces.
- **Line Width**: Select the thickness of connecting lines.
- **Reset to Default**: Reset all settings to default.
Using virtual domains

This section describes how to use virtual domains to operate your FortiGate unit as multiple virtual units, providing separate firewall and routing services to multiple networks.

This section describes:
- Virtual domains
- Enabling VDOMs
- Configuring VDOMs and global settings

Virtual domains

Virtual domains (VDOMs) enable a FortiGate unit to function as multiple independent units. A single FortiGate unit is then flexible enough to serve multiple departments of an organization, separate organizations or be the basis for a service provider’s managed security service.

VDOMs provide separate security domains that allow separate zones, user authentication, firewall policies, routing, and VPN configurations. Using VDOMs can also simplify administration of complex configurations because you do not have to manage as many routes or firewall policies at one time. See “VDOM configuration settings” on page 72.

To configure and use VDOMs, you must enable virtual domain configuration. See “Enabling VDOMs” on page 74.

When you create and configure a VDOM, you must assign interfaces or VLAN subinterfaces to it. Optionally, you can assign an administrator account that can log in only to that VDOM. If the VDOM is created to serve an organization, this enables the organization to manage its configuration independently. The operating mode, NAT/Route or Transparent, is independently selectable for each VDOM.

When a packet enters a VDOM, it is confined to that VDOM. In a VDOM, you can create firewall policies for connections between VLAN subinterfaces or zones in the VDOM. Packets do not cross the virtual domain border internally. To travel between VDOMs a packet must pass through a firewall on a physical interface. The packet then arrives at another VDOM on a different interface where it must pass through another firewall before entering. Both VDOMs are on the same FortiGate unit. The one exception is if you configure inter-VDOM routing using CLI commands.

The remainder of FortiGate functionality is global. It applies to all VDOMs. This means that there is one intrusion prevention configuration, one antivirus configuration, one web filter configuration, and so on. As well, VDOMs share firmware versions, antivirus and attack databases. For a complete list of shared configuration settings, see “Global configuration settings” on page 73.
By default, your FortiGate unit supports a maximum of 10 VDOMs in any combination of NAT/Route and Transparent modes. For FortiGate models numbered 3000 and higher, you can purchase a license key to increase the maximum number of VDOMs to 25, 50, 100 or 250. For more information see “License” on page 199.

**Note:** The FortiGate-224B in switch view does not support VDOMs.

If virtual domain configuration is enabled and you log in as the default super admin, you can go to System > Status and look at Virtual Domain in the License Information section to see the maximum number of virtual domains supported on your FortiGate unit.

By default, each FortiGate unit has a VDOM named root. This VDOM includes all of the FortiGate physical interfaces, VLAN subinterfaces, zones, firewall policies, routing settings, and VPN settings.

Management systems such as SNMP, logging, alert email, FDN-based updates and NTP-based time setting use addresses and routing in the management VDOM to communicate with the network. They can connect only to network resources that communicate with the management virtual domain. The management VDOM is set to root by default, but can be changed. For more information see “Changing the Management VDOM” on page 77.

Once you add a VDOM you can configure it by adding VLAN subinterfaces, zones, firewall policies, routing settings, and VPN settings. You can also move physical interfaces from the root VDOM to other VDOMs and move VLAN subinterfaces from one VDOM to another. For more information on VLANs, see “VLAN overview” on page 107.

For more information on VDOMs, see the *FortiGate VLANs and VDOMs Guide*.

**VDOM configuration settings**

The following configuration settings are exclusively part of a virtual domain and are not shared between virtual domains. A regular administrator for the VDOM sees only these settings. The default super admin can also access these settings, but must first select which VDOM to configure.

- System settings
  - Zones
  - DHCP services
  - Operation mode (NAT/Route or Transparent)
  - Management IP (Transparent mode)
- Router configuration
- Firewall settings
  - Policies
  - Addresses
  - Service groups and custom services
  - Schedules
  - Virtual IPs
  - IP pools
  - Protection Profiles
• VPN configuration
  • IPSec
  • PPTP
  • SSL
• User settings
  • Users
  • User groups
  • RADIUS and LDAP servers
  • Microsoft Windows Active Directory servers
• P2P Statistics (view/reset)
• Logging configuration, log access and log reports

Global configuration settings

The following configuration settings affect all virtual domains. When virtual domains are enabled, only the default super admin can access global settings.

• System settings
  • Physical interfaces and VLAN subinterfaces
    (Each physical interface or VLAN subinterface belongs to only one VDOM. Each VDOM can use or configure only its own interfaces.)
  • DNS settings
  • Host name, System time, Firmware version (on System Status page)
  • Idle and authentication timeout
  • Web-based manager language
  • LCD panel PIN, where applicable
  • Dead gateway detection
  • HA configuration
  • SNMP configuration
  • Replacement messages
  • Administrators
    (Each administrator belongs to only one VDOM. Each VDOM can configure only its own administrators.)
  • Access profiles
  • FortiManager configuration
  • Configuration backup and restore
  • FDN update configuration
  • Bug reporting
• VPN certificates
• Antivirus configuration
• Intrusion Prevention configuration
• Web filter configuration
• Antispam configuration
• IM configuration
• Statistics
• User lists and policies
Enabling VDOMs

Using the default admin administration account, you can enable multiple VDOM operation on the FortiGate unit.

To enable virtual domains

1. Log in to the web-based manager as admin.
2. Go to System > Status.
3. In System Information, next to Virtual Domain select Enable.

The FortiGate unit logs you off. You can now log in again as admin.

When virtual domains are enabled, the web-based manager and the CLI are changed as follows:

- Global and per-VDOM configurations are separated.
- A new VDOM entry appears under System.
- Only the admin account can view or configure global options.
- The admin account can configure all VDOM configurations.
- The admin account can connect through any interface in the root VDOM or though any interface that belongs to a VDOM for which a regular administrator account has been assigned.
- A regular administrator account can configure only the VDOM to which it is assigned and can access the FortiGate unit only through an interface that belongs to that VDOM.

When virtual domains are enabled, you can see what the current virtual domain is by looking at the bottom left of the screen. It will say Current VDOM: followed by the name of the virtual domain.

Configuring VDOMs and global settings

When Virtual Domains are enabled, only the default super admin account can:

- configure global settings
- create or delete VDOMs
- configure multiple VDOMs
- assign interfaces to a VDOM
- assign an administrator to a VDOM

A VDOM is not useful unless it contains at least two physical interfaces or virtual subinterfaces for incoming and outgoing traffic. Only the super admin can assign interfaces or subinterfaces to VDOMs. A regular administrator account can create a VLAN subinterface on a physical interface within their own VDOM.

Only the super admin can configure a VDOM unless you create and assign a regular administrator to that VDOM. Only the super admin can assign an administrator to a VDOM. An administrator account whose access profile provides read and write access to Admin Users can create additional administrators in its own VDOM.
Working with VDOMs and global settings

When you log in as admin and virtual domains are enabled you are automatically in global configuration, as demonstrated by the VDOM option under System.

Select System > VDOM to work with virtual domains.

Figure 31: VDOM list

<table>
<thead>
<tr>
<th>Create New</th>
<th>Management</th>
<th>Delete</th>
<th>Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Operation Mode</td>
<td>Interfaces</td>
<td>Management Virtual Domain</td>
</tr>
<tr>
<td>Customer 1</td>
<td>Transparent</td>
<td>port 1</td>
<td>No</td>
</tr>
<tr>
<td>Customer 2</td>
<td>NAT</td>
<td>port 2</td>
<td>No</td>
</tr>
<tr>
<td>Customer 3-a</td>
<td>NAT</td>
<td>Office A</td>
<td>No</td>
</tr>
<tr>
<td>Customer 3-b</td>
<td>NAT</td>
<td>Office B</td>
<td>No</td>
</tr>
<tr>
<td>Customer 3-c</td>
<td>Transparent</td>
<td>Office C</td>
<td>No</td>
</tr>
<tr>
<td>ITS</td>
<td>NAT</td>
<td>dmz</td>
<td>No</td>
</tr>
<tr>
<td>Sales</td>
<td>NAT</td>
<td>port 4</td>
<td>No</td>
</tr>
<tr>
<td>root</td>
<td>NAT</td>
<td>external, be, internal, port 3</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Create New**
Select to add a new VDOM. Enter the new VDOM name and select OK.
The VDOM must not have the same name as an existing VDOM, VLAN or zone. The VDOM name can be a maximum of 11 characters long without spaces.

**Management**
Change the management VDOM to the selected VDOM. The management VDOM is indicated in brackets. The default management VDOM is root.
If more than one VDOM is selected when Set Management is selected, the VDOM appearing first in the table will be assigned as the management VDOM. For more information see "Changing the Management VDOM" on page 77.

**Delete**
Delete the selected VDOM.
You cannot delete the root VDOM.

**Switch**
Select to enter that VDOM.
You can see which VDOM you are currently in by looking at the left side of the screen at the bottom where the name of the VDOM is displayed. The global settings screen does not have any VDOM name in this location.

**Name**
The name of the VDOM.

**Operation Mode**
The VDOM operation mode, either NAT or Transparent.

**Interfaces**
The interfaces associated with this VDOM, including virtual interfaces.

**Management Virtual Domain**
Indicates which VDOM is the management domain. All non-management domains are indicated with a “no”.

Adding interfaces to a VDOM

A VDOM must contain at least two interfaces. These can be physical or virtual interfaces such as VLAN subinterfaces. By default, all physical interfaces are in the root virtual domain.

As of FortiOS v3.0 MR1, inter-VDOM routing enables you to communicate between VDOMs internally without using a physical interface. This feature is only configurable with the CLI. For information on configuring inter-VDOM interfaces, see the FortiGate CLI Reference and the FortiGate VLANs and VDOMs Guide.
Configuring VDOMs and global settings

VLAN subinterfaces often need to be in a different VDOM than their physical interface. To do this, the super admin must first create the VDOM, then create the VLAN subinterface, and assign it to the required VDOM.

System > Network > Interfaces is only in global settings, and is not available within any VDOM. For information on creating VLAN subinterfaces, see “Adding VLAN subinterfaces” on page 109.

Assigning an interface to a VDOM

The following procedure describes how to reassign an existing interface from one virtual domain to another. It assumes VDOMs are enabled and more than one VDOM exists.

You cannot delete a VDOM if it is used in any configurations, such as having an interface in that VDOM. You cannot remove an interface from a VDOM if the interface is included in any of the following configurations:

- DHCP server
- zone
- routing
- firewall policy
- IP pool
- proxy arp (only accessible through the CLI)

Delete these items or modify them to remove the interface before proceeding.

Note: An interface or subinterface is available for reassigning or removing once the delete icon is displayed. Until then, the interface is used in a configuration somewhere.

To assign an interface to a VDOM

1. Log in as admin.
2. Go to System > Network > Interface.
3. Select Edit for the interface that you want to reassign.
4. Select the new Virtual Domain for the interface.
5. Configure other settings as required and select OK. For more information on the other interfaces settings see “Interface settings” on page 83.

The interface is assigned to the VDOM. Existing firewall IP pools and virtual IP addresses for this interface are deleted. You should manually delete any routes that include this interface, and create new routes for this interface in the new VDOM. Otherwise your network traffic will not be properly routed.

Assigning an administrator to a VDOM

If you are creating a VDOM to serve an organization that will be administering its own resources, you need to create an administrator account for that VDOM.

A VDOM admin can change configuration settings within that VDOM but cannot make changes that affect other VDOMs on the FortiGate unit.
A regular administrator assigned to a VDOM can log in to the web-based manager or the CLI only on interfaces that belong to that VDOM. The super admin can connect to the web-based manager or CLI through any interface on the FortiGate unit that permits management access. Only the super admin or a regular administrator of the root domain can log in by connecting to the console interface.

To assign an administrator to a VDOM

1. Log in as the super admin. Virtual domains must be enabled.
2. Go to System > Admin > Administrators.
3. Create and/or configure the new administrator account as required. For detailed information about configuring an administrator account, see "Configuring an administrator account" on page 166.
4. While configuring this admin account, select the VDOM this administrator manages from the Virtual Domain list.
5. Select Apply.

Changing the Management VDOM

The management VDOM on your FortiGate unit is where some default types of traffic originate. These types of traffic include:

- SNMP
- logging
- alert email
- FDN-based updates
- NTP-based time setting

Before you change the management VDOM, ensure virtual domains are enabled. Only one VDOM can be the management VDOM at any given time. If you accidently select more than one VDOM when setting the management VDOM, the VDOM closest to the top of the list will become the management VDOM.

Note: You cannot change the management VDOM if any administrators are using RADIUS authentication.

To change the management VDOM

1. Go to System > VDOM.
2. Select the VDOM that will be the new management VDOM.
3. Select Management to apply the changes. Management traffic will now originate from the new management VDOM.
System Network

This section describes how to configure your FortiGate unit to operate in your network. Basic network settings include configuring FortiGate interfaces and DNS settings. More advanced configuration includes adding VLAN subinterfaces and zones to the FortiGate network configuration.

This section describes:
- Interface
- Zone
- Network Options
- Routing table (Transparent Mode)
- Configuring the modem interface
- VLAN overview
- VLANs in NAT/Route mode
- VLANs in Transparent mode
- FortiGate IPv6 support

Note: Where you can enter both an IP address and a netmask in the same field, you can use the short form of the netmask. For example, 192.168.1.100/255.255.255.0 can also be entered as 192.168.1.100/24.

Interface

In NAT/Route mode, go to System > Network > Interface to configure FortiGate interfaces. You can
- modify the configuration of a physical interface
- add and configure VLAN subinterfaces
- configure an ADSL interface
- aggregate several physical interfaces into an IEEE 802.3ad interface (models 800 and higher only)
- combine physical interfaces into a redundant interface
- add wireless interfaces (FortiWiFi-50B, 60A, 60AM, and 60B units) and SSIDs (see “Adding a wireless interface to a FortiWiFi-50B, 60A, 60AM, and 60B unit” on page 122)
- view loopback and inter-VDOM link interfaces

Note: Unless stated otherwise, in this section the term interface can refer to a physical FortiGate interface or to a FortiGate VLAN subinterface.

For information about VLANs, see “FortiGate units and VLANs” on page 107.
Create New
Select Create New to create a VLAN subinterface. On models 800 and higher, you can also create an IEEE 802.3ad aggregated interface.

Switch Mode
Select to change between switch mode and interface mode. Switch mode has the internal ports all on one interface. Interface mode gives each port its own configurable interface.
Before switching modes, all references to ‘internal’ interfaces must be removed.
This option is visible only on models 100A and 200A for Rev2.0 and higher. Switch mode is also visible on the FortiGate-60B and FortiWiFi-60B. For more information see “Switch Mode” on page 82.

show backplane interfaces
Select to make the two backplane interfaces visible as port9 and port10. Once visible these interfaces can be treated as regular physical interfaces.
This option is available only on 5000 models.

Description icon
The tooltip for this icon displays the Description field for this interface.
### Name
The names of the physical interfaces on your FortiGate unit. This includes any alias names that have been configured.

The name and number of a physical interface depends on the model. Some names indicate the default function of the interface such as Internal, External and DMZ. Other names are generic such as port1.

FortiGate models numbered 50 and 60 provide a modem interface. See “Configuring the modem interface” on page 101.

The oob/ha interface is the FortiGate model 4000 out of band management interface. You can connect to this interface to manage the FortiGate unit. This interface is also available as an HA heartbeat interface.

On FortiGate-60ADSL units, you can configure the ADSL interface. See “Configuring an ADSL interface” on page 85.

On FortiGate models 800 and higher, if you combine several interfaces into an aggregate interface, only the aggregate interface is listed, not the component interfaces. The same is true for redundant interfaces. See “Creating an 802.3ad aggregate interface” on page 86 or “Creating a redundant interface” on page 87.

On the FortiGate model 224B in switch view, port1 through port26 are not shown. These are switch-VLAN ports. See “Viewing switch-LAN ports” on page 209.

If you have added VLAN subinterfaces, they also appear in the name list, below the physical or aggregated interface to which they have been added. See “VLAN overview” on page 107.

If you have loopback or inter-VDOM link virtual interfaces configured you will be able to view them. You can only edit these types of interfaces in the CLI. For more information on these interfaces see “Interfaces only configurable with CLI commands” on page 93 or the `config system interface` and `config system inter-vdom` commands in the FortiGate CLI Reference.

If virtual domain configuration is enabled, you can view information only for the interfaces that are in your current virtual domain, unless you are using the super admin account.

If you have interface mode enabled on a FortiGate model 100A or 200A Rev2.0 or higher or on the FortiGate-60B and FortiWiFi-60B models, you will see multiple internal interfaces. If switch mode is enabled, there will only be one internal interface. For more information see “Switch Mode” on page 82.

If your FortiGate unit supports AMC modules and if you have installed an AMC module containing interfaces (for example, the FortiGate-ASM-FB4 contains 4 interfaces) these interfaces are added to the interface status display. The interfaces are named AMC/1, AMC/2, and so on.

#### IP/Netmask
The current IP address/netmask of the interface.

#### Access
The administrative access configuration for the interface.

See “Additional configuration for interfaces” on page 94.

#### Virtual Domain
The virtual domain to which the interface belongs. This column is visible only to the super admin and only when virtual domain configuration is enabled.

#### Status
The administrative status for the interface.

If the administrative status is a green arrow, the interface is up and can accept network traffic. If the administrative status is a red arrow, the interface is administratively down and cannot accept traffic. To change the administrative status, select Bring Down or Bring Up.

#### Delete, edit, and view icons
Delete, edit, or view an entry.
Switch Mode

The internal interface on 100A, 200A FortiGate models is a four port switch. Normally the internal interface is configured as one interface shared by all four ports. Switch mode allows you to configure each interface on the switch separately with their own interfaces. The FortiGate-60B and FortiWiFi-60B internal interface is a 6-port switch that functions in the same way.

The switch mode feature has two states - switch mode and interface mode. Switch mode is the default mode with only one interface for the entire internal switch. Interface mode allows you to configure each of the internal switch interfaces separately. This allows you to assign different subnets and netmasks to each of the internal interfaces.

Switch mode is only available on 100A and 200A models of Rev2.0 and higher and on all 60B models. Consult your release notes for the most current list of supported models for this feature.

Note: FortiWiFi 60B units do not support switch mode in the GUI interface. They do support switch mode in the CLI.

Selecting the Switch Mode control on the System > Network > Interface screen takes you to the Switch Mode Management screen.

Caution: Before you are able to change between switch mode and interface mode all references to ‘internal’ interfaces must be removed. This includes references such as firewall policies, routing, DNS forwarding, DHCP services, VDOM interface assignments, VLANS, and routing. If they are not removed, you will not be able to switch modes, and you will see an error message.

Figure 34: Switch Mode Management

<table>
<thead>
<tr>
<th>Switch Mode Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Mode</td>
</tr>
<tr>
<td>Interface Mode</td>
</tr>
</tbody>
</table>

Switch Mode
Select Switch Mode. Only one internal interface is displayed. This is the default mode.

Interface Mode
Select Interface Mode. All internal interfaces on the switch are displayed as individually configurable interfaces.

OK
Select to save your changes and return to the Interface screen.

Cancel
Select to discard your changes and return to the Interface screen.

Switch mode in CLI
In addition to the GUI controls, Switch Mode can be configured using CLI commands:

```
config system global
  set internal-switch-mode {interface | switch}
end
```

As in the GUI, if you have not removed all references to the internal interface(s) you will see error messages. Once you have removed these references, your FortiGate unit will reboot and be in the new switch mode.
For more information see `config system global` in the *FortiGate CLI Reference*.

**Interface settings**

Go to **System > Network > Interface**. Select Create New to create a new interface. To edit an existing interface, select the Edit icon for that interface.

Some types of interfaces such as loopback and inter-vdom interfaces can only be configured using CLI commands. For more information see

You cannot create a virtual IPSec interface here, but you can specify its endpoint addresses, enable administrative access and provide a description. For more information, see “Configuring a virtual IPSec interface” on page 92.

To configure switch ports on a FortiGate-224B unit in switch view, see “Configuring a switch-LAN interface” on page 210.

**Figure 35: Create New Interface settings**

<table>
<thead>
<tr>
<th>Name</th>
<th>VLAN ID</th>
<th>Interface</th>
<th>Virtual Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>VLAN</td>
<td>external</td>
<td>root</td>
</tr>
</tbody>
</table>

**Figure 36: Edit Interface settings**

<table>
<thead>
<tr>
<th>Name</th>
<th>Alias</th>
<th>Virtual Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing mode</td>
<td>DHCP</td>
<td>root</td>
</tr>
<tr>
<td>DNS</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>Ping Server</td>
<td>HTTPS</td>
<td>Enable</td>
</tr>
<tr>
<td>Administrative Access</td>
<td>HTTP</td>
<td>Enable</td>
</tr>
<tr>
<td>MTU</td>
<td>Override MTU value (1500)</td>
<td>1500 (bytes)</td>
</tr>
</tbody>
</table>

**Name**

Enter a name for the interface. You cannot change the name of an existing interface.

**Alias**

Enter another name for the interface. The alias name is a way to easily distinguish this interface from another. This is available only for physical interfaces where the name is not configurable. The alias can be a maximum of 15 characters in length. The alias name is not part of the interface name, but it will appear in brackets beside the interface name. It will not appear in logs.
On models 800 and higher, you can create VLAN, 802.3ad Aggregate, and Redundant interfaces.

- On FortiWiFi-50B, 60A, 60AM, and 60B units, you can support up to four SSIDs by adding up to three wireless interfaces (for a total of four wireless interfaces).
- On the 60ADSL model, you can configure an ADSL interface.
- Other models support creation of VLAN interfaces only and have no Type field.
- To configure an ADSL interface, see “Configuring an ADSL interface” on page 85.
- To create a VLAN subinterface, see “FortiGate units and VLANs” on page 107.
- To create an aggregate interface, see “Creating an 802.3ad aggregate interface” on page 86.
- To create a redundant interface, see “Creating a redundant interface” on page 87.
- To create a wireless interface, see “Adding a wireless interface to a FortiWiFi-50B, 60A, 60AM, and 60B unit” on page 122.

You cannot change the type of an existing interface.

**Interface**

Select the name of the physical interface on which to create the VLAN. Once created, the VLAN subinterface is listed below its physical interface in the Interface list. You cannot change the interface of an existing VLAN subinterface. This field is only displayed when Type is set to VLAN.

**Physical Interface Members**

Move the interfaces to be included in the 802.3ad aggregate or Redundant interface from the Available interfaces list to the Selected interfaces list. This field is only displayed when Type is set to either 802.3ad aggregate or Redundant interface.

**VLAN ID**

Enter the VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface. You cannot change the VLAN ID of an existing VLAN subinterface. The VLAN ID can be any number between 1 and 4096 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch connected to the VLAN subinterface. See “VLAN overview” on page 107. This field is only displayed when Type is set to VLAN.

**Virtual Domain**

Select the virtual domain to which this VLAN subinterface belongs. This is available to the super admin account when virtual domain configuration is enabled. See “Using virtual domains” on page 71.

**Addressing mode**

To configure a static IP address for the interface, select Manual. You can also configure the interface for dynamic IP address assignment. See “Configuring DHCP on an interface” on page 88 or “Configuring an interface for PPPoE or PPPoA” on page 90.

**IP/Netmask**

Enter the IP address/subnet mask in the IP/Netmask field. The IP address must be on the same subnet as the network to which the interface connects. Two interfaces cannot have IP addresses on the same subnet. This field is only available when Manual addressing mode is selected.

**DDNS**

Select DDNS to configure a Dynamic DNS service for this interface. Additional fields are displayed. See “Configuring Dynamic DNS service for an interface” on page 91.

**Ping Server**

To enable dead gateway detection, enter the IP address of the next hop router on the network connected to the interface and select Enable. See “Dead gateway detection” on page 100.
Configuring an ADSL interface

The information that you need to provide for the ADSL interface depends on the addressing mode your ISP requires you to use. Static addressing using IPOA or EOA requires only an IP address and netmask. If you are using dynamic addressing, you need to configure it as described in “Configuring DHCP on an interface” on page 88 or “Configuring an interface for PPPoE or PPPoA” on page 90.

To configure an ADSL interface, your FortiGate unit cannot be in Transparent mode.

Go to **System > Network > Interface**. Select Create New or select the Edit icon of an existing interface. In the Addressing mode section, select IPoA or EoA.

### Administrative Access

Select the types of administrative access permitted on this interface.

- **HTTPS**
  - Allow secure HTTPS connections to the web-based manager through this interface.

- **PING**
  - Interface responds to pings. Use this setting to verify your installation and for testing.

- **HTTP**
  - Allow HTTP connections to the web-based manager through this interface. HTTP connections are not secure and can be intercepted by a third party.

- **SSH**
  - Allow SSH connections to the CLI through this interface.

- **SNMP**
  - Allow a remote SNMP manager to request SNMP information by connecting to this interface. See “Configuring SNMP” on page 143.

- **TELNET**
  - Allow Telnet connections to the CLI through this interface. Telnet connections are not secure and can be intercepted by a third party.

### MTU

To change the MTU, select Override default MTU value (1 500) and enter the MTU size based on the addressing mode of the interface:

- 68 to 1 500 bytes for static mode
- 576 to 1 500 bytes for DHCP mode
- 576 to 1 492 bytes for PPPoE mode
- up to 16 110 bytes for jumbo frames (FortiGate models numbered 3000 and higher)

This field is available only on physical interfaces. VLANs inherit the parent interface MTU size by default.

For more information on MTU and jumbo frames, see “Interface MTU packet size” on page 95.

### Secondary IP Address

Select the blue arrow to expand or hide this section and add additional IP addresses to this interface. See “Secondary IP Addresses” on page 96.

### Description

Optionally, enter a description up to 63 characters long.

---

**Note:** In Transparent mode, if you change the MTU of an interface, you must change the MTU of all interfaces to match the new MTU.
Creating an 802.3ad aggregate interface

You can aggregate (combine) two or more physical interfaces to increase bandwidth and provide some link redundancy. This has the benefit of higher bandwidth but has more potential points of failure than redundant interfaces. The interfaces must connect to the same next-hop routing destination.

FortiGate firmware on models 800 and higher implements IEEE standard 802.3ad for link aggregation.

An interface is available for aggregation only if

- it is a physical interface, not a VLAN interface
- it is not already part of an aggregated or redundant interface
- it is in the same VDOM as the aggregated interface
- it has no defined IP address and is not configured for DHCP or PPPoE
- it has no DHCP server or relay configured on it
- it does not have any VLAN subinterfaces
- it is not referenced in any firewall policy, VIP, IP Pool or multicast policy
- it is not an HA heartbeat interface

Note: While you can add accelerated interfaces (FA2 ports) to an aggregate link, you will lose the acceleration. For example, aggregating two accelerated ports would result in slower throughput than the two ports separately.
When an interface is included in an aggregate interface, it is not listed on the System > Network > Interface page. It is no longer individually configurable and is not available for inclusion in firewall policies, VIPs, IP pools or routing.

Figure 38: Settings for an 802.3ad aggregate interface

<table>
<thead>
<tr>
<th>New Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Virtual Domain</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical Interface Members:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Interfaces</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Selected Interfaces</td>
</tr>
<tr>
<td>external</td>
</tr>
<tr>
<td>internal</td>
</tr>
<tr>
<td>port2</td>
</tr>
</tbody>
</table>

To create an 802.3ad Aggregate interface

1. Go to System > Network > Interface.
2. Select Create New.
3. In the Name field, enter a name for the aggregated interface. The interface name must not be the same as any other interface, zone or VDOM.
4. From the Type list, select 802.3ad Aggregate.
5. One at a time, in the Available Interfaces list, select each interface that you want to include in the aggregate interface and then select the right arrow button to move it to the Selected Interfaces list.
6. If this interface operates in NAT/Route mode, you need to configure addressing for it. For information about dynamic addressing, see:
   - “Configuring DHCP on an interface” on page 88
   - “Configuring an interface for PPPoE or PPPoA” on page 90
7. Configure other interface options as required.
8. Select OK.

Creating a redundant interface

You can combine two or more physical interfaces to provide link redundancy. This feature allows you to connect to two or more switches to ensure connectivity in the event one physical interface or the equipment on that interface fails.

Redundant links differ from link aggregation in that traffic is only going over one interface at any time (no matter how many are in the redundant link), but redundant interfaces allow for more robust configurations with fewer possible points of failure. This is important in a fully meshed HA configuration.

FortiGate firmware on models 800 and higher implements redundant interfaces. An interface is available to be in a redundant interface only if:

- it is a physical interface, not a VLAN interface
- it is not already part of an aggregated or redundant interface
- it is in the same VDOM as the redundant interface
Interface System Network

- it has no defined IP address and is not configured for DHCP or PPPoE
- it has no DHCP server or relay configured on it
- it does not have any VLAN subinterfaces
- it is not referenced in any firewall policy, VIP, IP Pool or multicast policy
- it is not monitored by HA

When an interface is included in a redundant interface, it is not listed on the System > Network > Interface page. It is no longer individually configurable and is not available for inclusion in firewall policies, VIPs, IP pools or routing.

Figure 39: Settings for a redundant interface

To create a redundant interface

1. Go to System > Network > Interface.
2. Select Create New.
3. In the Name field, enter a name for the redundant interface.
   The interface name must not be the same as any other interface, zone or VDOM.
4. From the Type list, select Redundant Interface.
5. One at a time, in the Available Interfaces list, select each physical interface that you want to include in the redundant interface and then select the right arrow button to move it to the Selected Interfaces list. The interfaces you add will be used in the order they appear in the Selected Interfaces list. For example if the first interface in the list fails, the second interface is used.
6. If this interface operates in NAT/Route mode, you need to configure addressing for it. For information about dynamic addressing, see:
   - “Configuring DHCP on an interface” on page 88
   - “Configuring an interface for PPPoE or PPPoA” on page 90
7. Configure other interface options as required.
8. Select OK.

Configuring DHCP on an interface

If you configure an interface to use DHCP, the FortiGate unit automatically broadcasts a DHCP request. The interface is configured with the IP address and optionally DNS server addresses and default gateway address that the DHCP server provides.

Go to System > Network > Interface. Select Create New or select the Edit icon of an existing interface. In the Addressing mode section, select DHCP.
Figure 40: Interface DHCP settings

<table>
<thead>
<tr>
<th>Addressing mode</th>
<th>Status: connected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status:</td>
<td></td>
</tr>
<tr>
<td>Obtained IP/Netmask: 1.2.3.100/255.255.255.0</td>
<td>Renew</td>
</tr>
<tr>
<td>Expiry Date:</td>
<td>Tue Jun 20 13:44:29 2006</td>
</tr>
<tr>
<td>Default Gateway:</td>
<td>1.2.3.4</td>
</tr>
<tr>
<td>Distance:</td>
<td>1</td>
</tr>
</tbody>
</table>

- Retrieve default gateway from server.
- Override internal DNS.

Status
Displays DHCP status messages as the FortiGate unit connects to the DHCP server and gets addressing information. Select Status to refresh the addressing mode status message. This is only displayed if you selected Edit. Status can be one of:

- **initializing** - No activity.
- **connecting** - The interface is attempting to connect to the DHCP server.
- **connected** - The interface retrieves an IP address, netmask, and other settings from the DHCP server.
- **failed** - The interface was unable to retrieve an IP address and other information from the DHCP server.

- ** Obtained IP/Netmask **
The IP address and netmask leased from the DHCP server. This is only displayed if Status is connected.

- ** Renew **
Select to renew the DHCP license for this interface. This is only displayed if Status is connected.

- ** Expiry Date **
The time and date when the leased IP address and netmask is no longer valid. This is only displayed if Status is connected.

- ** Default Gateway **
The IP address of the gateway defined by the DHCP server. This is only displayed if Status is connected, and if Receive default gateway from server is selected.

- ** Distance **
Enter the administrative distance for the default gateway retrieved from the DHCP server. The administrative distance, an integer from 1-255, specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. The default distance for the default gateway is 1.

- ** Retrieve default gateway from server **
Enable Retrieve default gateway from server to retrieve a default gateway IP address from the DHCP server. The default gateway is added to the static routing table. 

### Configuring an interface for PPPoE or PPPoA

If you configure the interface to use PPPoE or PPPoA, the FortiGate unit automatically broadcasts a PPPoE or PPPoA request. You can disable Connect to Server if you are configuring the FortiGate unit offline and you do not want the FortiGate unit to send the PPPoE or PPPoA request.

FortiGate units support many of the PPPoE RFC features (RFC 2516) including unnumbered IPs, initial discovery timeout and PPPoE Active Discovery Terminate (PADT).

PPPoA is only available on FortiGate models that support ADSL.

Go to **System > Network > Interface**. Select Create New or select the Edit icon of an existing interface. In the Addressing mode section, select PPPoE or PPPoA.

#### Figure 42: Interface PPPoE settings

<table>
<thead>
<tr>
<th>Addressing mode</th>
<th>DHCP</th>
<th>PPPoE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unnumbered IP</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>Initial Disc Timeout</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Initial PADD Timeout</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Distance</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Retrieve default gateway from server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Override internal DNS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Figure 43: ADSL interface PPPoE or PPPoA settings

<table>
<thead>
<tr>
<th>Addressing mode</th>
<th>PPPoE</th>
<th>PPPoA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unnumbered IP</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>Initial Disc Timeout</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Initial PADD Timeout</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>Auto</td>
<td></td>
</tr>
<tr>
<td>Distance</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Retrieve default gateway from server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Override internal DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect to Server</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Dynamic DNS service for an interface

When the FortiGate unit has a static domain name and a dynamic public IP address, you can use a DDNS service to update Internet DNS servers when the IP address for the domain changes.

Dynamic DNS is available only in NAT/Route mode.

Go to **System > Network > Interface**. Select Create New or select the Edit icon of an existing interface. Enable DDNS, just below the Addressing mode section, and configure the DDNS service using the information they have provided to you.
If at any time your FortiGate unit cannot contact the DDNS server, it will retry three times at one minute intervals and then change to retrying at three minute intervals. This is to prevent flooding the DDNS server.

**Figure 44: DDNS service configuration**

| Server | The fully qualified domain name of the DDNS service. |
| Domain | The user name to use when connecting to the DDNS server. |
| Username | The password to use when connecting to the DDNS server. |

**Configuring a virtual IPSec interface**

You create a virtual IPSec interface by selecting IPSec Interface Mode in **VPN > IPSec > Auto Key** or **VPN > IPSec > Manual Key** when you create a VPN. You also select a physical or VLAN interface from the Local Interface list. The virtual IPSec interface is listed as a subinterface of that interface in **System > Network > Interface**. For more information, see

- "Overview of IPSec interface mode" on page 343
- "Auto Key" on page 345 or "Manual Key" on page 354

Go to **System > Network > Interface** and select Edit on an IPSec interface to:

- configure IP addresses for the local and remote endpoints of the IPSec interface so that you can run dynamic routing over the interface or use ping to test the tunnel
- enable administrative access through the IPSec interface
- enable logging on the interface
- enter a description for the interface

**Figure 45: Virtual IPSec interface settings**
Interfaces only configurable with CLI commands

While nearly all types of interfaces can be configured from the GUI interface, a few, such as the loopback and inter-vdom virtual interface types, can only be configured using CLI commands.

Virtual interfaces are not connected to any physical devices or cables outside the FortiGate unit. They allow additional connections inside the FortiGate unit, which allow for more complex configurations. Virtual interfaces also have the added benefit of speed - depending on CPU load they are considerably faster than physical interfaces. VLANs, loopback interfaces, and inter-vdom interfaces are all virtual interfaces.

Loopback interface

The loopback interface is a virtual interface. It was added to assist with blackhole routing where network traffic is just dropped. For more information on blackhole routing, see “Blackhole Routing” on page 234.

A loopback interface is not connected to hardware, so it does not have hardware connection issues. As long as the FortiGate unit is functioning the loopback interface is active. This ‘always up’ feature is useful in a number of situations, such as dynamic routing.

The CLI command to configure a loopback interface called loop1 with an IP address of 10.0.0.10 is:

```
config system interface
edit loop1
  set type loopback
  set ip 10.0.0.10 255.255.255.0
end
```

For more information, see config system interface in the FortiGate CLI Reference.
Inter-vdom interface

Virtual domains (VDOMs) help to separate traffic based on your needs. The inter-vdom interface is used to connect two virtual domains without using a physical interface. VDOMs must be enabled before you can create an inter-vdom interface.

Traffic between VDOMs over an inter-vdom interface has to leave and re-enter through the firewall maintaining the established level of security of physical interfaces on your FortiGate unit.

Before inter-vdom interfaces, the number of physical interfaces limited the possible configurations. Inter-vdom links are virtual interfaces, removing that limit. If your FortiGate unit has many VDOMs, inter-vdom interfaces allow you to configure things however you need from a simple stand alone VDOM configuration to a complex meshed VDOM configuration. For more information, see the FortiGate VLANs and VDOMs User Guide.

When creating the inter-vdom interface, there are two ends to configure - one connects to each VDOM. The CLI command to configure an inter-vdom interface or link interface called link1 that connects root VDOM to vdom1:

```fortigate
config global
config system vdom-link
edit link1
    config system interface
    edit link10
        set vdom root
        next
    edit link11
        set vdom vdom1
        next
end
```

For more information, see config system interface in the FortiGate CLI Reference.

Additional configuration for interfaces

Once the interface is selected with the basic settings configured, some additional configuration may be considered. Additional configuration for an interface consists of setting:

- Administrative access to an interface
- Interface MTU packet size
- Traffic logging for an interface
- Secondary IP Addresses

Administrative access to an interface

For a VDOM running in NAT/Route mode, you can control administrative access to the interfaces in that VDOM.

You can allow remote administration of the FortiGate unit. However, allowing remote administration from the Internet could compromise the security of the FortiGate unit. You should avoid this unless it is required for your configuration. To improve the security of a FortiGate unit that allows remote administration from the Internet:
Use secure administrative user passwords.
Change these passwords regularly.
Enable secure administrative access to this interface using only HTTPS or SSH.
Do not change the system idle timeout from the default value of 5 minutes (see “Settings” on page 175).
For more information on configuring administrative access in Transparent mode, see “Operation mode and VDOM management access” on page 158.

To control administrative access to an interface
1. Go to **System > Network > Interface**.
2. Choose an interface and select Edit.
4. Select OK to save the changes.

**Interface MTU packet size**

To improve network performance, you can change the maximum transmission unit (MTU) of the packets that the FortiGate unit transmits. Ideally, the MTU should be the same as the smallest MTU of all the networks between the FortiGate unit and the destination of the packets. If the packets that the FortiGate unit sends are larger, they are broken up or fragmented, which slows down transmission. Experiment by lowering the MTU to find an MTU size for best network performance.

FortiGate models numbered 3000 and higher support jumbo frames. Some models support a limit of 9,000 bytes while others support 16,110 bytes. Jumbo frames can be up to 9,000 bytes or 16,110, much larger than standard Ethernet frames. Standard Ethernet frames (packets) can be a maximum of 1,500 bytes including header information. As new Ethernet standards have been implemented (such as Gigabit Ethernet), 1,500-byte frames have been kept for backward compatibility.

To be able to send jumbo frames over a route, all Ethernet devices on that route must support jumbo frames. Otherwise your jumbo frames are not recognized and they are dropped.

If you have standard ethernet and jumbo frame traffic on the same interface, routing alone cannot route them to different routes based only on frame size. However you can use VLANs to make sure the jumbo frame traffic is routed over network devices that support jumbo frames. VLANs will inherit the MTU size from the parent interface. You will need to configure the VLAN to include both ends of the route as well as all switches and routers along the route. For more information on VLAN configurations, see the VLAN and VDOM guide.

To change the MTU size of the packets leaving an interface
1. Go to **System > Network > Interface**.
2. Choose a physical interface and select Edit.
3. Select Override default MTU value (1500).
4 Set the MTU size.

If you select an MTU size larger than your FortiGate unit supports, an error message will indicate this. In this situation, try a smaller MTU size until the value is supported. Supported maximums are 16110, 9000, and 1500.

**Note:** If you change the MTU, you need to reboot the FortiGate unit to update the MTU value of VLAN subinterfaces on the modified interface.

**Note:** In Transparent mode, if you change the MTU of an interface, you must change the MTU of all interfaces to match the new MTU.

**Traffic logging for an interface**

You can enable traffic logging for any interface. See “Traffic log” on page 481 for more information.

**Secondary IP Addresses**

An interface can be assigned more than one IP address. You can create and apply separate firewall policies for each IP address on an interface. You can also forward traffic and use RIP or OSPF routing with secondary IP addresses.

There can be up to 32 secondary IP addresses per interface. Primary and secondary IP addresses can share the same ping generator.

The following restrictions must be in place before you are able to assign a secondary IP address:

- A primary IP address must be assigned to the interface first.
- The interface must use manual addressing mode.
- By default, IP addresses cannot be part of the same subnet. To allow interface subnet overlap use the CLI command:

```
config system global
(global)# set allow-interface-subnet-overlap enable
(global)#end
```

Secondary IP addresses cannot terminate a VPN tunnel.

You can use the CLI command `config system interface` to add a secondary IP address to an interface. For more information, see `config secondaryip` under `system interface` in the FortiGate CLI Reference.

**Figure 46: Adding Secondary IP Addresses**

- **Administrative Access**
  - HTTPS
  - SSH
  - SNMP
  - Telnet

- **Status:**
  - Enabled

- **Ping Server:**
  - 10.10.10.1

- **IP / Netmask:**
  - 10.10.10.1/24

- **Add**
**IP/Netmask**

Enter the IP address/subnet mask in the IP/Netmask field. The Secondary IP address must be on a different subnet than the Primary IP address. Two interfaces cannot have IP addresses on the same subnet. This field is only available when Manual addressing mode is selected.

**Ping Server**

To enable dead gateway detection, enter the IP address of the next hop router on the network connected to the interface and select Enable. See “Dead gateway detection” on page 100. Multiple addresses can share the same ping server. This field is optional.

**Administrative Access**

Select the types of administrative access permitted on the secondary IP. These can be different from the primary address.

- **HTTPS**
  - Allow secure HTTPS connections to the web-based manager through this secondary IP.

- **PING**
  - Secondary IP responds to pings. Use this setting to verify your installation and for testing.

- **HTTP**
  - Allow HTTP connections to the web-based manager through this secondary IP. HTTP connections are not secure and can be intercepted by a third party.

- **SSH**
  - Allow SSH connections to the CLI through this secondary IP.

- **SNMP**
  - Allow a remote SNMP manager to request SNMP information by connecting to this secondary IP. See “Configuring SNMP” on page 143.

- **TELNET**
  - Allow Telnet connections to the CLI through this secondary IP. Telnet connections are not secure and can be intercepted by a third party.

**Add**

Select Add to add the configured secondary IP address to the secondary IP table shown below. Addresses in this table are not added to the interface until you select OK or Apply at the bottom of this screen.

**Secondary IP table**

A table that shows all the secondary IP addresses that have been added to this interface. These addresses are not permanently added to the interface until you select OK or Apply at the bottom of the screen. Otherwise some addresses may be removed from the table due to the above restrictions.

<table>
<thead>
<tr>
<th>#</th>
<th>The number of the secondary IP address. There can be up to 32 additional IP addresses on an interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/Netmask</td>
<td>The IP address and netmask for this secondary IP.</td>
</tr>
<tr>
<td>Ping Server</td>
<td>The IP address of the ping server for this address. The ping server can be shared by multiple addresses. The ping server is optional.</td>
</tr>
<tr>
<td>Enable</td>
<td>Indicates if the ping server option is selected.</td>
</tr>
<tr>
<td>Access</td>
<td>The administrative access methods for this address. They can be different from the primary IP address.</td>
</tr>
<tr>
<td>Delete Icon</td>
<td>Select to remove this secondary IP entry.</td>
</tr>
</tbody>
</table>

**Note:** It is recommended that after adding a secondary IP, you return to the secondary IP table and verify your new address is listed. If not, one of the restrictions prevented the address from being added.
Zone

You can use zones to group related interfaces and VLAN subinterfaces. Grouping interfaces and VLAN subinterfaces into zones simplifies policy creation. If you group interfaces and VLAN subinterfaces into a zone, you can configure policies for connections to and from this zone, but not between interfaces in the zone.

You can add zones, rename and edit zones, and delete zones from the zone list. When you add a zone, you select the names of the interfaces and VLAN subinterfaces to add to the zone.

Zones are added to virtual domains. If you have added multiple virtual domains to your FortiGate configuration, make sure you are configuring the correct virtual domain before adding or editing zones.

Figure 47: Zone list

<table>
<thead>
<tr>
<th>Name</th>
<th>Block intra-zone traffic</th>
<th>Interface Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone1</td>
<td>No</td>
<td>internal</td>
</tr>
<tr>
<td>Zone2</td>
<td>Yes</td>
<td>port2, port4</td>
</tr>
<tr>
<td>Zone3</td>
<td>Yes</td>
<td>port2, port3</td>
</tr>
</tbody>
</table>

Create New

Select Create New to create a new zone.

Name

The names of the zones that you have added.

Block intra-zone traffic

Displays Yes if traffic between interfaces in the same zone is blocked and No if traffic between interfaces in the same zone is not blocked.

Interface Members

The names of the interfaces added to the zone. Interface names depend on the FortiGate model.

Edit/View icons

Edit or view a zone.

Delete icon

Delete a zone.

Zone settings

Go to System > Network > Zone to configure zones. Select Create New or select the Edit icon for a zone to modify that zone.

Figure 48: Zone options

Name

Enter the name to identify the zone.

Block intra-zone traffic

Select Block intra-zone traffic to block traffic between interfaces or VLAN subinterfaces in the same zone.

Interface members

Select the interfaces that are part of this zone. This list includes configured VLANs.
Network Options

Network options include DNS server and dead gateway detection settings. These options are set on the Configuring Network Options screen.

Go to **System > Network > Options** to configure DNS servers and Dead Gateway Detection settings.

**Figure 49: Networking Options - FortiGate models 200 and higher**

<table>
<thead>
<tr>
<th>Networking Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Settings</td>
</tr>
<tr>
<td>Primary DNS Server</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
</tr>
<tr>
<td>Local Domain Name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dead Gateway Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection Interval</td>
</tr>
<tr>
<td>Fail-over Detection</td>
</tr>
<tr>
<td>Apply</td>
</tr>
</tbody>
</table>

**Figure 50: Networking Options - models numbered 100 and lower**

<table>
<thead>
<tr>
<th>Networking Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Settings</td>
</tr>
<tr>
<td>Obtain DNS server address automatically</td>
</tr>
<tr>
<td>Use the following DNS server addresses</td>
</tr>
<tr>
<td>Primary DNS Server</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
</tr>
<tr>
<td>Local Domain Name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enable DNS forwarding from:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
</tr>
<tr>
<td>802.11x</td>
</tr>
<tr>
<td>802.11z</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dead Gateway Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection Interval</td>
</tr>
<tr>
<td>Fail-over Detection</td>
</tr>
<tr>
<td>Apply</td>
</tr>
</tbody>
</table>

**Obtain DNS server address automatically**

This option applies only to FortiGate models 100 and lower.

When DHCP is used on an interface, also obtain the DNS server IP address. Available only in NAT/Route mode. You should also enable Override internal DNS in the DHCP settings of the interface. See “Configuring DHCP on an interface” on page 88.

**Use the following DNS server addresses**

This option applies only to FortiGate models 100 and lower.

Use the specified Primary and Secondary DNS server addresses.

- **Primary DNS Server**
  - Enter the primary DNS server IP address.

- **Secondary DNS Server**
  - Enter the secondary DNS server IP address.

- **Local Domain Name**
  - Enter the domain name to append to addresses with no domain portion when performing DNS lookups.
DNS Servers

Several FortiGate functions use DNS, including alert email and URL blocking. You can specify the IP addresses of the DNS servers to which your FortiGate unit connects. DNS server IP addresses are usually supplied by your ISP.

You can configure FortiGate models numbered 100 and lower to obtain DNS server addresses automatically. To obtain these addresses automatically, at least one FortiGate unit interface must use the DHCP or PPPoE addressing mode. See "Configuring DHCP on an interface" on page 88 or "Configuring an interface for PPPoE or PPPoA" on page 90.

FortiGate models 100 and lower can provide DNS Forwarding on their interfaces. Hosts on the attached network use the interface IP address as their DNS server. DNS requests sent to the interface are forwarded to the DNS server addresses that you configured or that the FortiGate unit obtained automatically.

Dead gateway detection

Dead gateway detection periodically pings a ping server to confirm network connectivity. Typically, the ping server is the next-hop router that leads to an external network or the Internet. The ping period (Detection Interval) and the number of failed pings that is considered to indicate a loss of connectivity (Fail-over Detection) are set in System > Network > Options.

To apply dead gateway detection to an interface, you must configure a ping server on it.

To add a ping server to an interface

1. Go to System > Network > Interface.
2. Choose an interface and select Edit.
3. Set Ping Server to the IP address of the next hop router on the network connected to the interface.
4. Select the Enable check box.
5. Select OK to save the changes.
Routing table (Transparent Mode)

In Transparent mode, go to System > Network > Routing Table to add static routes from the FortiGate unit to local routers.

Figure 51: Routing table

<table>
<thead>
<tr>
<th>#</th>
<th>IP</th>
<th>Mask</th>
<th>Gateway</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>10.10.10.254</td>
<td>10</td>
</tr>
</tbody>
</table>

Create New Add a new route.

# Route number.

IP The destination IP address for this route.

Mask The netmask for this route.

Gateway The IP address of the next hop router to which this route directs traffic.

Distance The relative preferability of this route. 1 is most preferred.

Delete icon Remove a route.

View/edit icon Edit or view a route.

Move To icon Change the position of a route in the list.

Transparent mode route settings

Go to System > Network > Routing Table and select Create New to add a route. You can also select the Edit icon of an existing route to modify it.

Figure 52: Transparent mode route options

Destination IP/Netmask Enter the destination IP address and netmask for this route.

Gateway Enter the IP address of the next hop router to which this route directs traffic. For an Internet connection, the next hop routing gateway routes traffic to the Internet.

Distance The relative preferability of this route. 1 is most preferred.

Configuring the modem interface

All FortiGate-50 series and FortiGate-60 series modules include modem support. You can use the modem as either a backup interface or a standalone interface in NAT/Route mode.

- In redundant (backup) mode, the modem interface automatically takes over from a selected ethernet interface when that ethernet interface is unavailable.
- In standalone mode, the modem interface is the connection from the FortiGate unit to the Internet.
When connecting to the ISP, in either configuration, you can configure the FortiGate unit to automatically have the modem dial up to three dialup accounts until the modem connects to an ISP.

FortiGate models 50AM, 60M have a built-in modem. For these models, you can configure modem operation in the web-based manager. See “Configuring modem settings”.

Other 50 and 60 models can connect to an external modem through a USB-to-serial converter. For these models, you must configure modem operation using the CLI. See the `system modem` command in the FortiGate CLI Reference.

**Note:** The modem interface is not the AUX port which is a port that is used for a remote console connection. The AUX port has no associated interface. The AUX port is only available on FortiGate models 1000A, 1000AFA2, and 3000A. For more information, see the `config system aux` command in the FortiGate CLI Reference.

### Configuring modem settings

Configure modem settings so that the FortiGate unit uses the modem to connect to your ISP dialup accounts. You can configure up to three dialup accounts, select standalone or redundant operation, and configure how the modem dials and disconnects.

You can configure and use the modem in NAT/Route mode only.

#### Figure 53: Modem settings (Standalone)

[Diagram of modem settings configuration]

- **Enable Modem**: Options for standalone or redundant operation.
- **Mode**: Options for dial-up or dial-on-demand.
- **Idle Timeout**: Time in minutes after which the modem disconnects.
- **Dial-up Accounts**: Fields for phone number, user name, and password for each account.

Apply changes after configuration.
Figure 54: Modem settings (Redundant)

Enable Modem
Select to enable the FortiGate modem.

Modem status
Modem status can be: not active, connecting, connected, disconnecting, or hung up.

Dial Now/Hang Up
(Standalone mode only) Select Dial Now to manually connect to a dialup account. If the modem is connected, you can select Hang Up to manually disconnect the modem.

Mode
Select Standalone or Redundant mode.
In Standalone mode, the modem is an independent interface.
In Redundant mode, the modem is a backup facility for a selected Ethernet interface.

Auto-dial
(Standalone mode only) Select to dial the modem automatically if the connection is lost or the FortiGate unit is restarted.
You cannot select Auto-dial if Dial on demand is selected.

Redundant for
(Standalone mode only) Select the ethernet interface for which the modem provides backup service.

Dial on demand
Select to dial the modem when packets are routed to the modem interface. The modem disconnects after the idle timeout period if there is no network activity.
You cannot select Dial on demand if Auto-dial is selected.

Idle timeout
Enter the timeout duration in minutes. After this period of inactivity, the modem disconnects.

Holddown Timer
(Reudndant mode only) Enter the time (1-60 seconds) that the FortiGate unit waits before switching back to the primary interface from the modem interface, after the primary interface has been restored. The default is 1 second. Configure a higher value if you find the FortiGate unit switching repeatedly between the primary interface and the modem interface.

Redial Limit
The maximum number of times (1-10) that the FortiGate unit modem attempts to reconnect to the ISP if the connection fails. The default redial limit is 1. Select None to have no limit on redial attempts.

Dialup Account
Configure up to three dialup accounts. The FortiGate unit tries connecting to each account in order until a connection can be established.
Configuring the modem interface

To configure the modem in Redundant mode, see “Redundant mode configuration” on page 104.

To configure the modem in Standalone mode, see “Standalone mode configuration” on page 105.

Redundant mode configuration

The modem interface in redundant mode backs up a selected ethernet interface. If that ethernet interface disconnects from its network, the modem automatically dials the configured dialup accounts. When the modem connects to a dialup account, the FortiGate unit routes IP packets normally destined for the selected ethernet interface to the modem interface.

The FortiGate unit disconnects the modem interface and switches back to the ethernet interface when the ethernet interface can again connect to its network. You can set a holddown timer which delays switching back to the ethernet interface to ensure it is stable and fully active before switching the traffic.

There is an optional timeout setting, after which the modem will disconnect if there is no network activity. This is useful in saving money on dialup connection charges.

For the FortiGate unit to be able to switch from an ethernet interface to the modem you must select the name of the interface in the modem configuration and configure a ping server for that interface. You must also configure firewall policies for connections between the modem interface and other FortiGate interfaces.

Note: Do not add policies for connections between the modem interface and the ethernet interface that the modem is backing up.

To configure redundant mode

1. Go to System > Network > Modem.
2. Select Redundant mode.
3. Enter the following information:
   - Mode: Redundant
   - Redundant for: From the list, select the interface to back up.
   - Holddown timer: Enter the number of seconds to continue using the modem after the interface is restored.
   - Redial Limit: Enter the maximum number of times to retry if the ISP does not answer.
   - Dialup Account 1, Dialup Account 2, Dialup Account 3: Enter the ISP phone number, user name and password for up to three dialup accounts.
4. Select Apply.
Configure a ping server for the ethernet interface the modem backs up.
See "To add a ping server to an interface" on page 100.

Configure firewall policies for connections to the modem interface.
See "Adding firewall policies for modem connections" on page 106.

Standalone mode configuration

In standalone mode, the modem connects to a dialup account to provide a connection to the Internet. You can configure the modem to dial when the FortiGate unit restarts or when there are unrouted packets. You can also hang up or redial the modem manually.

If the connection to the dialup account fails, the FortiGate unit will redial the modem. The modem redials the number of times specified by the redial limit, or until it connects to a dialup account.

There is an optional timeout setting, after which the modem will disconnect if there is no network activity. This is useful in saving money on dialup connection charges.

You must configure firewall policies for connections between the modem interface and other FortiGate interfaces.

You must also go to Router > Static to configure static routes to route traffic to the modem interface. For example, if the modem interface is acting as the FortiGate unit external interface you must set the device setting of the FortiGate unit default route to modem.

To operate in standalone mode

1. Go to System > Network > Modem.
2. Enter the following information:

   Mode: Standalone
   Auto-dial: Select if you want the modem to dial when the FortiGate unit restarts.
   Dial on demand: Select if you want the modem to connect to its ISP whenever there are unrouted packets.
   Idle timeout: Enter the timeout duration in minutes. After this period of inactivity, the modem disconnects.
   Redial Limit: Enter the maximum number of times to retry if the ISP does not answer.
   Dialup Account 1: Enter the ISP phone number, user name and password for up to three dialup accounts.

3. Select Apply.

4. Configure firewall policies for connections to the modem interface.
   See "Adding firewall policies for modem connections" on page 106.

5. Go to Router > Static to configure static routes to route traffic to the modem interface. For these routes, set device to Modem.
   See "Adding a static route to the routing table" on page 238.
Adding firewall policies for modem connections

The modem interface requires firewall addresses and policies. You can add one or more addresses to the modem interface. For information about adding addresses, see “Configuring addresses” on page 291.

You can configure firewall policies to control the flow of packets between the modem interface and the other interfaces on the FortiGate unit. For information about adding firewall policies, see “Adding a firewall policy” on page 270.

Connecting and disconnecting the modem

The modem must be in Standalone mode before starting these procedures.

To connect to a dialup account

1. Go to System > Network > Modem.
2. Select Enable USB Modem.
3. Make sure there is correct information for one or more Dialup Accounts.
4. Select Apply if you make any configuration changes.
5. Select Dial Now.

The FortiGate unit dials into each dialup account in turn until the modem connects to an ISP.

To disconnect the modem

Use the following procedure to disconnect the modem from a dialup account.

1. Go to System > Network > Modem.
2. Select Hang Up to disconnect from the currently connected dialup account.

Checking modem status

You can determine the connection status of your modem and which dialup account is active. If the modem is connected to the ISP, you can see the IP address and netmask.

To check the modem status, go to System > Network > Modem.

Modem status is one of the following:

- **not active**: The modem is not connected to the ISP.
- **connecting**: The modem is attempting to connect to the ISP.
- **connected**: The modem is connected to the ISP.
- **disconnecting**: The modem is disconnecting from the ISP.
- **hung up**: The modem has disconnected from the ISP. (Standalone mode only) The modem will not redial unless you select Dial Now.

A green check mark indicates the active dialup account.

The IP address and netmask assigned to the modem interface appears on the System Network Interface page of the web-based manager.
VLAN overview

A VLAN is a group of PCs, servers, and other network devices that communicate as if they were on the same LAN segment, independent of where they are located. For example, the workstations and servers for an accounting department could be scattered throughout an office or city and connected to numerous network segments, but still belong to the same VLAN.

A VLAN segregates devices logically instead of physically. Each VLAN is treated as a broadcast domain. Devices in VLAN 1 can connect with other devices in VLAN 1, but cannot connect with devices in other VLANs. The communication among devices on a VLAN is independent of the physical network.

A VLAN segregates devices by adding 802.1Q VLAN tags to all of the packets sent and received by the devices in the VLAN. VLAN tags are 4-byte frame extensions that contain a VLAN identifier as well as other information.

For more information on VLANs, see the FortiGate VLANs and VDOMs Guide.

Figure 55: Basic VLAN topology

FortiGate units and VLANs

In a typical VLAN configuration, 802.1Q-compliant VLAN layer-2 switches or layer-3 routers or firewalls add VLAN tags to packets. Packets passing between devices in the same VLAN can be handled by layer-2 switches. Packets passing between devices in different VLANs must be handled by a layer-3 device such as router, firewall, or layer-3 switch.
Using VLANs, a single FortiGate unit can provide security services and control connections between multiple security domains. Traffic from each security domain is given a different VLAN ID. The FortiGate unit can recognize VLAN IDs and apply security policies to secure network and IPSec VPN traffic between security domains. The FortiGate unit can also apply authentication, protection profiles, and other firewall policy features for network and VPN traffic that is allowed to pass between security domains.

VLANs in NAT/Route mode

Operating in NAT/Route mode, the FortiGate unit functions as a layer-3 device to control the flow of packets between VLANs. The FortiGate unit can also remove VLAN tags from incoming VLAN packets and forward untagged packets to other networks, such as the Internet.

In NAT/Route mode, the FortiGate units support VLANs for constructing VLAN trunks between an IEEE 802.1Q-compliant switch (or router) and the FortiGate units. Normally the FortiGate unit internal interface connects to a VLAN trunk on an internal switch, and the external interface connects to an upstream Internet router untagged. The FortiGate unit can then apply different policies for traffic on each VLAN that connects to the internal interface.

In this configuration, you add VLAN subinterfaces to the FortiGate internal interface that have VLAN IDs that match the VLAN IDs of packets in the VLAN trunk. The FortiGate unit directs packets with VLAN IDs to subinterfaces with matching VLAN IDs.

You can also define VLAN subinterfaces on all FortiGate interfaces. The FortiGate unit can add VLAN tags to packets leaving a VLAN subinterface or remove VLAN tags from incoming packets and add a different VLAN tags to outgoing packets.

Rules for VLAN IDs

In NAT/Route mode, two VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID. However, you can add two or more VLAN subinterfaces with the same VLAN IDs to different physical interfaces. There is no internal connection or link between two VLAN subinterfaces with same VLAN ID. Their relationship is the same as the relationship between any two FortiGate network interfaces.

Rules for VLAN IP addresses

IP addresses of all FortiGate interfaces cannot overlap. That is, the IP addresses of all interfaces must be on different subnets. This rule applies to both physical interfaces and to VLAN subinterfaces.

Note: If you are unable to change your existing configurations to prevent IP overlap, enter the CLI command `config system global and set allow-interface-subnet-overlap enable` to allow IP address overlap. If you enter this command, multiple VLAN interfaces can have an IP address that is part of a subnet used by another interface. This command is recommended for advanced users only.
Figure 45 shows a simplified NAT/Route mode VLAN configuration. In this example, the FortiGate internal interface connects to a VLAN switch using an 802.1Q trunk and is configured with two VLAN subinterfaces (VLAN 100 and VLAN 200). The external interface connects to the Internet. The external interface is not configured with VLAN subinterfaces.

When the VLAN switch receives packets from VLAN 100 and VLAN 200, it applies VLAN tags and forwards the packets to local ports and across the trunk to the FortiGate unit. The FortiGate unit is configured with policies that allow traffic to flow between the VLANs and from the VLANs to the external network.

**Figure 56: FortiGate unit in NAT/Route mode**

Adding VLAN subinterfaces

The VLAN ID of each VLAN subinterface must match the VLAN ID added by the IEEE 802.1Q-compliant router. The VLAN ID can be any number between 1 and 4096. Each VLAN subinterface must also be configured with its own IP address and netmask.

Note: A VLAN must not have the same name as a virtual domain or zone.

You add VLAN subinterfaces to the physical interface that receives VLAN-tagged packets.

**To add a VLAN subinterface in NAT/Route mode**

1. Go to System > Network > Interface.
2. Select Create New to add a VLAN subinterface.
3. Enter a Name to identify the VLAN subinterface.
VLANs in Transparent mode

In Transparent mode, the FortiGate unit can apply firewall policies and services, such as authentication, protection profiles, and other firewall features, to traffic on an IEEE 802.1 VLAN trunk. You can insert the FortiGate unit operating in Transparent mode into the trunk without making changes to your network. In a typical configuration, the FortiGate internal interface accepts VLAN packets on a VLAN trunk from a VLAN switch or router connected to internal VLANs. The FortiGate external interface forwards tagged packets through the trunk to an external VLAN switch or router which could be connected to the Internet. The FortiGate unit can be configured to apply different policies for traffic on each VLAN in the trunk.

For VLAN traffic to be able to pass between the FortiGate Internal and external interface you would add a VLAN subinterface to the internal interface and another VLAN subinterface to the external interface. If these VLAN subinterfaces have the same VLAN IDs, the FortiGate unit applies firewall policies to the traffic on this VLAN. If these VLAN subinterfaces have different VLAN IDs, or if you add more than two VLAN subinterfaces, you can also use firewall policies to control connections between VLANs.

1 Select the physical interface that receives the VLAN packets intended for this VLAN subinterface.
2 Enter the VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface.
3 If you are the super admin, select the virtual domain to add this VLAN subinterface to. Otherwise, you can only create VLAN subinterfaces in your own VDOM.
4 Configure the VLAN subinterface settings as you would for any FortiGate interface.
5 Select OK to save your changes.

The FortiGate unit adds the new VLAN subinterface to the interface that you selected in step 4.

To add firewall policies for VLAN subinterfaces

Once you have added VLAN subinterfaces you can add firewall policies for connections between VLAN subinterfaces or from a VLAN subinterface to a physical interface.

1 Go to Firewall > Address.
2 Select Create New to add firewall addresses that match the source and destination IP addresses of VLAN packets.
3 Go to Firewall > Policy.
4 Create or add firewall policies as required.
If the network uses IEEE 802.1 VLAN tags to segment your network traffic, you can configure a FortiGate unit operating in Transparent mode to provide security for network traffic passing between different VLANs. To support VLAN traffic in Transparent mode, you add virtual domains to the FortiGate unit configuration. A virtual domain consists of two or more VLAN subinterfaces or zones. In a virtual domain, a zone can contain one or more VLAN subinterfaces.

When the FortiGate unit receives a VLAN tagged packet at an interface, the packet is directed to the VLAN subinterface with matching VLAN ID. The VLAN subinterface removes the VLAN tag and assigns a destination interface to the packet based on its destination MAC address. The firewall policies for this source and destination VLAN subinterface pair are applied to the packet. If the packet is accepted by the firewall, the FortiGate unit forwards the packet to the destination VLAN subinterface. The destination VLAN ID is added to the packet by the FortiGate unit and the packet is sent to the VLAN trunk.

**Note:** There is a maximum of 255 interfaces total allowed per VDOM in Transparent mode. This includes VLANs. If no other interfaces are configured for a VDOM, you can configure up to 255 VLANs in that VDOM.

**Figure 57: FortiGate unit with two virtual domains in Transparent mode**

**Figure 58** shows a FortiGate unit operating in Transparent mode and configured with three VLAN subinterfaces. In this configuration the FortiGate unit could be added to this network to provide virus scanning, web content filtering, and other services to each VLAN.
Rules for VLAN IDs

In Transparent mode two VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID. However, you can add two or more VLAN subinterfaces with the same VLAN IDs to different physical interfaces. There is no internal connection or link between two VLAN subinterfaces with the same VLAN ID. Their relationship is the same as the relationship between any two FortiGate network interfaces.

Note: There is a maximum of 255 VLANs allowed per interface in Transparent mode.

Transparent mode virtual domains and VLANs

VLAN subinterfaces are added to and associated with virtual domains. By default the FortiGate configuration includes one virtual domain, named root, and you can add as many VLAN subinterfaces as you require to this virtual domain.

You can add more virtual domains if you want to separate groups of VLAN subinterfaces into virtual domains. For information on adding and configuring virtual domains, see “Using virtual domains” on page 71.
To add a VLAN subinterface in Transparent mode

The VLAN ID of each VLAN subinterface must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch. The VLAN ID can be any number between 1 and 4096. You add VLAN subinterfaces to the physical interface that receives VLAN-tagged packets.

**Note:** A VLAN must not have the same name as a virtual domain or zone.

1. Go to **System > Network > Interface**.
2. Select Create New to add a VLAN subinterface.
3. Enter a Name to identify the VLAN subinterface.
4. Select the physical interface that receives the VLAN packets intended for this VLAN subinterface.
5. Enter the VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface.
6. Select which virtual domain to add this VLAN subinterface to.
   See “Using virtual domains” on page 71 for information about virtual domains.
7. Configure the administrative access, and log settings as you would for any FortiGate interface.
   See “Interface settings” on page 83 for more descriptions of these settings.
8. Select OK to save your changes.
   The FortiGate unit adds the new subinterface to the interface that you selected.
9. Select Bring up to start the VLAN subinterface.

To add firewall policies for VLAN subinterfaces

Once you have added VLAN subinterfaces you can add firewall policies for connections between VLAN subinterfaces or from a VLAN subinterface to a physical interface.

1. Go to **Firewall > Address**.
2. Select Create New to add firewall addresses that match the source and destination IP addresses of VLAN packets.
   See “About firewall addresses” on page 289.
3. Go to **Firewall > Policy**.
4. Add firewall policies as required.
Figure 59: FortiGate unit with two virtual domains in Transparent mode

Figure 60 shows a FortiGate unit operating in Transparent mode and configured with three VLAN subinterfaces. In this configuration the FortiGate unit could be added to this network to provide virus scanning, web content filtering, and other services to each VLAN.

Figure 60: FortiGate unit in Transparent mode
Troubleshooting ARP Issues

Address Resolution Protocol (ARP) traffic is vital to communication on a network and is enabled on FortiGate interfaces by default. Normally you want ARP packets to pass through the FortiGate unit, especially if it is sitting between a client and a server or between a client and a router.

Duplicate ARP packets

ARP traffic can cause problems, especially in Transparent mode where ARP packets arriving on one interface are sent to all other interfaces, including VLAN subinterfaces. Some Layer 2 switches become unstable when they detect the same MAC address originating on more than one switch interface or from more than one VLAN. This instability can occur if the Layer 2 switch does not maintain separate MAC address tables for each VLAN. Unstable switches may reset causing network traffic to slow down.

ARP Forwarding

One solution to this problem is to enable ARP forwarding. It can be enabled in the GUI or CLI. In the GUI, go to System > Config > Operation and select ARP Forwarding. For details on the CLI, see the FortiGate CLI Reference.

When enabled, the Fortigate unit allows duplicate ARP packets resolving the previous delivery problems. However, this also opens up your network to potential hacking attempts that spoof packets.

For more secure solutions, see the FortiGate VLANs and VDOMs Guide.

FortiGate IPv6 support

You can assign both an IPv4 and an IPv6 address to any interface on a FortiGate unit. The interface functions as two interfaces, one for IPv4-addressed packets and another for IPv6-addressed packets.

FortiGate units support IPv6 routing, tunneling, firewall policies and IPSec VPN. You must use the Command Line Interface (CLI) to configure your FortiGate unit for IPv6 operation. IPv6 configuration is not supported in the web-based manager.

See the FortiGate IPv6 Support Technical Note available from the Fortinet Knowledge Center.

See the FortiGate CLI Reference for information on the following commands:
Table 4: IPv6 CLI commands

<table>
<thead>
<tr>
<th>Feature</th>
<th>CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface configuration, including periodic router advertisements</td>
<td>config system interface&lt;br&gt;See the keywords beginning with &quot;ip6&quot;.&lt;br&gt;config ip6-prefix-list</td>
</tr>
<tr>
<td>Static routing</td>
<td>config router static6</td>
</tr>
<tr>
<td>IPv6 tunneling</td>
<td>config system ipv6_tunnel</td>
</tr>
<tr>
<td>Firewall</td>
<td>config firewall address6&lt;br&gt;config firewall addrgrp6&lt;br&gt;config firewall policy6</td>
</tr>
<tr>
<td>IPv6 IPSec VPNs</td>
<td>config vpn ipsec</td>
</tr>
<tr>
<td>Execute</td>
<td>execute ping6</td>
</tr>
</tbody>
</table>
System Wireless

This section describes how to configure the Wireless LAN interfaces on FortiWiFi units.

This section describes:
- About FortiWiFi-50B power over ethernet (POE)
- FortiWiFi wireless interfaces
- Channel assignments
- FortiWiFi-50B, 60A, 60AM, and 60B system wireless settings
- FortiWiFi-60 System wireless settings
- Wireless MAC Filter
- Wireless Monitor

About FortiWiFi-50B power over ethernet (POE)

You can use power over ethernet (POE) technology to provide power and network connectivity to FortiWiFi-50B units. The FortiWiFi-50B unit is a powered device (PD) that supports the IEEE 802.3af POE standard.

Connect the FortiWiFi-50B wan1 interface to power sourcing equipment (PSE) such as a POE ethernet switch to provide power and a network connection for the FortiWiFi-50B unit. Using POE to provide power to a FortiWiFi-50B unit makes it easier to deploy the unit in a location where an AC power connection is not available.

FortiWiFi wireless interfaces

FortiWiFi-50B, 60A, 60AM, and 60B units support up to four wireless interfaces and four different SSIDs. Each wireless interface should have a different SSID and each wireless interface can have different security settings. For information about how to add wireless interfaces, see “Adding a wireless interface to a FortiWiFi-50B, 60A, 60AM, and 60B unit” on page 122.

You can configure the FortiWiFi unit to:
- Provide an access point that clients with wireless network cards can connect to. This is called Access Point mode, which is the default mode. FortiWiFi-50B, 60A, 60AM, and 60B wireless access points can include up to 4 wireless interfaces.

or

- Connect the FortiWiFi unit to another wireless networks. This is called Client mode. FortiWiFi-50B, 60A, 60AM, and 60B units operating in client mode can also include up to 4 wireless interfaces.

FortiWiFi units support the following wireless network standards:
• IEEE 802.11a (5-GHz Band) (not supported by FortiWiFi-50B units)
• IEEE 802.11b (2.4-GHz Band)
• IEEE 802.11g (2.4-GHz Band)
• WEP64 and WEP128 Wired Equivalent Privacy (WEP)
• Wi-Fi Protected Access (WPA), WPA2 and WPA2 Auto using pre-shared keys or RADIUS servers

Channel assignments

The following tables list the channel assignments for wireless LANs.
The following sections list the channel assignments for wireless LANs.

• IEEE 802.11a channel numbers
• IEEE 802.11b channel numbers
• IEEE 802.11g channel numbers

IEEE 802.11a channel numbers

Table 5 lists IEEE 802.11a channels supported for FortiWiFi products that support the IEEE 802.11a wireless standard. 802.11a is not supported by FortiWiFi-50B units.

All channels are restricted to indoor usage except the Americas, which allows for indoor and outdoor use on channels 52 through 64 in the United States.

Table 5: IEEE 802.11a (5-GHz Band) channel numbers

<table>
<thead>
<tr>
<th>Channel number</th>
<th>Frequency (MHz)</th>
<th>Americas</th>
<th>Europe</th>
<th>Taiwan</th>
<th>Singapore</th>
<th>Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>5170</td>
<td>–</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>36</td>
<td>5180</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>38</td>
<td>5190</td>
<td>–</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>40</td>
<td>5200</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>42</td>
<td>5210</td>
<td>–</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>44</td>
<td>5220</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>46</td>
<td>5230</td>
<td>–</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>48</td>
<td>5240</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>52</td>
<td>5260</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>56</td>
<td>5280</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>60</td>
<td>5300</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>64</td>
<td>5320</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>149</td>
<td>5745</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>153</td>
<td>5765</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>157</td>
<td>5785</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>161</td>
<td>5805</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>
IEEE 802.11b channel numbers

Table 6 lists IEEE 802.11b channels supported for FortiWiFi products that support the IEEE 802.11b wireless standard. All FortiWiFi products support 802.11b.

Mexico is included in the Americas regulatory domain. Channels 1 through 8 are for indoor use only. Channels 9 through 11 can be used indoors and outdoors. You must make sure that the channel number complies with the regulatory standards of Mexico.

<table>
<thead>
<tr>
<th>Channel number</th>
<th>Frequency (MHz)</th>
<th>Americas</th>
<th>EMEA</th>
<th>Israel</th>
<th>Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2412</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>2417</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>2422</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>2427</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>5</td>
<td>2432</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>6</td>
<td>2437</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7</td>
<td>2442</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>8</td>
<td>2447</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>9</td>
<td>2452</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>10</td>
<td>2457</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>11</td>
<td>2462</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>12</td>
<td>2467</td>
<td>–</td>
<td>X</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>13</td>
<td>2472</td>
<td>–</td>
<td>X</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>14</td>
<td>2484</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>X</td>
</tr>
</tbody>
</table>

IEEE 802.11g channel numbers

Table 7 lists IEEE 802.11b channels supported for FortiWiFi products that support the IEEE 802.11g wireless standard. All FortiWiFi products support 802.11g.
FortiWiFi-50B, 60A, 60AM, and 60B system wireless settings

Go to **System > Wireless > Settings** to configure wireless settings. You can configure wireless settings for the FortiWiFi-50B, 60A, 60AM, 60B unit and for the wireless interfaces added to the unit. Most wireless configuration settings are only available in access point mode.

The default wireless configuration includes one wireless interface, called wlan. If you are operating your FortiWiFi unit in access point mode, you can add up to three more wireless interfaces (for a total of 4) using the procedure described in “Adding a wireless interface to a FortiWiFi-50B, 60A, 60AM, and 60B unit” on page 122.

**Note:** All wireless interfaces have the same wireless parameters. This means that all wireless interfaces have the same setting for band, geography, channel, Tx power, and beacon interval.

Figure 61 shows a sample FortiWiFi-50B wireless configuration that includes three wireless interfaces (wlan-vlan2, wlan-vlan3, and wlan-vlan4) added to the wlan interface using the procedure “Adding a wireless interface to a FortiWiFi-50B, 60A, 60AM, and 60B unit” on page 122.

### Table 7: IEEE 802.11g (2.4-GHz Band) channel numbers

<table>
<thead>
<tr>
<th>Channel number</th>
<th>Frequency (MHz)</th>
<th>Americas</th>
<th>EMEA</th>
<th>Israel</th>
<th>Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CCK</td>
<td>ODFM</td>
<td>CCK</td>
<td>ODFM</td>
</tr>
<tr>
<td>1</td>
<td>2412</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>2417</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>3</td>
<td>2422</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>4</td>
<td>2427</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>5</td>
<td>2432</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>6</td>
<td>2437</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7</td>
<td>2442</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>8</td>
<td>2447</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>9</td>
<td>2452</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>10</td>
<td>2457</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>11</td>
<td>2462</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>12</td>
<td>2467</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>13</td>
<td>2472</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>14</td>
<td>2484</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>X</td>
</tr>
</tbody>
</table>

**Note:** All wireless interfaces have the same wireless parameters. This means that all wireless interfaces have the same setting for band, geography, channel, Tx power, and beacon interval.
Operation Mode
The current operating mode. Select Change to change the operation mode.
Access Point mode makes the FortiWiFi unit act as a wireless access point to which multiple clients can connect. Client mode configures the FortiWiFi unit to connect to another wireless network as a client.

Band
Select the wireless frequency band you want to use.
- For FortiWiFi-50B units you can select 802.11b, and 802.11g.
- For FortiWiFi-60A, 60AM, and 60B units you can select from: 802.11a, 802.11b, and 802.11g.

Geography
Select your country or region. This determines which channels are available. You can select Americas, EMEA, Israel, or Japan. If you are in any other region, select World.

Channel
Select a channel for your wireless network or select Auto. Clients of the wireless network must configure their computers to use this channel. The channels that you can select depend on the Geography setting. See “Channel assignments” on page 118 for channel information.

Tx Power
Set the transmitter power level. The default power level is the maximum of 17 dBm.

Beacon Interval
Set the interval between beacon packets. Access Points broadcast Beacons or Traffic Indication Messages (TIM) to synchronize wireless networks. In an environment with high interference, decreasing the Beacon Interval might improve network performance. In a location with few wireless nodes, you can increase this value.

Wireless interface list

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>SSID</th>
<th>SSID Broadcast</th>
<th>Security Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan</td>
<td>00:0C:29:CA:AF:01</td>
<td>wifi50b-vlan1</td>
<td></td>
<td>WEP64 (Key Index[1])</td>
</tr>
<tr>
<td>wlan-vlan2</td>
<td>00:0C:29:CA:AF:02</td>
<td>wifi50b-vlan2</td>
<td></td>
<td>WPA2</td>
</tr>
<tr>
<td>wlan-vlan3</td>
<td>00:0C:29:CA:AF:03</td>
<td>wifi50b-vlan3</td>
<td></td>
<td>WPA2</td>
</tr>
<tr>
<td>wlan-vlan4</td>
<td>00:0C:29:CA:AF:04</td>
<td>wifi50b-vlan4</td>
<td></td>
<td>WIP128 (Key Index[4])</td>
</tr>
</tbody>
</table>

Wireless interface list

**Interface**
The name of the wireless interface. Select the name to edit the interface. The default configuration includes the wlan interface. To add more wireless interfaces, see “Adding a wireless interface to a FortiWiFi-50B, 60A, 60AM, and 60B unit” on page 122.

**MAC Address**
The MAC address of the Wireless interface.

**SSID**
The wireless service set identifier (SSID) or network name for the wireless interface. Clients who want to use the wireless interface must configure their computers to connect to the network that broadcasts this network name.
Adding a wireless interface to a FortiWiFi-50B, 60A, 60AM, and 60B unit

On FortiWiFi-50B, 60A, 60AM, and 60B units, you can use the following steps to support up to four SSIDs by adding up to three wireless interfaces (for a total of four wireless interfaces). Each wireless interface should have a different SSID and each wireless interface can have different security settings.

Note: All wireless interfaces have the same wireless parameters. This means that all wireless interfaces have the same setting for band, geography, channel, Tx power, and beacon interval.

1. Go to System > Network > Interface.
2. Select Create New.
3. In the Name field, enter a name for the wireless interface.
   The interface name must not be the same as any other interface, zone or VDOM.
4. Configure interface options as required.
   Interface options are described in “Interface settings” on page 83.
5. From the Type list, select Wireless.
6. In the Wireless Settings section, enter the following information:

   **Figure 62: Wireless interface settings (WEP64)**

<table>
<thead>
<tr>
<th>Wireless Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>Forti50B-vlan1</td>
</tr>
<tr>
<td>SSID Broadcast</td>
<td>✓</td>
</tr>
<tr>
<td>Security Mode</td>
<td>WEP64</td>
</tr>
<tr>
<td>Key</td>
<td>✽</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>2346</td>
</tr>
<tr>
<td>Fragmentation</td>
<td>2346</td>
</tr>
</tbody>
</table>

   **Figure 63: Wireless interface settings (WAP2)**

<table>
<thead>
<tr>
<th>Wireless Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>Forti50B-vlan12</td>
</tr>
<tr>
<td>SSID Broadcast</td>
<td>✓</td>
</tr>
<tr>
<td>Security Mode</td>
<td>WPA2</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>TKIP</td>
</tr>
<tr>
<td>Authentication</td>
<td>Pre-shared Key</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>2346</td>
</tr>
<tr>
<td>Fragmentation</td>
<td>2346</td>
</tr>
</tbody>
</table>

**SSID Broadcast** Green checkmark icon indicates that the wireless interface broadcasts its SSID. Broadcasting the SSID makes it possible for clients to connect to your wireless network without first knowing the SSID.

**Security Mode** Displays information about the security mode as defined when you configure the wireless interface. See “Adding a wireless interface to a FortiWiFi-50B, 60A, 60AM, and 60B unit” on page 122. For WEP64 and WEP128 the security mode includes a key index which just indicates that a key has been defined for this wireless interface.
SSID

Enter the wireless service set identifier (SSID) or network name for this wireless interface. Users who want to use the wireless network must configure their computers to connect to the network that broadcasts this network name.

SSID Broadcast

Select if you want the wireless interface to broadcast its SSID. Broadcasting the SSID makes it possible for clients to connect to your wireless network without first knowing the SSID. Your wireless network may be more secure if you do not broadcast the SSID because clients that do not know the SSID are less likely to find the network.

Security mode

Select the security mode used by the wireless interface. Wireless clients must use the same security mode to be able to connect to this wireless interface. To increase wireless network security, select the most secure security mode that your wireless clients can use.

- None to provide no security.
- WEP64 to use 64-bit web equivalent privacy (WEP), select. To use WEP64 you must enter a Key containing 10 hexadecimal digits (0-9 a-f). All wireless clients must use the same key.
- WEP128 to use 128-bit WEP. To use WEP128 you must enter a Key containing 26 hexadecimal digits (0-9 a-f). All wireless clients must use the same key.
- WPA to use basic Wi-Fi protected access (WPA) security. To use WPA you must select a data encryption method. You must also enter a pre-shared key containing at least 8 characters or select a RADIUS server. All wireless clients must use the same pre-shared key and data encryption method. If you select a RADIUS server the wireless clients must have accounts on the RADIUS server.
- WPA2 to use WPA2 security. WPA2 provides more security features and is more secure than WPA. To use WPA2 you must select a data encryption method and enter a pre-shared key containing at least 8 characters. All wireless clients must use the same pre-shared key and data encryption method. If you select a RADIUS server the wireless clients must have accounts on the RADIUS server.
- WPA2 Auto provides the same security features as WPA2. However, WPA2 Auto also accepts wireless clients using WPA security. To use WPA2 Auto you must select a data encryption method You must also enter a pre-shared key containing at least 8 characters or select a RADIUS server. All wireless clients must use the same pre-shared key and data encryption method. If you select a RADIUS server the wireless clients must have accounts on the RADIUS server.

WPA2 and WPA2 Auto are only available in Access Point mode.

Key

Enter the key required for WEP64 or WEP128.

Data Encryption

Select a data encryption method to be used by WPA, WPA2, or WPA Auto. Select TKIP to use the Temporal Key Integrity Protocol (TKIP). Select AES to use advanced encryption standard (AES) encryption. AES is considered more secure than TKIP. Some implementations of WPA may not support AES.

Pre-shared Key

Enter the pre-shared key used by WPA, WPA2, or WPA2 Auto.

RADIUS Server

Select to use WPA Radius or WPA2 Radius security. You can use WPA or WPA2 Radius security to integrate your wireless network configuration with a RADIUS or Windows AD server. Select a RADIUS server name from the list. The Radius server must be configured in User > RADIUS. For more information, see "RADIUS servers" on page 381.
RTS Threshold  The Request to Send (RTS) threshold sets the time the unit waits for Clear to Send (CTS) acknowledgement from another wireless device.

Fragmentation Threshold  Set the maximum size of a data packet before it is broken into two or more packets. Reducing the threshold can improve performance in environments that have high interference.

7  Select OK.

FortiWiFi-60 System wireless settings

Go to System > Wireless > Settings to configure wireless settings.

Figure 64: Configuring wireless parameters

<table>
<thead>
<tr>
<th>Wireless Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
</tr>
<tr>
<td>Operation Mode</td>
</tr>
<tr>
<td>Geography</td>
</tr>
<tr>
<td>SSID</td>
</tr>
<tr>
<td>SSID Broadcast</td>
</tr>
<tr>
<td>RTS Threshold</td>
</tr>
<tr>
<td>Fragmentation Threshold</td>
</tr>
<tr>
<td>Beacon Interval</td>
</tr>
<tr>
<td>Tx Power</td>
</tr>
</tbody>
</table>

MAC Address  The MAC address of the Wireless interface.

Operation Mode  The current operating mode. Select Change to change it. Access Point mode makes the FortiWiFi unit act as a wireless access point to which multiple clients can connect. Client mode configures the unit to connect to another wireless network as a client.

Geography  Select your country or region. This determines which channels are available. You can select Americas, EMEA, Israel, or Japan. If you are in any other region, select World.

Channel  Select a channel for your FortiWiFi wireless network. Clients of the wireless network must configure their computers to use this channel. The channels that you can select depend on the Geography setting. See “Channel assignments” on page 118 for channel information.

SSID  Enter the wireless service set identifier (SSID) or network name for the FortiWiFi-60 unit. Clients who want to use the wireless network must configure their computers to connect to the network that broadcasts this network name.

SSID Broadcast  Select Enable if you want the FortiWiFi-60 unit to broadcast the SSID. Broadcasting the SSID makes it possible for clients to connect to your wireless network without first knowing the SSID.

Security mode  To use WEP, select WEP64 or WEP128. To use WPA (available in Access Point mode only), select WPA Pre-shared Key or WPA_Radius. Clients of the FortiWiFi wireless network must configure their computers with the same settings.
Go to System > Wireless > MAC Filter to allow or deny wireless access to wireless clients based on the MAC address of the client wireless cards. For a given wireless interface you can add MAC addresses and select allow or deny.

Select allow to only allow wireless access to the listed MAC addresses. Select deny to stop the listed MAC addresses from accessing the wireless interface. If you select deny only the listed MAC addresses are denied access. All other MAC addresses can access the wireless interface.

- FortiWiFi-50B, 60A, 60AM, and 60B Wireless MAC Filter list
- FortiWiFi-60 Wireless MAC Filter

FortiWiFi-50B, 60A, 60AM, and 60B Wireless MAC Filter list

You can add multiple wireless interfaces to a FortiWiFi-50B, 60A, 60AM, and 60B unit. From the MAC filter list you can select the edit icon for a wireless interface to configure the MAC filter list for that wireless interface.

**Figure 65: FortiWiFi-50B, 60A, 60AM, and 60B wireless MAC filter list**

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Addresses</th>
<th>List Access</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan</td>
<td>Deny</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wlan+vlan1</td>
<td>Allow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wlan+vlan3</td>
<td>Deny</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wlan+vlan4</td>
<td>Deny</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Wireless MAC filter interface list**

**Interface**
The name of the wireless interface.
MAC address  The list of MAC addresses in the MAC filter list for the wireless interface.

List Access  Allow or deny access to the listed MAC addresses for the wireless interface.

Enable  Select to enable the MAC filter list for the wireless interface.

Edit icon  Edit the MAC address list for an interface.

**Figure 66: FortiWiFi-50B, 60A, 60AM, and 60B wireless interface MAC filter**

<table>
<thead>
<tr>
<th>List Access</th>
<th>Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td></td>
</tr>
<tr>
<td>Address 01:CD:AB:CA:AF:D3</td>
<td></td>
</tr>
<tr>
<td>Address 03:CL:AA:CA:AF:D3</td>
<td></td>
</tr>
<tr>
<td>Address 05:CL:AA:CA:AF:D3</td>
<td></td>
</tr>
</tbody>
</table>

**Edit the MAC filter list for a wireless interface**

**List Access**  Select whether to allow or deny the addresses in the MAC Address list from accessing the wireless network.

**MAC Address**  Enter the MAC address to add to the list.

**Add**  Add the entered MAC address to the list.

**Remove**  Select one or more MAC addresses in the list and select Remove to deleted the MAC addresses from the list.

**OK**  Select OK to save your changes.

**FortiWiFi-60 Wireless MAC Filter**

**Figure 67: FortiWiFi-60 wireless MAC filter**
Wireless Monitor

Go to System > Wireless > Monitor to see who is connected to your wireless LAN. This feature is available only if you are operating the wireless interface in WPA security mode.

Figure 68: FortiWiFi-50B, 60A, 60AM, and 60B wireless monitor

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Frequency</th>
<th>Signal Strength (dBm)</th>
<th>Noise (dBm)</th>
<th>S/N (dB)</th>
<th>Rx (Bytes)</th>
<th>Tx (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan0</td>
<td>2.432GHz</td>
<td>-95</td>
<td>-95</td>
<td>0</td>
<td>0</td>
<td>60</td>
</tr>
<tr>
<td>wlan-vlan2</td>
<td>2.432GHz</td>
<td>-95</td>
<td>-95</td>
<td>0</td>
<td>0</td>
<td>60</td>
</tr>
<tr>
<td>wlan-vlan3</td>
<td>2.432GHz</td>
<td>-95</td>
<td>-95</td>
<td>0</td>
<td>0</td>
<td>60</td>
</tr>
<tr>
<td>wlan-vlan4</td>
<td>2.432GHz</td>
<td>-95</td>
<td>-95</td>
<td>0</td>
<td>0</td>
<td>60</td>
</tr>
</tbody>
</table>

Clients: 0

Figure 69: FortiWiFi-60 wireless monitor

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0e:89:8e:75:df</td>
<td>10.10.00.2</td>
<td></td>
</tr>
<tr>
<td>00:0e:89:04:62:0a</td>
<td>10.10.00.4</td>
<td></td>
</tr>
<tr>
<td>00:0e:89:46:45:12</td>
<td>10.10.00.5</td>
<td></td>
</tr>
</tbody>
</table>

Statistics

Statistical information about wireless performance for each wireless interface. Statistics are available for FortiWiFi-50B, 60A, 60AM, and 60B units.

AP Name

The name of the wireless interface.

Frequency

The frequency that the wireless interface is operating with. Should be around 5-GHz for 802.11a interfaces and around 2.4-GHz for 802.11b and 802.11g networks.

Signal Strength (dBm)

The strength of the signal from the client.

Noise (dBm)

The received noise level.

S/N (dB)

The signal-to-noise ratio in deciBels calculated from signal strength and noise level.
<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx (KBytes)</td>
<td>The amount of data in kilobytes received this session.</td>
</tr>
<tr>
<td>Tx (KBytes)</td>
<td>The amount of data in kilobytes sent this session.</td>
</tr>
<tr>
<td>Clients</td>
<td>The number of clients connected to the WLAN and information about each of them. Clients information is available for FortiWiFi-50B, 60A, 60AM, and 60B units.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the connected wireless client.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the connected wireless client.</td>
</tr>
<tr>
<td>AP Name</td>
<td>The name of the wireless interface that the client is connected to.</td>
</tr>
<tr>
<td>ID</td>
<td>The user ID of the connected client using WPA RADIUS security mode. This field is blank if the client uses WPA Pre-Shared Key or WEP security modes. Available on FortiWiFi-60 units only.</td>
</tr>
</tbody>
</table>
System DHCP

This section describes how to use DHCP to provide convenient automatic network configuration for your clients.

This section describes:

- FortiGate DHCP servers and relays
- Configuring DHCP services
- Viewing address leases

FortiGate DHCP servers and relays

The DHCP protocol enables hosts to automatically obtain their assigned IP address. Optionally, they can also obtain default gateway and DNS server settings. A FortiGate interface or VLAN subinterface can provide the following DHCP services:

- Regular DHCP servers for regular Ethernet connections
- IPSec DHCP servers for IPSec (VPN) connections
- DHCP relay for regular Ethernet or IPSec (VPN) connections

An interface cannot provide both a server and a relay for connections of the same type (regular or IPSec).

Note: You can configure a Regular DHCP server on an interface only if the interface has a static IP address. You can configure an IPSec DHCP server on an interface that has either a static or a dynamic IP address.

You can configure one or more DHCP servers on any FortiGate interface. A DHCP server dynamically assigns IP addresses to hosts on the network connected to the interface. The host computers must be configured to obtain their IP addresses using DHCP.

If an interface is connected to multiple networks via routers, you can add a DHCP server for each network. The IP range of each DHCP server must match the network address range. The routers must be configured for DHCP relay.

To configure a DHCP server, see “Configuring a DHCP server” on page 131.

You can configure a FortiGate interface as a DHCP relay. The interface forwards DHCP requests from DHCP clients to an external DHCP server and returns the responses to the DHCP clients. The DHCP server must have appropriate routing so that its response packets to the DHCP clients arrive at the FortiGate unit.

To configure a DHCP relay see “Configuring an interface as a DHCP relay agent” on page 131.

DHCP services can also be configured through the Command Line Interface (CLI). See the FortiGate CLI Reference for more information.
Configuring DHCP services

Go to **System > DHCP > Service** to configure DHCP services. On each FortiGate interface, you can configure a DHCP relay and add DHCP servers as needed.

On FortiGate models 50 and 60, a DHCP server is configured, by default, on the Internal interface, as follows:

- **IP Range**: 192.168.1.110 to 192.168.1.210
- **Netmask**: 255.255.255.0
- **Default gateway**: 192.168.1.99
- **Lease time**: 7 days
- **DNS Server 1**: 192.168.1.99

You can disable or change this default DHCP Server configuration.

These settings are appropriate for the default Internal interface IP address of 192.168.1.99. If you change this address to a different network, you need to change the DHCP server settings to match.

**Figure 70: DHCP service list - FortiGate-200A shown**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Server Name/Relay IP</th>
<th>Type</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>Relay</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dmz1</td>
<td>Relay</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dmz2</td>
<td>Relay</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wan1</td>
<td>Relay</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Servers</td>
<td>Serv1</td>
<td>Regular</td>
</tr>
<tr>
<td>wan2</td>
<td>Relay</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Servers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Interface**: List of FortiGate interfaces. Expand each listed interface to view the Relay and Servers.

**Server Name/Relay IP**: Name of FortiGate DHCP server or IP address of DHCP server accessed by relay.

**Type**: Type of DHCP relay or server: Regular or IPSec.

**Enable**: Green check mark icon indicates that server or relay is enabled.

**Add DHCP Server icon**: Configure and add a DHCP server for this interface.

**Edit**: Edit DHCP relay or server configuration.

**Delete**: Delete a DHCP server.
Configuring an interface as a DHCP relay agent

Go to System > DHCP > Service and select an edit icon to view or modify the DHCP relay configuration for an interface.

Figure 71: Edit DHCP relay settings for an interface

| Interface Name | The name of the interface. |
| Enable         | Enable the DHCP relay agent on this interface. |
| Type           | Select the type of DHCP service required. |
|                | Regular Configure the interface to be a DHCP relay agent for computers on the network connected to this interface. |
|                | IPSEC Configure the interface to be a DHCP relay agent only for remote VPN clients with an IPSec VPN connection to this interface. |
| DHCP Server IP | Enter the IP address of the DHCP server that will answer DHCP requests from computers on the network connected to the interface. |

Configuring a DHCP server

Go to System > DHCP > Service to configure a DHCP server on an interface. Select Add a DHCP Server beside the interface or select Edit beside an existing DHCP server to change its settings.

Figure 72: DHCP Server options

<table>
<thead>
<tr>
<th>Name</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Regular</td>
</tr>
<tr>
<td>IP Range</td>
<td>-</td>
</tr>
<tr>
<td>Network Mask</td>
<td></td>
</tr>
<tr>
<td>Default Gateway</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td></td>
</tr>
<tr>
<td>Lease Time</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Option 1</td>
<td></td>
</tr>
<tr>
<td>Option 2</td>
<td></td>
</tr>
<tr>
<td>Option 3</td>
<td></td>
</tr>
<tr>
<td>DNS Server 1</td>
<td></td>
</tr>
<tr>
<td>DNS Server 2</td>
<td></td>
</tr>
<tr>
<td>DNS Server 3</td>
<td></td>
</tr>
<tr>
<td>WINS Server 1</td>
<td></td>
</tr>
<tr>
<td>WINS Server 2</td>
<td></td>
</tr>
<tr>
<td>Exclude Ranges</td>
<td>Add</td>
</tr>
<tr>
<td>Starting IP</td>
<td>End IP</td>
</tr>
<tr>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td>Cancel</td>
</tr>
</tbody>
</table>
Viewing address leases

Go to System > DHCP > Address Leases to view the IP addresses that the DHCP servers have assigned and the corresponding client MAC addresses.

Figure 73: Address leases list

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP</th>
<th>MAC</th>
<th>Expire</th>
</tr>
</thead>
</table>

Interface
Select interface for which to list leases.

Refresh
Select Refresh to update Address leases list.

IP
The assigned IP address.
MAC  The MAC address of the device to which the IP address is assigned.
Expire  Expiry date and time of the DHCP lease.

Reserving IP addresses for specific clients

You can reserve an IP address for a specific client identified by the client device MAC address and the connection type, regular Ethernet or IPSec. The DHCP server always assigns the reserved address to that client. You can define up to 50 reserved addresses.

Use the CLI `system dhcp reserved-address` command. For more information, see the *FortiGate CLI Reference*. 
System Config

This section describes the configuration of several non-network features, such as HA, SNMP, custom replacement messages, and VDOM operation.

This section describes:

- HA
- SNMP
- Replacement messages
- Operation mode and VDOM management access

HA, SNMP and Replacement messages are part of the global configuration of the FortiGate unit. Changing operation mode applies to each individual VDOM.

HA

FortiGate high availability (HA) provides a solution for two key requirements of critical enterprise networking components: enhanced reliability and increased performance. This section contains a brief description of HA web-based manager configuration options, the HA cluster members list, HA statistics, and disconnecting cluster members.

For complete information about how to configure and operate FortiGate HA clusters see the FortiGate HA Overview, the FortiGate HA Guide, and the Fortinet Knowledge Center.

Note: For FortiOS v3.0 MR2 and previous versions, this HA section included extensive detail about HA. Starting with FortiOS v3.0 MR3 you should refer to the FortiGate HA Overview or the FortiGate HA Guide for the full HA story.

HA is not available on FortiGate models 50A, 50AM, and 224B. HA is available on all other FortiGate models, including the FortiGate-50B.

The following topics are included in this section:

- HA options
- Cluster members list
- Viewing HA statistics
- Changing subordinate unit host name and device priority
- Disconnecting a cluster unit from a cluster

HA options

Configure HA options so that a FortiGate unit can join a cluster or to change the configuration of an operating cluster or cluster member.

To configure HA options so that a FortiGate unit can join an HA cluster, go to System > Config > HA.
If HA is already enabled, go to **System > Config > HA** to display the cluster members list. Select edit for the FortiGate unit with Role of master (also called the primary unit). When you edit the HA configuration of the primary unit, all changes are synchronized to the other cluster units.

**Figure 74: FortiGate-1000AFA2 unit HA configuration**

[Image of HA configuration settings]

**Note:** If your FortiGate cluster uses virtual domains, you are configuring HA virtual clustering. Most virtual cluster HA options are the same as normal HA options. However, virtual clusters include VDOM partitioning options. Other differences between configuration options for regular HA and for virtual clustering HA are described below and in the *FortiGate HA Overview* and the *FortiGate HA Guide*.

To configure HA options for a FortiGate unit with virtual domains enabled, log in as the global admin administrator and go to **System > Config > HA**.
Figure 75: FortiGate-5001SX HA virtual cluster configuration

**Mode**

Select an HA mode for the cluster or return the FortiGate units in the cluster to standalone mode. When configuring a cluster, you must set all members of the HA cluster to the same HA mode. You can select Standalone (to disable HA), Active-Passive, or Active-Active. If virtual domains are enabled you can select Active-Passive or Standalone.

**Device Priority**

Optionally set the device priority of the cluster unit. Each cluster unit can have a different device priority. During HA negotiation, the unit with the highest device priority usually becomes the primary unit.

In a virtual cluster configuration, each cluster unit can have two device priorities, one for each virtual cluster. During HA negotiation, the unit with the highest device priority in a virtual cluster becomes the primary unit for that virtual cluster.

Changes to the device priority are not synchronized. You can accept the default device priority when first configuring a cluster. When the cluster is operating you can change the device priority for different cluster units as required.
Group Name  Add a name to identify the cluster. The maximum group name length is 7 characters. The group name must be the same for all cluster units before the cluster units can form a cluster. After a cluster is operating you can change the group name. The group name change is synchronized to all cluster units.

The default group name is FGT-HA. You can accept the default group name when first configuring a cluster. When the cluster is operating you can change the group name if required. Two clusters on the same network cannot have the same group name.

Password  Add a password to identify the cluster. The maximum password length is 15 characters. The password must be the same for all cluster units before the cluster units can form a cluster.

The default is no password. You can accept the default when first configuring a cluster. When the cluster is operating you can add a password if required. Two clusters on the same network must have different passwords.

Enable Session pickup  Enable session pickup so that if the primary unit fails, all sessions are picked up by the cluster unit that becomes the new primary unit.

Session pickup is disabled by default. You can accept the default setting for session pickup and then chose to enable session pickup after the cluster is operating.

Port Monitor  Enable or disable monitoring FortiGate interfaces to verify that the monitored interfaces are functioning properly and connected to their networks.

If a monitored interface fails or is disconnected from its network the interface leaves the cluster and a link failover occurs. The link failover causes the cluster to reroute the traffic being processed by that interface to the same interface of another cluster unit that still has a connection to the network. This other cluster unit becomes the new primary unit.

Port monitoring is disabled by default. Leave port monitoring disabled until the cluster is operating and then only enable port monitoring for connected interfaces.

You can monitor up to 16 interfaces. This limit only applies to FortiGate units with more than 16 physical interfaces.

Heartbeat Interface  Enable or disable HA heartbeat communication for each interface in the cluster and set the heartbeat interface priority. The heartbeat interface with the highest priority processes all heartbeat traffic. If two or more heartbeat interfaces have the same priority, the heartbeat interface that is highest in the interface list processes all heartbeat traffic.

The default heartbeat interface configuration is different for each FortiGate but usually sets the priority of two heartbeat interfaces to 50.

You can accept the default heartbeat interface configuration if one or both of the default heartbeat interfaces are connected.

The heartbeat interface priority range is 0 to 512. The default priority when you select a new heartbeat interface is 0.

You must select at least one heartbeat interface. If heartbeat communication is interrupted the cluster stops processing traffic. For more information about configuring heartbeat interfaces see the FortiGate HA Guide.

You can select up to 8 heartbeat interfaces. This limit only applies to FortiGate units with more than 8 physical interfaces.

VDOM partitioning  If you are configuring virtual clustering you can select the virtual domains to be in virtual cluster 1 and the virtual domains to be in virtual cluster 2. The root virtual domain must always be in virtual cluster 1.

For more information about configuring VDOM partitioning see the FortiGate HA Guide.
Cluster members list

Display the cluster members list to view the status of an operating cluster and the status of the FortiGate units in the cluster. To display the cluster members list, log into an operating cluster and go to **System > Config > HA**.

**Figure 76: Example FortiGate-5001SX cluster members list**

If virtual domains are enabled, you can display the cluster members list to view the status of the operating virtual clusters. The virtual cluster members list shows the status of both virtual clusters including the virtual domains added to each virtual cluster.

To display the virtual cluster members list for an operating cluster log in as the global admin administrator and go to **System > Config > HA**.

**Figure 77: Example FortiGate-5001SX virtual cluster members list**
View HA Statistics  Display the serial number, status, and monitor information for each cluster unit. See “Viewing HA statistics” on page 141.

Up and down arrows  Change the order in which cluster members are listed. The operation of the cluster or of the units in the cluster are not affected. All that changes is the order in which cluster units are displayed on the cluster members list.

Cluster member  Illustrations of the front panels of the cluster units. If the network jack for an interface is shaded green, the interface is connected. Pause the mouse pointer over each illustration to view the cluster unit host name, serial number, how long the unit has been operating (up time), and the interfaces that are configured for port monitoring.

Hostname  The host name of the FortiGate unit. The default host name of the FortiGate unit is the FortiGate unit serial number.

- To change the primary unit host name, go to System > Status and select Change beside the current host name.
- To change a subordinate unit host name, from the cluster members list select the edit icon for a subordinate unit.

Role  The status or role of the cluster unit in the cluster.

- Role is MASTER for the primary (or master) unit
- Role is SLAVE for all subordinate (or backup) cluster units

Priority  The device priority of the cluster unit. Each cluster unit can have a different device priority. During HA negotiation, the unit with the highest device priority becomes the primary unit.

The device priority range is 0 to 255.

Disconnect from cluster  Disconnect a selected cluster unit from the cluster. See “Disconnecting a cluster unit from a cluster” on page 142.

Edit  Select Edit to change a cluster unit HA configuration.

- For a primary unit, select Edit to change the cluster HA configuration. You can also change the device priority of the primary unit.
- For a primary unit in a virtual cluster, select Edit to change the virtual cluster HA configuration. You can also change the virtual cluster 1 and virtual cluster 2 device priority of this cluster unit.
- For a subordinate unit, select Edit to change the subordinate unit host name and device priority. See “Changing subordinate unit host name and device priority” on page 142.
- For a subordinate unit in a virtual cluster, select Edit to change the subordinate unit host name. In addition you can change the device priority for the subordinate unit for the selected virtual cluster. See “Changing subordinate unit host name and device priority” on page 142.

Download debug log  Download an encrypted debug log to a file. You can send this debug log file to Fortinet Technical Support (http://support.fortinet.com) to help diagnose problems with the cluster or with individual cluster units.
Viewing HA statistics

From the cluster members list you can select View HA statistics to display the serial number, status, and monitor information for each cluster unit. To view HA statistics, go to **System > Config > HA** and select View HA Statistics.

**Figure 78: Example HA statistics (active-passive cluster)**

<table>
<thead>
<tr>
<th>Unit</th>
<th>Status</th>
<th>Up Time</th>
<th>Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>slat_1</td>
<td>![Status Icon]</td>
<td>5 days 18 hours 37 seconds</td>
<td>CPU Usage: 85</td>
</tr>
<tr>
<td></td>
<td>![Serial Number]</td>
<td></td>
<td>Memory Usage: 107</td>
</tr>
<tr>
<td>slat_2</td>
<td>![Status Icon]</td>
<td>2 days 23 hours 47 minutes 7 seconds</td>
<td>CPU Usage: 54</td>
</tr>
<tr>
<td></td>
<td>![Serial Number]</td>
<td></td>
<td>Memory Usage: 107</td>
</tr>
</tbody>
</table>

- **Refresh every**: Select to control how often the web-based manager updates the HA statistics display.
- **Back to HA monitor**: Close the HA statistics list and return to the cluster members list.

**Unit**: The host name and serial number of the cluster unit.

**Status**: Indicates the status of each cluster unit. A green check mark indicates that the cluster unit is operating normally. A red X indicates that the cluster unit cannot communicate with the primary unit.

**Up Time**: The time in days, hours, minutes, and seconds since the cluster unit was last started.

**Monitor**: Displays system status information for each cluster unit.

**CPU Usage**: The current CPU status of each cluster unit. The web-based manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.

**Memory Usage**: The current memory status of each cluster unit. The web-based manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.

**Active Sessions**: The number of communications sessions being processed by the cluster unit.

**Total Packets**: The number of packets that have been processed by the cluster unit since it last started up.

**Virus Detected**: The number of viruses detected by the cluster unit.

**Network Utilization**: The total network bandwidth being used by all of the cluster unit interfaces.

**Total Bytes**: The number of bytes that have been processed by the cluster unit since it last started up.

**Intrusion Detected**: The number of intrusions or attacks detected by Intrusion Protection running on the cluster unit.
Changing subordinate unit host name and device priority

To change the host name and device priority of a subordinate unit in an operating cluster, go to System > Config > HA to display the cluster members list. Select Edit for any slave (subordinate) unit in the cluster members list.

To change the host name and device priority of a subordinate unit in an operating cluster with virtual domains enabled, log in as the global admin administrator and go to System > Config > HA to display the cluster members list. Select Edit for any slave (subordinate) unit in the cluster members list.

You can change the host name (Peer) and device priority (Priority) of this subordinate unit. These changes only affect the configuration of the subordinate unit.

Figure 79: Changing the subordinate unit host name and device priority

<table>
<thead>
<tr>
<th>HA Peer Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer: FortiGate-A</td>
</tr>
<tr>
<td>Priority: 128</td>
</tr>
</tbody>
</table>

Peer
View and optionally change the subordinate unit host name.

Priority
View and optionally change the subordinate unit device priority.
The device priority is not synchronized among cluster members. In a functioning cluster you can change device priority to change the priority of any unit in the cluster. The next time the cluster negotiates, the cluster unit with the highest device priority becomes the primary unit.
The device priority range is 0 to 255. The default device priority is 128.

Disconnecting a cluster unit from a cluster

You can go to System > Config > HA and select a Disconnect from cluster icon to disconnect a cluster unit from a functioning cluster without disrupting the operation of the cluster. You can disconnect a cluster unit if you need to use the disconnected FortiGate unit for another purpose, such as to act as a standalone firewall.

Figure 80: Disconnect a cluster member

<table>
<thead>
<tr>
<th>Disconnect Cluster Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number: FOT3002601021077</td>
</tr>
<tr>
<td>Interface: Internal</td>
</tr>
<tr>
<td>IP/Netmask: 192.168.20.1/24</td>
</tr>
</tbody>
</table>

Serial Number
Displays the serial number of the cluster unit to be disconnected from the cluster.
SNMP

Simple Network Management Protocol (SNMP) allows you to monitor hardware on your network. You can configure the hardware, or FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager is a computer running an application that can read the incoming traps from the agent and track the information. Using an SNMP manager, you can access SNMP traps and data from any FortiGate interface or VLAN subinterface configured for SNMP management access.

**Note:** Part of configuring an SNMP manager is to list it as a host in a community on the FortiGate unit it will be monitoring. Otherwise the SNMP monitor will not receive any traps from that FortiGate unit, or be able to query it.

The FortiGate SNMP implementation is read-only. SNMP v1 and v2c compliant SNMP managers have read-only access to FortiGate system information and can receive FortiGate traps. To monitor FortiGate system information and receive FortiGate traps you must compile Fortinet proprietary MIBs as well as Fortinet-supported standard MIBs into your SNMP manager.

RFC support includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II) (for more information, see “Fortinet MIBs” on page 146.

Configuring SNMP

Go to System > Config > SNMP v1/v2c to configure the SNMP agent.

**Figure 81: Configuring SNMP**

<table>
<thead>
<tr>
<th>SNMP Agent</th>
<th>Description</th>
<th>Location</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Agent</td>
<td>Enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>FortiGate unit</td>
<td>Server Room</td>
<td>System Admin ext 345</td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SNMP Agent**

Enable the FortiGate SNMP agent.

**Description**

Enter descriptive information about the FortiGate unit. The description can be up to 35 characters long.

**Location**

Enter the physical location of the FortiGate unit. The system location description can be up to 35 characters long.
Configuring an SNMP community

An SNMP community is a grouping of equipment for network administration purposes. Add SNMP communities so that SNMP managers can connect to the FortiGate unit to view system information and receive SNMP traps. You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiGate unit for a different set of events. You can also add the IP addresses of up to 8 SNMP managers to each community.

Figure 82: SNMP community options (part 1)
To configure an interface for SNMP access

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections.

1. Go to System > Network > Interface.
2. Choose an interface that an SNMP manager connects to and select Edit.
In Administrative Access, select SNMP.

Select OK.

To configure SNMP access in Transparent mode

1. Go to System > Config > Operation Mode.
2. Enter the IP address that you want to use for management access and the netmask in the Management IP/Netmask field.
3. Select Apply.

Fortinet MIBs

The FortiGate SNMP agent supports Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiGate unit configuration.

The FortiGate MIB is listed in Table 8 along with the two RFC MIBs. You can obtain these MIB files from Fortinet technical support. To be able to communicate with the SNMP agent, you must compile all of these MIBs into your SNMP manager.

Your SNMP manager might already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database. If the standard MIBs used by the Fortinet SNMP agent are already compiled into your SNMP manager you do not have to compile them again.

Table 8: Fortinet MIBs

<table>
<thead>
<tr>
<th>MIB file name or RFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fortinet.3.00.mib</td>
<td>The proprietary Fortinet MIB includes detailed FortiGate system configuration information and trap information. Your SNMP manager requires this information to monitor FortiGate configuration settings and receive traps from the FortiGate SNMP agent. See “FortiGate traps” on page 147 and “Fortinet MIB fields” on page 149.</td>
</tr>
</tbody>
</table>
| RFC-1213 (MIB II)    | The FortiGate SNMP agent supports MIB II groups with the following exceptions.  
  • No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10).  
  • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all FortiGate traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB. |
| RFC-2665 (Ethernet-like MIB) | The FortiGate SNMP agent supports Ethernet-like MIB information with the following exception.  
  No support for the dot3Tests and dot3Errors groups. |
FortiGate traps

The FortiGate agent can send traps to SNMP managers that you have added to SNMP communities. To receive traps, you must load and compile the Fortinet 3.0 MIB into the SNMP manager.

All traps include the trap message as well as the FortiGate unit serial number and hostname.

Table 9: Generic FortiGate traps

<table>
<thead>
<tr>
<th>Trap message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ColdStart</td>
<td>Standard traps as described in RFC 1215.</td>
</tr>
<tr>
<td>WarmStart</td>
<td></td>
</tr>
<tr>
<td>LinkUp</td>
<td></td>
</tr>
<tr>
<td>LinkDown</td>
<td></td>
</tr>
</tbody>
</table>

Table 10: FortiGate system traps

<table>
<thead>
<tr>
<th>Trap message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU usage high (fnTrapCpuHigh)</td>
<td>CPU usage exceeds 90%. This threshold can be set in the CLI using config system global.</td>
</tr>
<tr>
<td>Memory low (fnTrapMemLow)</td>
<td>Memory usage exceeds 90%. This threshold can be set in the CLI using config system global.</td>
</tr>
<tr>
<td>Interface IP change (fnTrapIfChange)</td>
<td>Change of IP address on a FortiGate interface. The trap message includes the name of the interface, the new IP address and the serial number of the FortiGate unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE.</td>
</tr>
<tr>
<td>Temperature too high (fnTrapTempHigh)</td>
<td>Hardware sensor detects high temperature. This is available only for FortiGate 5001.</td>
</tr>
<tr>
<td>Voltage out of range (fnTrapVoltageOutOfRange)</td>
<td>Hardware sensor detects abnormal power levels. This is available only for FortiGate 5001.</td>
</tr>
<tr>
<td>(fnFMTrapIfChange)</td>
<td>No message. Interface changes IP. Only sent to monitoring FortiManager.</td>
</tr>
<tr>
<td>(fnFMTrapConfChange)</td>
<td>Any configuration changes made to FortiGate unit, excluding any changes made by a connected FortiManager unit.</td>
</tr>
</tbody>
</table>

Table 11: FortiGate VPN traps

<table>
<thead>
<tr>
<th>Trap message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN tunnel is up (fnTrapVpnTunUp)</td>
<td>An IPSec VPN tunnel started.</td>
</tr>
<tr>
<td>VPN tunnel down (fnTrapVpnTunDown)</td>
<td>An IPSec VPN tunnel shuts down.</td>
</tr>
</tbody>
</table>
### Table 12: FortiGate IPS traps

<table>
<thead>
<tr>
<th>Trap message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Anomaly fnTrapIpsAnomaly</td>
<td>IPS anomaly detected.</td>
</tr>
<tr>
<td>IPS Signature fnTrapIpsSignature)</td>
<td>IPS signature detected.</td>
</tr>
</tbody>
</table>

### Table 13: FortiGate antivirus traps

<table>
<thead>
<tr>
<th>Trap message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus detected fnTrapAvEvent)</td>
<td>The FortiGate unit detects a virus and removes the infected file from an HTTP or FTP download or from an email message.</td>
</tr>
<tr>
<td>Oversize file/email detected fnTrapAvOversize)</td>
<td>The FortiGate unit antivirus scanner detects an oversized file.</td>
</tr>
<tr>
<td>Filename block detected fnTrapAvPattern)</td>
<td>The FortiGate unit antivirus scanner blocks a file matching a pattern.</td>
</tr>
<tr>
<td>Fragmented email detected fnTrapAvFragmented)</td>
<td>The FortiGate unit antivirus scanner detects a fragmented file or attachment.</td>
</tr>
</tbody>
</table>

### Table 14: FortiGate logging traps

<table>
<thead>
<tr>
<th>Trap message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log full fnTrapLogFull)</td>
<td>On a FortiGate unit with a hard drive, hard drive usage exceeds 90%. On a FortiGate unit without a hard drive, log to memory usage exceeds 90%. This threshold can be set in the CLI using config system global.</td>
</tr>
</tbody>
</table>

### Table 15: FortiGate HA traps

<table>
<thead>
<tr>
<th>Trap message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA switch fnTrapHaSwitch)</td>
<td>The primary unit in an HA cluster fails and is replaced with a new primary unit.</td>
</tr>
<tr>
<td>HA Heartbeat Failure fnTrapHaHBFail)</td>
<td>HA monitored interface fails heartbeat.</td>
</tr>
</tbody>
</table>

### Table 16: FortiBridge traps

<table>
<thead>
<tr>
<th>Trap message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiBridge detects fail fnTrapBridge)</td>
<td>A FortiBridge unit detects a FortiGate unit failure.</td>
</tr>
</tbody>
</table>
Fortinet MIB fields

The Fortinet MIB contains fields reporting current FortiGate unit status information. The tables below list the names of the MIB fields and describe the status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the fortinet.3.00.mib file into your SNMP manager and browsing the Fortinet MIB fields.

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnSysModel</td>
<td>FortiGate model number, for example, 400 for the FortiGate-400.</td>
</tr>
<tr>
<td>fnSysSerial</td>
<td>FortiGate unit serial number.</td>
</tr>
<tr>
<td>fnSysVersion</td>
<td>The firmware version currently running on the FortiGate unit.</td>
</tr>
<tr>
<td>fnSysVersionAv</td>
<td>The antivirus definition version installed on the FortiGate unit.</td>
</tr>
<tr>
<td>fnSysVersionNids</td>
<td>The attack definition version installed on the FortiGate unit.</td>
</tr>
<tr>
<td>fnSysHaMode</td>
<td>The current High-Availability (HA) mode (standalone, A-A, A-P)</td>
</tr>
<tr>
<td>fnSysOpMode</td>
<td>The FortiGate unit operation mode (NAT or Transparent).</td>
</tr>
<tr>
<td>fnSysCpuUsage</td>
<td>The current CPU usage (as a percent).</td>
</tr>
<tr>
<td>fnSysMemUsage</td>
<td>The current memory utilization (in MB).</td>
</tr>
<tr>
<td>fnSysDiskCapacity</td>
<td>The hard disk capacity (MB)</td>
</tr>
<tr>
<td>fnSysDiskUsage</td>
<td>The current hard disk usage (MB)</td>
</tr>
<tr>
<td>fnSysSesCount</td>
<td>The current IP session count.</td>
</tr>
</tbody>
</table>

Table 18: HA MIB fields

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnHaSchedule</td>
<td>Load balancing schedule for A-A mode.</td>
</tr>
<tr>
<td>fnHaStatsTable</td>
<td>Statistics for the individual FortiGate unit in the HA cluster.</td>
</tr>
<tr>
<td>fnHaStatsIndex</td>
<td>The index number of the unit in the cluster.</td>
</tr>
<tr>
<td>fnHaStatsSerial</td>
<td>The FortiGate unit serial number.</td>
</tr>
<tr>
<td>fnHaStatsCpuUsage</td>
<td>The current FortiGate unit CPU usage (%).</td>
</tr>
<tr>
<td>fnHaStatsMemUsage</td>
<td>The current unit memory usage (MB).</td>
</tr>
<tr>
<td>fnHaStatsNetUsage</td>
<td>The current unit network utilization (Kbps).</td>
</tr>
<tr>
<td>fnHaStatsSesCount</td>
<td>The number of active sessions.</td>
</tr>
<tr>
<td>fnHaStatsPktCount</td>
<td>The number of packets processed.</td>
</tr>
<tr>
<td>fnHaStatsByteCount</td>
<td>The number of bytes processed by the FortiGate unit</td>
</tr>
<tr>
<td>fnHaStatsIdsCount</td>
<td>The number of attacks that the IPS detected in the last 20 hours.</td>
</tr>
<tr>
<td>fnHaStatsAvCount</td>
<td>The number of viruses that the antivirus system detected in the last 20 hours.</td>
</tr>
</tbody>
</table>
Table 19: Administrator accounts

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnAdminNumber</td>
<td>The number of administrators on the FortiGate unit.</td>
</tr>
<tr>
<td>fnAdminTable</td>
<td>Table of administrators.</td>
</tr>
<tr>
<td>fnAdminIndex</td>
<td>Administrator account index number.</td>
</tr>
<tr>
<td>fnAdminName</td>
<td>The user name of the administrator account.</td>
</tr>
<tr>
<td>fnAdminAddr</td>
<td>An address of a trusted host or subnet from which this administrator account can be used.</td>
</tr>
<tr>
<td>fnAdminMask</td>
<td>The netmask for fnAdminAddr.</td>
</tr>
</tbody>
</table>

Table 20: Local users

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnUserNumber</td>
<td>The number of local user accounts on the FortiGate unit.</td>
</tr>
<tr>
<td>fnUserTable</td>
<td>Table of local users.</td>
</tr>
<tr>
<td>fnUserIndex</td>
<td>Local user account index number.</td>
</tr>
<tr>
<td>fnUserName</td>
<td>The user name of the local user account.</td>
</tr>
<tr>
<td>fnUserAuth</td>
<td>The authentication type for the local user:</td>
</tr>
<tr>
<td></td>
<td>local - a password stored on the FortiGate unit</td>
</tr>
<tr>
<td></td>
<td>radius-single - a password stored on a RADIUS server</td>
</tr>
<tr>
<td></td>
<td>radius-multiple - any user who can authenticate on the RADIUS server can log on</td>
</tr>
<tr>
<td></td>
<td>ldap - a password stored on an LDAP server</td>
</tr>
<tr>
<td>fnUserState</td>
<td>Whether the local user is enabled or disabled.</td>
</tr>
</tbody>
</table>

Table 21: Options

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnOptIdleTimeout</td>
<td>The idle period in minutes after which the administrator must re-authenticate.</td>
</tr>
<tr>
<td>fnOptAuthTimeout</td>
<td>The idle period in minutes after which a user must re-authenticate with the firewall.</td>
</tr>
<tr>
<td>fnOptLanguage</td>
<td>The web-based manager language.</td>
</tr>
<tr>
<td>fnOptLcdProtection</td>
<td>Whether an LCD PIN has been set.</td>
</tr>
</tbody>
</table>

Table 22: Logging

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnLogOption</td>
<td>Logging preferences.</td>
</tr>
</tbody>
</table>

Table 23: Custom messages

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnMessages</td>
<td>The number of custom messages on the FortiGate unit.</td>
</tr>
</tbody>
</table>
### Table 24: Virtual domains

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnVdNumber</td>
<td>The number of virtual domains on the FortiGate unit.</td>
</tr>
<tr>
<td>fnVdTable</td>
<td>Table of virtual domains.</td>
</tr>
<tr>
<td>fnVdIndex</td>
<td>Internal virtual domain index number on the FortiGate unit.</td>
</tr>
<tr>
<td>fnVdName</td>
<td>The name of the virtual domain.</td>
</tr>
</tbody>
</table>

### Table 25: Active IP sessions

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnIpSessIndex</td>
<td>The index number of the active IP session.</td>
</tr>
<tr>
<td>fnIpSessProto</td>
<td>The IP protocol (TCP, UDP, ICMP, etc.) of the session.</td>
</tr>
<tr>
<td>fnIpSessFromAddr</td>
<td>The source IP address of the active IP session.</td>
</tr>
<tr>
<td>fnIpSessFromPort</td>
<td>The source port of the active IP session.</td>
</tr>
<tr>
<td>fnIpSessToPort</td>
<td>The destination IP address of the active IP session.</td>
</tr>
<tr>
<td>fnIpSessToAddr</td>
<td>The destination port of the active IP session.</td>
</tr>
<tr>
<td>fnIpSessExp</td>
<td>The expiry time or time-to-live in seconds for the session.</td>
</tr>
</tbody>
</table>

### Table 26: Dialup VPNs

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnVpnDialupIndex</td>
<td>The index of the dialup VPN peer.</td>
</tr>
<tr>
<td>fnVpnDialupGateway</td>
<td>The remote gateway IP address.</td>
</tr>
<tr>
<td>fnVpnDialupLifetime</td>
<td>VPN tunnel lifetime in seconds.</td>
</tr>
<tr>
<td>fnVpnDialupTimeout</td>
<td>Time remaining until the next key exchange (seconds).</td>
</tr>
<tr>
<td>fnVpnDialupSrcBegin</td>
<td>Remote subnet address.</td>
</tr>
<tr>
<td>fnVpnDialupSrcEnd</td>
<td>Remote subnet mask.</td>
</tr>
<tr>
<td>fnVpnDialupDstAddr</td>
<td>Local subnet address.</td>
</tr>
</tbody>
</table>
Table 27: VPN Tunnels

<table>
<thead>
<tr>
<th>MIB field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnVpnTunEntIndex</td>
<td>The unique index of the VPN tunnel.</td>
</tr>
<tr>
<td>fnVpnTunEntPhase1Name</td>
<td>The descriptive name of the Phase1 configuration.</td>
</tr>
<tr>
<td>fnVpnTunEntPhase2Name</td>
<td>The descriptive name of the Phase2 configuration.</td>
</tr>
<tr>
<td>fnVpnTunEntRemGwyIp</td>
<td>The IP of the remote gateway.</td>
</tr>
<tr>
<td>fnVpnTunEntRemGwyPort</td>
<td>The port of the remote gateway.</td>
</tr>
<tr>
<td>fnVpnTunEntLocGwyIp</td>
<td>The IP of the local gateway.</td>
</tr>
<tr>
<td>fnVpnTunEntLocGwyPort</td>
<td>The port of the local gateway.</td>
</tr>
<tr>
<td>fnVpnTunEntSelectorSrcBeginIp</td>
<td>Beginning of the address range of a source selector.</td>
</tr>
<tr>
<td>fnVpnTunEntSelectorSrcEndIp</td>
<td>Ending of the address range of a source selector.</td>
</tr>
<tr>
<td>fnVpnTunEntSelectorSrcPort</td>
<td>Source selector port</td>
</tr>
<tr>
<td>fnVpnTunEntSelectorDstBeginIp</td>
<td>Beginning of the address range of a destination selector</td>
</tr>
<tr>
<td>fnVpnTunEntSelectorDstEndIp</td>
<td>Ending of the address range of a destination selector.</td>
</tr>
<tr>
<td>fnVpnTunEntSelectorDstPort</td>
<td>Destination selector port.</td>
</tr>
<tr>
<td>fnVpnTunEntSelectorProto</td>
<td>Protocol number for the selector.</td>
</tr>
<tr>
<td>fnVpnTunEntSelectorLifeSecs</td>
<td>Lifetime of the tunnel in seconds.</td>
</tr>
<tr>
<td>fnVpnTunEntSelectorLifeBytes</td>
<td>Lifetime of the tunnel in bytes.</td>
</tr>
<tr>
<td>fnVpnTunEntTimeout</td>
<td>Timeout of the tunnel in seconds.</td>
</tr>
<tr>
<td>fnVpnTunEntInOctets</td>
<td>Number of bytes received on the tunnel.</td>
</tr>
<tr>
<td>fnVpnTunEntOutOctets</td>
<td>Number of bytes sent out on the tunnel.</td>
</tr>
<tr>
<td>fnVpnTunEntStatus</td>
<td>Current status of the tunnel - either up or down.</td>
</tr>
</tbody>
</table>
Replacement messages

Go to **System > Config > Replacement Messages** to change replacement messages and customize alert email and information that the FortiGate unit adds to content streams such as email messages, web pages, and FTP sessions.

The FortiGate unit adds replacement messages to a variety of content streams. For example, if a virus is found in an email message, the file is removed from the email and replaced with a replacement message. The same applies to pages blocked by web filtering and email blocked by spam filtering.

**Note:** Disclaimer replacement messages provided by Fortinet are examples only.

**Replacement messages list**

**Figure 84: Replacement messages list**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Replacement for invalid email service.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Replacement for invalid HTTP service.</td>
</tr>
<tr>
<td>FTP</td>
<td>Replacement for invalid FTP service.</td>
</tr>
<tr>
<td>IM</td>
<td>Replacement for invalid IM service.</td>
</tr>
<tr>
<td>Alert Mail</td>
<td>Replacement for alert email</td>
</tr>
<tr>
<td>Spam</td>
<td>Replacement for invalid SMTP service.</td>
</tr>
<tr>
<td>Email IP</td>
<td>Replacement for blocked email IP address.</td>
</tr>
<tr>
<td>DNS/SSL/ORDB</td>
<td>Replacement for blocked email DNS/SSL/ORDB address.</td>
</tr>
<tr>
<td>HELO/ERLO domain</td>
<td>Replacement for invalid SMTP HELO/ERLO domain.</td>
</tr>
<tr>
<td>Email address</td>
<td>Replacement for blocked email address.</td>
</tr>
<tr>
<td>Mime header</td>
<td>Replacement for invalid mime header.</td>
</tr>
<tr>
<td>Returned email domain</td>
<td>Replacement for returned email domain.</td>
</tr>
<tr>
<td>Blocked word</td>
<td>Replacement for blocked blocked word.</td>
</tr>
<tr>
<td>Spam submission message</td>
<td>False positive spam submission message.</td>
</tr>
<tr>
<td>Administration</td>
<td>Replacement for administration messages.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Replacement for authentication pages.</td>
</tr>
<tr>
<td>FortiGuard Web Filtering</td>
<td>FortiGuard Web filtering replacement messages.</td>
</tr>
<tr>
<td>IM and P2P</td>
<td>Replacement for blocked IM and P2P.</td>
</tr>
<tr>
<td>SSL VPN</td>
<td>Replacement for SSL VPN message.</td>
</tr>
</tbody>
</table>
Replacement messages

Changing replacement messages

Figure 85: Sample HTTP virus replacement message

Message setup: HTTP virus message
Allowed Formats: HTML
Size: 8192 characters

You are not permitted to download the file "FILE" because it is infected with the virus "VIRUS".

URL = http://URL

Replacement messages can be text or HTML messages. You can add HTML code to HTML messages. Allowed Formats shows you which format to use in the replacement message. There is a limitation of 8192 characters for each replacement message.
In addition, replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message. Table 28 lists the replacement message tags that you can add.

Table 28: Replacement message tags

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%%AUTH_LOGOUT%%</td>
<td>The URL that will immediately delete the current policy and close the session. Used on the auth-keepalive page.</td>
</tr>
<tr>
<td>%%AUTH_REDIR_URL%%</td>
<td>The auth-keepalive page can prompt the user to open a new window which links to this tag.</td>
</tr>
<tr>
<td>%%CATEGORY%%</td>
<td>The name of the content category of the web site.</td>
</tr>
<tr>
<td>%%DEST_IP%%</td>
<td>The IP address of the request destination from which a virus was received. For email this is the IP address of the email server that sent the email containing the virus. For HTTP this is the IP address of web page that sent the virus.</td>
</tr>
<tr>
<td>%%EMAIL_FROM%%</td>
<td>The email address of the sender of the message from which the file was removed.</td>
</tr>
<tr>
<td>%%EMAIL_TO%%</td>
<td>The email address of the intended receiver of the message from which the file was removed.</td>
</tr>
<tr>
<td>%%FAILED_MESSAGE%%</td>
<td>The failed to login message displayed on the auth-login-failed page.</td>
</tr>
<tr>
<td>%%FILE%%</td>
<td>The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages.</td>
</tr>
<tr>
<td>%%FORTIGUARD_WF%%</td>
<td>The FortiGuard - Web Filtering logo.</td>
</tr>
<tr>
<td>%%FORTINET%%</td>
<td>The Fortinet logo.</td>
</tr>
<tr>
<td>%%HC_ACTIVEX%%</td>
<td>This activex control for the FortiGate-224B Host Check feature.</td>
</tr>
<tr>
<td>%%HC_FC_LINK%%</td>
<td>The link to the downloadable FortiClient Host Security image on a FortiGate-224B unit.</td>
</tr>
<tr>
<td>%%HC_REMEDY_LINK%%</td>
<td>Link to rerun Host Check on a FortiGate-224B unit.</td>
</tr>
<tr>
<td>%%HC_URL_LINK%%</td>
<td>Link(s) for third-party security software on a FortiGate-224B unit. These links are defined in Switch &gt; Port Quarantine &gt; Dynamic Policy.</td>
</tr>
<tr>
<td>%%HTTP_ERR_CODE%%</td>
<td>The HTTP error code. &quot;404&quot; for example.</td>
</tr>
<tr>
<td>%%HTTP_ERR_DESC%%</td>
<td>The HTTP error description.</td>
</tr>
<tr>
<td>%%KEEPALIVEURL%%</td>
<td>auth-keepalive-page automatically connects to this URL every %%%TIMEOUT%% seconds to renew the connection policy.</td>
</tr>
<tr>
<td>%%NIDSEVENT%%</td>
<td>The IPS attack message. %%%NIDSEVENT%% is added to alert email intrusion messages.</td>
</tr>
<tr>
<td>%%OVERRIDE%%</td>
<td>The link to the FortiGuard Web Filtering override form. This is visible only if the user belongs to a group that is permitted to create FortiGuard web filtering overrides.</td>
</tr>
<tr>
<td>%%OVRD_FORM%%</td>
<td>The FortiGuard web filter block override form. This tag must be present in the FortiGuard Web Filtering override form and should not be used in other replacement messages.</td>
</tr>
<tr>
<td>%%PROTOCOL%%</td>
<td>The protocol (http, ftp, pop3, imap, or smtp) in which a virus was detected. %%%PROTOCOL%% is added to alert email virus messages.</td>
</tr>
</tbody>
</table>
Changing the authentication login page

Users see the authentication login page when they use a VPN or a firewall policy that requires authentication. You can customize this page in the same way as you modify other replacement messages, but there are some unique requirements:

- The login page must be an HTML page containing a form with ACTION="/" and METHOD="POST"
- The form must contain the following hidden controls:
  - `<INPUT TYPE="hidden" NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%STATEID%%" VALUE="%%STATEVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%REDIRID%%" VALUE="%%PROTURI%%">`
- The form must contain the following visible controls:
  - `<INPUT TYPE="text" NAME="%%USERNAMEID%%" size=25>`
  - `<INPUT TYPE="password" NAME="%%PASSWORDID%%" size=25>`

Example

The following is an example of a simple authentication page that meets the requirements listed above.

```html
<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD><BODY><H4>You must authenticate to use this service.</H4><FORM ACTION="/" method="post">
  <INPUT NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%" TYPE="hidden">
  ...<br>
</FORM></BODY></HTML>
```
Changing the FortiGuard web filtering block override page

The `%OVRD_FORM%% tag provides the form used to initiate an override if FortiGuard - Web Filtering blocks access to a web page. Do not remove this tag from the replacement message.

Changing the SSL-VPN login message

The SSL VPN login message presents a web page through which users log in to the SSL-VPN web portal. The page is linked to FortiGate functionality and you must construct it according to the following guidelines to ensure that it will work.

- The login page must be an HTML page containing a form with ACTION="%%SSL_ACT%%' and METHOD="%%SSL_METHOD%%'
- The form must contain the `%%SSL_LOGIN%% tag to provide the login form.
- The form must contain the `%%SSL_HIDDEN%% tag.

Changing the authentication disclaimer page

The Authentication Disclaimer page, available on some models, makes a statement about usage policy to which the user must agree before the FortiGate unit permits access. You enable the disclaimer in the firewall policy. See User Authentication Disclaimer in "Firewall policy options" on page 272. You should change only the disclaimer text itself, not the HTML form code.

Changing the Host Check pages (FortiGate-224B unit only)

The Scan Access, Remedy Failed, Quarantined, Allow Access and Deny Access pages are text messages in HTML format. You can modify the messages as needed. There are no special requirements. The Portal page and the Submit Result page contain special elements that you must not remove.
Portal page

The Portal page is displayed to provide FortiClient or third-party antivirus software downloads as a remedy for a failed host check. There are two tags that provide links to downloadable software:

- the `%%HC_FC_LINK%%` tag is for FortiClient
- the `%%HC_URL_LINK%%` tag is for third-party software

You could omit one of these tags if it is not needed in your network. For example, if you only provide FortiClient software, you could omit the tag for third-party software.

The `%%HC_REMEDY_LINK%%` tag is required so that the user can choose to re-run the host check after installing the antivirus software.

Submit Result page

The Submit Result page runs the host check and provides a button to submit the results to the FortiGate-224B unit. Most elements of this page are compulsory. They are as follows:

- The Body tag for the page must contain `onload="host_checker()"` so that the host check is performed.
- The tag `%%HC_ACTIVEX%%` must appear in the head part of the HTML page to load the required host check ActiveX control.
- The following form must appear in the body of the HTML page:

  ```html
  <form method=post name=recover
    action="%%HC_PORTAL_PAGE%%">
    <input type=hidden name="%%HC_PORT_NAME%%" value="%%HC_FROM_PORT%%">
    <input type=hidden name="%%HC_TYPE_NAME%%">
    <input type=hidden name="%%HC_RESULT_NAME%%">
    <input class=button type=submit name="%%HC_SUBMIT_NAME%%" value="Submit">
  </form>
  ```

Operation mode and VDOM management access

You can change the operation mode of each VDOM independently of other VDOMs. This allows any combination of NAT/Route and Transparent operating modes on the FortiGate unit VDOMs.

Management access to a VDOM can be restricted based on which interfaces and protocols can be used to connect to the FortiGate unit.
Changing operation mode

You can set the operating mode for your VDOM and perform sufficient network configuration to ensure that you can connect to the web-based manager in the new mode.

Note: The FortiGate-224B unit in switch view does not support Transparent mode.

To switch from NAT/Route to Transparent mode

1. Go to System > Config > Operation Mode or select Change beside Operation Mode on the System Status page for the virtual domain.
2. From the Operation Mode list, select Transparent.
3. Enter the following information and select Apply.
   - **Management IP/Netmask**: Enter the management IP address and netmask. This must be a valid IP address for the network from which you want to manage the FortiGate unit.
   - **Default Gateway**: Enter the default gateway required to reach other networks from the FortiGate unit.

To switch from Transparent to NAT/Route mode

1. Go to System > Config > Operation Mode or select Change beside Operation Mode on the System Status page for the virtual domain.
2. From the Operation Mode list, select NAT.
3. Enter the following information and select Apply.
   - **Interface IP/Netmask**: Enter a valid IP address and netmask for the network from which you want to manage the FortiGate unit.
   - **Device**: Select the interface to which the Interface IP/Netmask settings apply.
Management access

You can configure management access on any interface in your VDOM. See “For a VDOM running in NAT/Route mode, you can control administrative access to the interfaces in that VDOM.” on page 94. In NAT/Route mode, the interface IP address is used for management access. In Transparent mode, you configure a single management IP address that applies to all interfaces in your VDOM that permit management access. The FortiGate also uses this IP address to connect to the FDN for virus and attack updates (see “FortiGuard Center” on page 186).

The system administrator (admin) can access all VDOMs, and create regular administrator accounts. A regular administrator account can access only the VDOM to which it belongs. The management computer must connect to an interface in that VDOM. It does not matter to which VDOM the interface belongs. In both cases, the management computer must connect to an interface that permits management access and its IP address must be on the same network. Management access can be via HTTP, HTTPS, telnet, or SSH sessions if those services are enabled on the interface. HTTPS and SSH are preferred as they are more secure.

You can allow remote administration of the FortiGate unit. However, allowing remote administration from the Internet could compromise the security of the FortiGate unit. You should avoid this unless it is required for your configuration. To improve the security of a FortiGate unit that allows remote administration from the Internet:

• Use secure administrative user passwords.
• Change these passwords regularly.
• Enable secure administrative access to this interface using only HTTPS or SSH.
• Use Trusted Hosts to limit where the remote access can originate from.
• Do not change the system idle timeout from the default value of 5 minutes (see “Settings” on page 175).
System Administrators

This section describes how to configure administrator accounts on your FortiGate unit. Administrators access the FortiGate unit to configure its operation. In its factory default configuration, the unit has one administrator, admin. After connecting to the web-based manager or the CLI, you can configure additional administrators with various levels of access to different parts of the FortiGate unit configuration.

Note: Always end your FortiGate session by logging out, in the CLI or the web-based manager. If you do not, the session remains open.

This section describes:
- Administrators
- Access profiles
- Central Management
- Settings
- Monitoring administrators

Administrators

There are two levels of administrator accounts:
- regular administrator - an administrator with any access profile other than super_admin
- system administrator - includes the factory default system administrator 'admin', and any other administrators assigned to the super_admin profile

A regular administrator account has access to configuration options as determined by its access profile. If virtual domains are enabled, the regular administrator is assigned to one VDOM and cannot access global configuration options or the configuration for any other VDOM. For information about which options are global and which are per-VDOM, see “VDOM configuration settings” on page 72 and “Global configuration settings” on page 73.

Any administrator assigned to the super_admin access profile, including the default administrator account 'admin', has full access to the FortiGate unit configuration. In addition, they can:
- enable VDOM configuration
- create VDOMs
- configure VDOMs
- assign regular administrators to VDOMs
- configure global options
The super_admin access profile cannot be changed - it does not appear in the list of profiles in **System > Access Profile**, but it is one of the selections in the Access Profile drop-down list in **System > Admin** New/Edit Administrator dialog box.

**Figure 86: super_admin profile in Administrator dialog box**

<table>
<thead>
<tr>
<th>Administrator</th>
<th>NewAdmin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Regular</td>
</tr>
<tr>
<td></td>
<td>RADIUS</td>
</tr>
<tr>
<td></td>
<td>PKI</td>
</tr>
<tr>
<td>Password</td>
<td>*********</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>*********</td>
</tr>
<tr>
<td>Trusted Host #1</td>
<td>0.0.0.0/0.0.0.0</td>
</tr>
<tr>
<td>Trusted Host #2</td>
<td>0.0.0.0/0.0.0.0</td>
</tr>
<tr>
<td>Trusted Host #3</td>
<td>0.0.0.0/0.0.0.0</td>
</tr>
<tr>
<td>Access Profile</td>
<td>[Please Select]</td>
</tr>
</tbody>
</table>

**Users assigned to the super_admin profile:**

- Cannot delete logged-in users who are also assigned the super_admin profile
- Can delete other users assigned the super_admin profile and/or change the configured authentication method, password, or access profile, only if the other users are not logged in
- Can delete the default ‘admin’ account only if another user with the super_admin profile is logged in and the default ‘admin’ user is not
- By default, ‘admin’ has no password. The password should be 32 characters or less.

**Note:** For users with super_admin access profile, you can reset the password in the CLI. If you change the password of a user who is logged in, they will be logged out and made to re-authenticate with the new password.

For a user ITAdmin with the access profile super_admin, to set the password to 123456:
```
config sys admin
edit ITAdmin
    set password 123456
end
```

For a user ITAdmin with the access profile super_admin, to reset the password from 123456 to the default ‘empty’:
```
config sys admin
edit ITAdmin
    unset password 123456
end
```
You can authenticate an administrator using a password stored on the FortiGate unit or a RADIUS server, or use PKI certificate-based authentication. Optionally, you can store all administrator accounts on a RADIUS server. RADIUS-based accounts on the same RADIUS server share the same access profile.

**Configuring RADIUS authentication for administrators**

If you want to use a RADIUS server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure the FortiGate unit to access the RADIUS server
- create a user group with the RADIUS server as its only member

The following procedures assume that there is a RADIUS server on your network populated with the names and passwords of your administrators. For information on how to set up a RADIUS server, see the documentation for your RADIUS server.

**To configure the FortiGate unit to access the RADIUS server**

1. Go to **User > RADIUS**.
2. Select Create New.
3. Enter the following information:
   - **Name**: A name for the RADIUS server. You use this name when you create the user group.
   - **Server Name/IP**: The domain name or IP address of the RADIUS server.
   - **Server Secret**: The RADIUS server secret. The RADIUS server administrator can provide this information.
4. Select OK.

**To create the administrator user group**

1. Go to **User > User Group**.
2. Select Create New.
3. In the **Group Name** field, type a name for the administrator group.
4. In the **Available Users** list, select the RADIUS server name.
5. Select the green right arrow to move the name to the **Members** list.
6. Select any protection profile.
7. Select OK.
Configuring PKI certificate authentication for administrators

Public Key Infrastructure (PKI) authentication utilizes a certificate authentication library that takes a list of ‘peers’, ‘peer’ groups, and/or user groups and returns authentication ‘successful’ or ‘denied’ notifications. Users only need a valid certificate for successful authentication - no username or password are necessary.

If you want to use PKI authentication for an administrator, you must configure the authentication before you create the administrator accounts. To do this you need to:

- create a PKI user group

The following procedures assume that there is a RADIUS server on your network populated with the names and passwords of your administrators. For information on how to set up a RADIUS server, see the documentation for your RADIUS server.

Go to User > PKI to configure PKI users.

Figure 87: User > PKI user list

| Create New | Add a new PKI user. |
| User Name | The name of the PKI user. |
| Subject | The text string that appears in the subject field of the certificate of the authenticating user. |
| Issuer | The CA certificate that is used to authenticate this user. |
| Delete icon | Delete this PKI user. |
| Edit icon | Edit this PKI user. |

Note: The following fields in the PKI User List correspond to the noted fields in the PKI User dialog:

User Name: Name
Subject: Subject
CA: Issuer (CA certificate)

To configure the FortiGate unit to access the RADIUS server

1 Go to User > RADIUS.
2 Select Create New.
3 Enter the following information:
   - Name: A name for the RADIUS server. You use this name when you create the user group.
   - Server Name/IP: The domain name or IP address of the RADIUS server.
   - Server Secret: The RADIUS server secret. The RADIUS server administrator can provide this information.
4 Select OK.
To create the administrator user group

1. Go to **User > User Group**.
2. Select Create New.
3. In the Group Name field, type a name for the administrator group.
4. In the Available Users list, select the RADIUS server name.
5. Select the green right arrow to move the name to the Members list.
6. Select any protection profile.
7. Select OK.

Viewing the administrators list

Use the default ‘admin’ account, an account with the super_admin access profile, or an administrator with Access Control Read Write to add new administrator accounts and control their permission levels. Go to **System > Admin > Administrators**.

Unless your administrator account has the super_admin access profile, the Administrators list shows only the administrators for the current virtual domain.

**Figure 88: Administrators list**

<table>
<thead>
<tr>
<th>Name</th>
<th>Trusted Hosts</th>
<th>Profile</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin2</td>
<td>0.0.0.0/0, 0.0.0.0/0, 0.0.0.0/0</td>
<td>super_admin</td>
<td>RADIUS</td>
</tr>
<tr>
<td>RADIUSProfile</td>
<td>0.0.0.0/0, 0.0.0.0/0, 0.0.0.0/0</td>
<td>prof_admin</td>
<td>RADIUS+Wildcard</td>
</tr>
<tr>
<td>admin</td>
<td>0.0.0.0/0, 0.0.0.0/0, 0.0.0.0/0</td>
<td>super_admin</td>
<td>Local</td>
</tr>
<tr>
<td>peer-admin</td>
<td>0.0.0.0/0, 0.0.0.0/0, 0.0.0.0/0</td>
<td>prof_admin</td>
<td>PKI</td>
</tr>
</tbody>
</table>

Create New
Add an administrator account.

Name
The login name for an administrator account.

Trusted hosts
The IP address and netmask of trusted hosts from which the administrator can log in. For more information, see “Using trusted hosts” on page 168.

Profile
The access profile for the administrator.

Type
The type of authentication for this administrator, one of:
- Local - a local password
- RADIUS - authentication of a specific account on a RADIUS server
- RADIUS+Wildcard - authentication of any account on a RADIUS server.
- PKI - PKI-based certificate authentication of an account.

Delete icon
Delete the administrator account.
You cannot delete the original ‘admin’ account until you create another user with the super_admin profile.

Edit or View icon
Edit or view the administrator account.

Change Password icon
Change the password for the administrator account.

To change an administrator password

1. Go to **System > Admin > Administrators**.
2. Select the Change Password icon next to the administrator account you want to change the password for.
3. Enter and confirm the new password.

4. Select OK.

**Configuring an administrator account**

Use the default ‘admin’ account, an account with the super_admin access profile, or an administrator with Access Control Read Write to create a new administrator. Go to **System > Admin > Administrators** and select Create New.

**Figure 89: Administrator account configuration - regular (local) authentication**

```
New Administrator

<table>
<thead>
<tr>
<th>Administrator</th>
<th>Type</th>
<th>Password</th>
<th>Confirm Password</th>
<th>Trusted Host #1</th>
<th>Trusted Host #2</th>
<th>Trusted Host #3</th>
<th>Access Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[Regular]</td>
<td></td>
<td></td>
<td>0.0.0.0/0.0.0.0</td>
<td>0.0.0.0/0.0.0.0</td>
<td>0.0.0.0/0.0.0.0</td>
<td>[Please Select]</td>
</tr>
</tbody>
</table>

OK  Cancel
```

**Figure 90: Administrator account configuration - RADIUS authentication**

```
New Administrator

<table>
<thead>
<tr>
<th>Administrator</th>
<th>Type</th>
<th>User Group</th>
<th>Password</th>
<th>Confirm Password</th>
<th>Trusted Host #1</th>
<th>Trusted Host #2</th>
<th>Trusted Host #3</th>
<th>Access Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[Regular]</td>
<td>RadiusGroup</td>
<td></td>
<td></td>
<td>0.0.0.0/0.0.0.0</td>
<td>0.0.0.0/0.0.0.0</td>
<td>0.0.0.0/0.0.0.0</td>
<td>[Please Select]</td>
</tr>
</tbody>
</table>

OK  Cancel
```
### Administrator account configuration - PKI authentication

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Enter the login name for the administrator account. The name of the administrator should not contain the characters <code>&lt;&gt;()#&quot;'</code>. Using these characters in the administrator account name can result in a cross site scripting (XSS) vulnerability.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of administrator account:</td>
</tr>
<tr>
<td>Regular</td>
<td>Select to create a Local administrator account.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Select to authenticate the administrator using a RADIUS server. RADIUS authentication for administrators must be configured first. See “Configuring RADIUS authentication for administrators” on page 163.</td>
</tr>
<tr>
<td>PKI</td>
<td>Select to enable certificate-based authentication for the administrator. Only one configured administrator can have the PKI option enabled at all times.</td>
</tr>
<tr>
<td>User Group</td>
<td>If you are using RADIUS or PKI certificate-based authentication, select the administrator user group that includes the RADIUS server/PKI (peer) users as members of the User Group. The administrator user group cannot be deleted once the group is selected for authentication.</td>
</tr>
<tr>
<td>Wildcard</td>
<td>Select to allow all accounts on the RADIUS server to be administrators. This is available only if RADIUS is selected.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password for the administrator account. For improved security, the password should be at least 6 characters long. If RADIUS is enabled, the FortiGate unit attempts RADIUS authentication first, and if that fails, it attempts password authentication. This is not available if Wildcard is selected. Not available when PKI authentication is selected.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Type the password for the administrator account a second time to confirm that you have typed it correctly. This is not available if Wildcard is selected. Not available when PKI authentication is selected.</td>
</tr>
<tr>
<td>Trusted Host</td>
<td>Optionally, type the trusted host IP address and netmask that administrator login is restricted to on the FortiGate unit. You can specify up to three trusted hosts. These addresses all default to 0.0.0.0/0. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see “Using trusted hosts” on page 168.</td>
</tr>
<tr>
<td>Access Profile</td>
<td>Select the access profile for the administrator. The pre-configured super_admin profile provides full access to the FortiGate unit. You can also select Create New to create a new access profile. For more information on access profiles, see “Configuring an access profile” on page 172.</td>
</tr>
</tbody>
</table>
To configure an administrator account

1. Go to System > Admin > Administrators.

2. Select Create New to add an administrator account or select the Edit icon to make changes to an existing administrator account.

3. In the Administrator field, type a login name for the administrator account. If you are using RADIUS authentication for this administrator but not using the wildcard option, the administrator name must match an account on the RADIUS server.

4. Select the type of authentication:
   - If you are using RADIUS authentication for this administrator:
     - Select RADIUS.
     - Select Wildcard if you want all accounts on the RADIUS server to be administrators of this FortiGate unit.
     - Select the administrators user group from the User Group list.
   - If you are using PKI certificate-based authentication for this administrator:
     - Select PKI.
     - Select the administrators user group from the User Group list.

5. Type and confirm the password for the administrator account.
   - This step does not apply if you are using RADIUS Wildcard or PKI certificate-based authentication.

6. Optionally, type a Trusted Host IP address and netmask from which the administrator can log into the web-based manager.

7. Select the access profile for the administrator.

8. Select OK.

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiGate unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply both to the web-based manager and to the CLI when accessed through telnet or SSH. CLI access through the console connector is not affected.

The trusted host addresses all default to 0.0.0.0/0. If you set one of the 0.0.0.0/0 addresses to a non-zero address, the other 0.0.0.0/0 will be ignored. The only way to use a wildcard entry is to leave the trusted hosts at 0.0.0.0/0. However, this is an unsecure configuration.
Access profiles

Each administrator account belongs to an access profile. The access profile separates FortiGate features into access control categories for which you can enable read and/or write access. The following table lists the web-based manager pages to which each category provides access:

Table 29: Access profile control of access to Web-based manager pages

<table>
<thead>
<tr>
<th>Access control</th>
<th>Affected web-based manager pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Users</td>
<td>System &gt; Admin System &gt; Admin &gt; FortiManager System &gt; Admin &gt; Settings</td>
</tr>
<tr>
<td>Antivirus Configuration</td>
<td>AntiVirus</td>
</tr>
<tr>
<td>Auth Users</td>
<td>User</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>Firewall</td>
</tr>
<tr>
<td>FortiGuard Update</td>
<td>System &gt; Maintenance &gt; FortiGuard Center</td>
</tr>
<tr>
<td>IPS Configuration</td>
<td>Intrusion Protection</td>
</tr>
<tr>
<td>Log &amp; Report</td>
<td>Log &amp; Report</td>
</tr>
<tr>
<td>Maintenance</td>
<td>System &gt; Maintenance</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>System &gt; Network &gt; Interface System &gt; Network &gt; Zone System &gt; DHCP</td>
</tr>
<tr>
<td>Router Configuration</td>
<td>Router</td>
</tr>
<tr>
<td>Spamfilter Configuration</td>
<td>AntiSpam</td>
</tr>
<tr>
<td>System Configuration</td>
<td>System &gt; Status, including Session info System &gt; Config System &gt; Hostname System &gt; Network &gt; Options System &gt; Admin &gt; FortiManager System &gt; Admin &gt; Settings System &gt; Status &gt; System Time</td>
</tr>
<tr>
<td>VPN Configuration</td>
<td>VPN</td>
</tr>
<tr>
<td>Webfilter Configuration</td>
<td>Web Filter</td>
</tr>
</tbody>
</table>

Read-only access enables the administrator to view the web-based manager page. The administrator needs write access to change the settings on the page.

You can now expand the firewall configuration access control to enable more granular control of access to the firewall functionality. You can control administrator access to policy, address, service, schedule, profile, and other (VIP) configurations.

**Note:** When Virtual Domain Configuration is enabled (see “Settings” on page 175), only the administrators with the access profile super_admin have access to global settings. When Virtual Domain Configuration is enabled, other administrator accounts are assigned to one VDOM and cannot access global configuration options or the configuration for any other VDOM.

For information about which settings are global, see “VDOM configuration settings” on page 72.
The access profile has a similar effect on administrator access to CLI commands. The following table shows which command types are available in each access control category. You can access “get” and “show” commands with read access. Access to “config” commands requires write access.

Table 30: Access profile control of access to CLI commands

<table>
<thead>
<tr>
<th>Access control</th>
<th>Available CLI commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Users (admingrp)</td>
<td>system admin, system accprofile</td>
</tr>
<tr>
<td>Antivirus Configuration (avgrp)</td>
<td>antivirus</td>
</tr>
<tr>
<td>Auth Users (authgrp)</td>
<td>user</td>
</tr>
<tr>
<td>Firewall Configuration (fwgrp)</td>
<td>firewall, set fwgrp custom, config fwgrp-permission</td>
</tr>
<tr>
<td>FortiProtect Update (updategrp)</td>
<td>system autoupdate, execute update-av, execute update-ips, execute update-now</td>
</tr>
<tr>
<td>IPS Configuration (ipsgrp)</td>
<td>ips</td>
</tr>
<tr>
<td>Log &amp; Report (loggrp)</td>
<td>alertemail, log, system fortianalyzer, execute log</td>
</tr>
<tr>
<td>Maintenance (mntgrp)</td>
<td>execute formatlogdisk, execute restore, execute backup, execute batch, execute usb-disk</td>
</tr>
<tr>
<td>Network Configuration (netgrp)</td>
<td>system arp-table, system dhcp, system interface, system zone, execute dhcp lease-clear, execute dhcp lease-list, execute clear system arp table, execute interface</td>
</tr>
<tr>
<td>Router Configuration (routegrp)</td>
<td>router, execute router, execute mrouter</td>
</tr>
</tbody>
</table>
Go to System > Admin > Access Profile to add access profiles for FortiGate administrators. Each administrator account belongs to an access profile. You can create access profiles that deny access to, allow read-only, or allow both read- and write-access to FortiGate features.

When an administrator has read-only access to a feature, the administrator can access the web-based manager page for that feature but cannot make changes to the configuration. There are no Create or Apply buttons and lists display only the View ( ) icon instead of icons for Edit, Delete or other modification commands.

### Viewing the access profiles list

Use the admin account or an account with Admin Users read and write access to create or edit access profiles. Go to System > Admin > Access Profile.

**Table 30: Access profile control of access to CLI commands**

<table>
<thead>
<tr>
<th>Access Profile</th>
<th>CLI Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spamfilter Configuration (spamgrp)</td>
<td>spamfilter</td>
</tr>
<tr>
<td>System Configuration (sysgrp)</td>
<td>system except accprofile, admin, arp-table, autoupdate, fortianalyzer, interface, and zone, execute date, execute ha, execute ping, execute ping-options, execute ping6, execute time, execute traceroute, execute cfg, execute factoryreset, execute reboot, execute shutdown, execute deploy, execute set-next-reboot, execute ssh, execute telnet, execute disconnect-admin-session, execute usb</td>
</tr>
<tr>
<td>VPN Configuration (vpngrp)</td>
<td>vpn execute vpn</td>
</tr>
<tr>
<td>Webfilter Configuration (webgrp)</td>
<td>webfilter</td>
</tr>
</tbody>
</table>

Go to System > Admin > Access Profile to add access profiles for FortiGate administrators. Each administrator account belongs to an access profile. You can create access profiles that deny access to, allow read-only, or allow both read- and write-access to FortiGate features.

When an administrator has read-only access to a feature, the administrator can access the web-based manager page for that feature but cannot make changes to the configuration. There are no Create or Apply buttons and lists display only the View ( ) icon instead of icons for Edit, Delete or other modification commands.
Configuring an access profile

Use the admin account or an account with Admin Users read and write access to edit an access profile. Go to System > Admin > Access Profile and select Create New.

Figure 93: Access profile option

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Enter the name of the access profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Access Control lists the items to which the access profile controls access.</td>
</tr>
<tr>
<td>None</td>
<td>Select None to disable access to all Access Control categories.</td>
</tr>
<tr>
<td>Read</td>
<td>Select Read to select Read access in all Access Control categories.</td>
</tr>
<tr>
<td>Read Write</td>
<td>Select Read Write to select Read and Write access in all Access Control categories.</td>
</tr>
<tr>
<td>Access Control categories</td>
<td>Select Read and/or Read/Write access for Access Control categories as required. For detailed information about the access control categories, see “Access profiles” on page 169.</td>
</tr>
</tbody>
</table>
Central Management

Go to System > Admin > Central Management to configure the FortiGate unit to be managed through either:

- FortiManager
- FortiGuard Management Service

With FortiManager and FortiGuard, the administrative functionality is similar - the FortiGate unit is centrally managed in each case. This option allows you to backup the FortiGate configuration to another location other than your local PC, which can be useful when you administer multiple FortiGate units.

Figure 94: Central Management configurations - FortiManager and FortiGuard

Central Management

Enable Central Management
Type: FortiManager, FortiGuard Management Service
ID
Allow automatic backup of configuration on logout/timeout

Central Management

Enable Central Management
Type: FortiManager, FortiGuard Management Service
Account ID
Allow automatic backup of configuration on logout/timeout

Central Management

Enable Central Management
Type
FortiManager: Select to use FortiManager as the central management service for the FortiGate unit. Enter the IP Address of the FortiManager Server.
FortiGuard Management Service: Select to use the FortiGuard Management Service as the central management service for the FortiGate unit. Enter the Account ID you were given when you registered for this service. Click Change to open the FortiGuard Distribution Network screen and select the Account ID in Management Service Options (see Figure 95).
If you do not have an account ID, register for the FortiGuard Management Service with Fortinet Customer Service.

Allow automatic backup of configuration on logout/timeout
Enable to have configuration backup occur when the admin session is closed - you log out of the FortiGate unit or the admin timeout is reached.
Configuration revision control (managed through the FortiManager server or FortiGuard Management Service) allows you to manage multiple versions of your FortiGate unit’s configuration files. This feature requires a configured Central Management server. When revision control is enabled on your FortiGate unit, you will be able to view a list of saved revisions of your FortiGate unit’s configuration.

Figure 96: Revision Control screen

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date/Time</th>
<th>Administrator</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>12/04/2006 15:00:00</td>
<td>admin</td>
<td>27</td>
</tr>
<tr>
<td>1</td>
<td>12/04/2006 15:00:14</td>
<td>admin</td>
<td>27</td>
</tr>
</tbody>
</table>

Page Navigation

A series of controls that allow you to navigate within the revision control screen information if there is more than one page. This includes:

- return to the first page
- back up one page
- select the page to jump to
- go forward one page
- go to last page

Revision

An incremental number indicating the order the configurations were saved. These may not be consecutive numbers if one or more configurations are deleted. The most recent, also the largest number, is first in the list.

Date/Time

Displays the date and time when this configuration was saved.

Administrator

Displays the administrator account that was used to back up this revision.

Comments

Any relevant description or notes that were saved with the revision.

This is a good place to include information about why the revision was saved, who saved it, and if there is a date when it can be deleted to free up space.


For further information about system maintenance, FortiGuard, and configuration backup and restore, see “Maintenance System Configuration” on page 179.

Settings

Go to System > Admin > Settings to set the following options:

- Ports for HTTP and HTTPS administrative access
- The idle timeout setting
- Display settings that include the language of the web-based manager and the number of lines displayed in generated reports
- PIN protection for LCD and control buttons (LCD-equipped models only)
- Enable SCP capability for users logged in via SSH

---

Diff icon

Select the diff icon to compare two revisions. This will display a window that lets you compare the selected revision to one of:

- the current configuration
- a selected revision from the displayed list including revision history and templates
- a specified revision number

Download icon

Select the download icon to download this revision to your local PC.

Revert icon

Select to go back to the selected revision. You will be prompted to confirm this action.

---

Figure 97: Administrators Settings

<table>
<thead>
<tr>
<th>Administrators Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Administration Ports</strong></td>
</tr>
<tr>
<td>HTTP</td>
</tr>
<tr>
<td>HTTPS</td>
</tr>
<tr>
<td>Telnet Port</td>
</tr>
<tr>
<td>SSH Port</td>
</tr>
<tr>
<td>Enable v1 compatibility</td>
</tr>
<tr>
<td><strong>Idle Timeout</strong></td>
</tr>
<tr>
<td><strong>Language</strong></td>
</tr>
<tr>
<td><strong>Lines Per Page</strong></td>
</tr>
<tr>
<td><strong>LCD Panel</strong></td>
</tr>
<tr>
<td>PIN Protection</td>
</tr>
<tr>
<td>Enable SCP</td>
</tr>
</tbody>
</table>

---

| Admin Settings |
Web Administration Ports

HTTP
Enter the TCP port to be used for administrative HTTP access. The default is 80.

HTTPS
Enter the TCP port to be used for administrative HTTPS access. The default is 443.

Telnet Port
Enter the telnet port to be used for administrative access. The default is 23.

SSH Port
Enter the SSH port to be used for administrative access. The default is 22.

Enable v1 compatibility
Select to enable compatibility with SSH v1 in addition to v2. (Optional)

Timeout Settings

Idle Timeout
Enter the number of minutes that an administrative connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours). To improve security, keep the idle timeout at the default value of 5 minutes.

Display Settings

Language
Select a language for the web-based manager to use. Choose from English, Simplified Chinese, Traditional Chinese, Japanese, Korean, or French. You should select the language that the management computer operating system uses.

Lines per Page
Set the number of lines per page to display in table lists. The default is 50. Range is from 20 - 1000.

LCD Panel (LCD-equipped models only)

PIN Protection
Select the PIN Protection check box and type a 6-digit PIN. Administrators must enter the PIN to use the control buttons and LCD.

Enable SCP
Enable if you want users logged in through the SSH to be able to use the SCP to copy the configuration file.

Note: If you make a change to the default port number for http, https, telnet, or SSH, ensure that the port number is unique.
Monitoring administrators

To see the number of logged-in administrators, go to **System > Status**. Under System Information, you will see Current Administrators. Click on Details to view information about the administrators currently logged in to the FortiGate unit.

**Figure 98: System Information > Current Administrators**

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>TEST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime</td>
<td>0 day(s) 4 hour(s) 54 min(s)</td>
</tr>
<tr>
<td>System Time</td>
<td>Thu Mar 15 10:20:00 2007 [Change]</td>
</tr>
<tr>
<td>HA Status</td>
<td>Standalone [Configure]</td>
</tr>
<tr>
<td>Host Name</td>
<td>TEST [Change]</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>Fortigate-300 3.00,build0532,070314 [Update]</td>
</tr>
<tr>
<td>Operation Mode</td>
<td>NAT [Change]</td>
</tr>
<tr>
<td>Virtual Domain</td>
<td>Disabled [Enable]</td>
</tr>
<tr>
<td>Current Administrators</td>
<td>1 [Details]</td>
</tr>
</tbody>
</table>

**Figure 99: Administrators logged in monitor window**

<table>
<thead>
<tr>
<th>User Name</th>
<th>Type</th>
<th>From</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>WEB</td>
<td>172.20.120.41</td>
<td>Fri Sep 15 10:44:49 2005</td>
</tr>
<tr>
<td>admin</td>
<td>CLI</td>
<td>jsconsole</td>
<td>Fri Sep 15 10:45:01 2005</td>
</tr>
</tbody>
</table>

**Disconnect**

Select to disconnect the selected administrators. This is available only if your access profile gives you System Configuration write permission.

**Refresh**

Select to update the list.

**Close**

Select to close the window.

**check box**

Select and then select Disconnect to log off this administrator. This is available only if your access profile gives you System Configuration write access. You cannot log off the default ‘admin’ user.

**User Name**

The administrator account name.

**Type**

The type of access: WEB or CLI.

**From**

If Type is WEB, the value in From is the administrator’s IP address. If Type is CLI, the value in From is “ssh” or “telnet” and either the administrator’s IP address or “console”.

**Time**

The date and time that the administrator logged on.
System Maintenance

This section describes how to back up and restore your system configuration and how to configure automatic updates from the FortiGuard Distribution Network.

This section describes:

- Maintenance System Configuration
- Revision Control
- FortiGuard Center
- License

Maintenance System Configuration

Go to System > Maintenance > Backup & Restore to back up and restore the system configuration and to manage firmware.

You can back up the system configuration, including web content files and spam filtering files, to the management computer or to a USB disk on models that support a USB disk. You can also restore the system configuration from previously downloaded backup files.

If you want the backup file to include VPN certificates, you must enable encryption of the backup file.

When virtual domain configuration is enabled, the content of the backup file depends on the administrator account that created it. A backup of the system configuration from the super admin account contains global settings and the settings for each VDOM. Only the super admin can restore the configuration from this file. When you back up the system configuration from a regular administrator account, the backup file contains the global settings and the settings for the VDOM to which the regular administrator belongs. Only a regular administrator account can restore the configuration from this file.

Note: If you have a FortiGate model numbered 100 or lower, the Firmware section of the Maintenance screen will not be displayed. In this situation you can change your firmware version by going to System > Status and selecting Update for Firmware Version. If you have a FortiGate model number 100A or higher you will be able to see the Firmware section by default.

Some FortiGate models support FortiClient by storing a FortiClient image that users can download. The FortiClient section of Backup and Restore is available only if your FortiGate model supports FortiClient. This feature is currently available on FortiGate 1000A, 3600A, and 5005FA2 models.
The Backup and Restore screen is broken into smaller sections to make it easier to explain. These sections are:

- **Backup and Restore**
- **Firmware**
- **FortiClient**
- **Firmware Upgrade**
- **Advanced**
Backup and Restore

Backup and Restore is where you configure your system configuration backups. You can also choose which backed up configuration to restore.

Both Backup and Restore have central management options. To use central management, you must first configure it using the System > Admin Central management screen, see “Central Management” on page 173.

Figure 102: Backup and Restore local options

![Backup and Restore local options](image1)

Figure 103: Backup and Restore FortiManager options

![Backup and Restore FortiManager options](image2)

Last Backup
The date and time of the last local or remote backup. Backing up to USB does not save the time of backup.

Backup
Back up the current configuration.

Backup configuration to:
Select one of the displayed options:
- Local PC
- USB Disk - if the unit supports USB Disks and one of:
  - Management Station
  - FortiManager
  - FortiGuard

The USB Disk option will be grayed out if the FortiGate unit supports USB disks but none are connected. Apart from Local PC, all these options are available only if that device or service is connected to the FortiGate unit.

Encrypt configuration file
Select to encrypt the backup file. Enter a password in the Password field and enter it again in the Confirm field. You will need this password to restore the file. To backup VPN certificates, encryption must be enabled on the backup file. This option is not available for FortiManager backup option.

Filename
Enter a name for the backup file. This control is available only when USB drive is connected.

Comment
Enter a comment to be stored with the backup on the FortiManager device.
### Remote Management Options

Your FortiGate unit has the option of being managed by either a FortiManager device, or through a remote management FortiGuard service. Either of these FortiGuard Management Service options allow for your FortiGate unit’s configuration to be backed up to another location than your local PC. This is useful when administering multiple FortiGate units. To use the FortiGuard Management Service you must subscribe to it through customer support.

When Restoring from a remote location you will be presented with a list of revisions to choose from to restore your FortiGate unit’s configuration.

In both Backup and Restore sections this is shown in the following options explained below.

**Management Station**

This option appears when no Remote Management has been configured. This option will not be selectable.

Once Remote Management has been configured, this option will disappear to be replaced by the configured option.

**FortiManager**

Once Remote Management has been set to FortiManager, this option is visible. When properly configured, and the connection has been made to the FortiManager device this option will become selectable.

**FortiGuard**

Once Remote Management has been set to FortiGuard Management Service, this option is visible. When properly configured, and the connection has been made to the service this option will become selectable.
Firmware

Firmware displays the current version of firmware installed on your FortiGate unit, and which firmware image is currently in use if you have more than one.

**Figure 104:** Firmware

<table>
<thead>
<tr>
<th>Partition</th>
<th>Active</th>
<th>Last Upgrade</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✔️</td>
<td>-</td>
<td>FortiGate-3000A.0.00000001</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>-</td>
<td>[Upload and Reboot]</td>
</tr>
</tbody>
</table>

**Partition**
A partition can contain one version of the firmware and the system configuration. FortiGate models numbered 100 and higher have two partitions. One partition is active and the other is a backup.

**Active**
A green check mark indicates which partition contains the firmware and configuration currently in use.

**Last Upgrade**
The date and time of the last update to this partition.

**Firmware Version**
The version and build number of the FortiGate firmware. If your FortiGate model has a backup partition, you can:

- Select Upload to replace with firmware from the management computer or a USB disk.
- Select Upload and Reboot to replace the firmware and make this the active partition.

**Boot alternate firmware**
Restart the FortiGate unit using the backup firmware. This is available only on FortiGate models numbered 100 or higher.

FortiClient

FortiGate models 1000A, 3600A, and 5005FA2 can store a FortiClient software image that users can download and install. This software is accessed through the FortiClient web portal on the FortiGate unit.

**Figure 105:** FortiClient

- **Software Image**: The current FortiClient image on this FortiGate unit. Select Upload to upload a new FortiClient image from your management computer.
- **Antivirus Database**: The current version of FortiGuard antivirus database on this FortiGate unit. For more details, see “Configuring the FortiGate unit for FDN and FortiGuard services” on page 188.
- **Antivirus Engine**: The current version of FortiGuard antivirus engine on this FortiGate unit. For more details, see “Configuring the FortiGate unit for FDN and FortiGuard services” on page 188.
- **Web Portal Port**: Select the port for the web portal where users will be redirected if they are denied access due to FortiClient check options in the firewall policy. Select Save after changing the port number to commit your change.

The default port number is 8009. The port number should only be changed if there is a conflict.
Firmware Upgrade

Firmware upgrade displays your options for upgrading to a new version using the FortiGuard network if that option is available to you. It is not available on all models, and you must register for the service through customer support.

Figure 106: Firmware Upgrade

<table>
<thead>
<tr>
<th>Upgrade method</th>
<th>Select to upgrade from FortiGuard network or upgrade by file</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Please Select]</td>
<td>Select one of the available firmware versions.</td>
</tr>
<tr>
<td>Allow firmware downgrade</td>
<td>Select to be able to install older versions than the one currently installed.</td>
</tr>
<tr>
<td></td>
<td>This is useful if the current version changed functionality you need and you have to revert to the old image.</td>
</tr>
<tr>
<td>Upgrade by File</td>
<td>Select Browse to select a file on your local PC to upload to the FortiGate unit</td>
</tr>
<tr>
<td>OK</td>
<td>Select OK to enable your selection.</td>
</tr>
</tbody>
</table>

Advanced

The advanced section includes the USB Auto Install feature, importing CLI commands, and the debug log.

Figure 107: Advanced

Advanced (USB Auto-Install)

This section is available only if a USB disk is connected to the FortiGate unit. Select the options as required and restart the FortiGate unit.

- If you select both configuration and firmware update, both occur on the same reboot. The FortiGate unit will not reload a firmware or configuration file that is already loaded.

On system restart, automatically update FortiGate configuration

Automatically update the configuration on restart. Ensure that the Default configuration file name matches the configuration file name on the USB disk.
USB Disks

FortiGate units with a USB interface support USB disks for backing up and restoring configurations.

FortiUSB and generic USB disks are supported. However, the USB disk must be formatted as a FAT16 disk. No other partition type is supported.

**Note:** Formatting your USB disk will delete all information on your USB disk.

To format your USB disk when it is connected to your FortiGate unit, at the CLI prompt type `exe usb-disk format`.

To format your USB disk when it is connected to a Windows system, at the DOS command prompt type `format <drive_letter>: /FS:FAT /V:<drive_label>` where `<drive_letter>` is the letter of the connected USB drive you want to format, and `<drive_label>` is the name you want to give the USB drive for identification.

Revision Control

Revision Control allows you to manage multiple versions of your FortiGate unit’s configuration files. It requires a configured Central Management server. This server can either be a FortiManager device or the FortiGuard Management Service. To use the FortiGuard Management Service you must subscribe to it through customer support.

If central management is not configured on your FortiGate unit, when you select this option you will see a message telling you to:

- enable Central Management, see “Central Management” on page 173
- obtain a valid license

When revision control is enabled on your FortiGate unit you will be able to view a list of saved revisions of your FortiGate unit’s configuration.
FortiGuard Center

The FortiGuard Center configures your FortiGate unit for the FortiGuard Distribution Network (FDN) and FortiGuard Services. The FDN provides updates to antivirus and attack definitions. FortiGuard Services provides online IP address black list, URL black list, and other spam filtering tools.

FortiGuard Distribution Network

The FortiGuard Distribution Network (FDN) is a world-wide network of FortiGuard Distribution Servers (FDSs). The FDN provides updates to antivirus (including grayware) and IPS attack definitions. When the FortiGate unit connects to the FDN, it connects to the nearest FDS based on the current time zone setting.
The FortiGate unit supports the following update features:

- User-initiated updates from the FDN,
- Hourly, daily, or weekly scheduled antivirus and attack definition updates from the FDN,
- Push updates from the FDN,
- Update status including version numbers, expiry dates, and update dates and times,
- Push updates through a NAT device.

You must register the FortiGate unit on the Fortinet support web page. To register your FortiGate unit, go to Product Registration and follow the instructions.

To receive scheduled updates, the FortiGate unit must be able to connect to the FDN using HTTPS on port 443. For information about configuring scheduled updates, see “To enable scheduled updates” on page 194.

You can also configure the FortiGate unit to receive push updates. For this to succeed, the FDN must be able to route packets to the FortiGate unit using UDP port 9443. For information about configuring push updates, see “To enable push updates” on page 195. If the FortiGate unit is behind a NAT device, see “Enabling push updates through a NAT device” on page 196.

**FortiGuard Services**

Worldwide coverage of FortiGuard services are provided by FortiGuard Service Points. When your FortiGate unit connects to the FDN, it is connecting to the closest FortiGuard Service Point. Fortinet adds new Service Points as required.

By default, the FortiGate unit communicates with the closest Service Point. If the Service Point becomes unreachable for any reason, the FortiGate unit contacts another Service Point and information is available within seconds. By default, the FortiGate unit communicates with the Service Point via UDP on port 53. Alternately, the UDP port used for Service Point communication can be switched to port 8888 by going to System > Maintenance > FortiGuard Center.

If you need to change the default FortiGuard Service Point host name, use the hostname keyword in the system fortiguard CLI command. You cannot change the FortiGuard Service Point name using the web-based manager.

For detailed information about FortiGuard services, see the FortiGuard Center web page.

**FortiGuard Antispam Service**

FortiGuard Antispam is an antispam system from Fortinet that includes an IP address black list, a URL black list, and spam filtering tools. The IP address black list contains IP addresses of email servers known to be used to generate spam. The URL black list contains URLs of websites found in spam email.

FortiGuard Antispam processes are completely automated and configured by Fortinet. With constant monitoring and dynamic updates, FortiGuard Antispam is always current. Enable or disable FortiGuard Antispam in firewall protection profiles. For more information, see “Spam filtering options” on page 336.
Every FortiGate unit comes with a free 30-day FortiGuard Antispam trial license. FortiGuard Antispam license management is performed by Fortinet servers; there is no need to enter a license number. The FortiGate unit automatically contacts a FortiGuard Antispam Service Point when enabling FortiGuard Antispam. To renew the FortiGuard Antispam license after the free trial, contact Fortinet Technical Support.

Enable FortiGuard Antispam globally in System > Maintenance > FortiGuard Center and then configure the Spam Filtering options in each firewall protection profile. See “Spam filtering options” on page 336.

**FortiGuard Web Filtering Service**

FortiGuard Web Filtering is a managed web filtering solution provided by Fortinet. FortiGuard Web Filtering sorts hundreds of millions of web pages into a wide range of categories users can allow, block, or monitor. The FortiGate unit accesses the nearest FortiGuard Web Filtering Service Point to determine the category of a requested web page then follows the firewall policy configured for that user or interface.

Every FortiGate unit comes with a free 30-day FortiGuard Web Filtering trial license. FortiGuard license management is performed by Fortinet servers. There is no need to enter a license number. The FortiGate unit automatically contacts a FortiGuard Service Point when enabling FortiGuard category blocking. To renew a FortiGuard license after the free trial, contact Fortinet Technical Support.

Enable FortiGuard Web Filtering globally in System > Maintenance > FortiGuard Center and then configure the FortiGuard Web Filtering options in each firewall protection profile. See “FortiGuard Web Filtering options” on page 334.

**FortiGuard Management and Analysis Services**

FortiGuard Management and Analysis Services are remote services that provide more features for FortiGate units. These are both subscription services.

FortiGuard Management Service provides features found in a FortiManager unit. This service allows you to remotely manage your FortiGate unit by backing up your FortiGate unit configuration to a location other than your local PC, and restoring your FortiGate unit configuration from a list of these backups.

FortiGuard Analysis Service provides features found in a FortiAnalyzer unit. This service allows you to store logging data remotely, and generate reports on that log data remotely.

**Configuring the FortiGate unit for FDN and FortiGuard services**

Go to System > Maintenance > FortiGuard Center to configure access to FDN updates and FortiGuard services on the Update Center page.

The three sections of the Update Center are:

- Support Contract and FortiGuard Subscription Services
- AntiVirus and IPS Downloads
- Web Filtering and AntiSpam Options
Support Contract and FortiGuard Subscription Services

The Support Contract and FortiGuard Subscription Services sections are displayed in abbreviated form on the System Status page. See “Viewing system status” on page 49.

Figure 109: Support Contract and FortiGuard Subscription Services section

<table>
<thead>
<tr>
<th>FortiGuard Subscription Services</th>
<th>Support Contract</th>
<th>FortiOS 3.0.0 (Expires 2008-05-17)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AntiVirus</td>
<td>Valid License</td>
<td>Expires 2008-05-17</td>
</tr>
<tr>
<td>AV Definitions</td>
<td>7.6.18 (Updated 2007-06-28 via scheduled update)</td>
<td></td>
</tr>
<tr>
<td>IPS Definitions</td>
<td>2.0.15 (Updated 2007-06-28 via scheduled update)</td>
<td></td>
</tr>
<tr>
<td>Web Filtering</td>
<td>Valid License</td>
<td>Expires 2008-05-10</td>
</tr>
<tr>
<td>AntSpam</td>
<td>Valid License</td>
<td>Expires 2008-05-10</td>
</tr>
<tr>
<td>Management Service</td>
<td>Valid License</td>
<td>Expires 2007-09-01</td>
</tr>
<tr>
<td>Analysis Service</td>
<td>Valid License</td>
<td>Expires 2007-07-01, 10 GB quotas, 25 MB daily quota</td>
</tr>
</tbody>
</table>

- **Support Contract**
  - The availability or status of your FortiGate unit support contract. The status displayed can be one of: Unreachable, Not Registered or Valid Contract.
  - If Valid Contract is shown, the FortiOS version, expiry date of contract, and Support Level are also displayed.
  - [Register] Select to register your FortiGate unit support contract. This is only displayed when Support Contract is Not Registered.

- **FortiGuard Subscription Services**
  - Availability and status information for each of the FortiGuard subscription services including:
    - AntiVirus AV Definitions
    - Intrusion Protection IPS Definitions
    - Web Filtering
    - AntiSpam
    - Management Service
    - Analysis Service
FortiGate Version 3.0 MR5 Administration Guide

FortiGuard Center System Maintenance

AntiVirus and IPS Downloads
Select the blue arrow next to AntiVirus and IPS Downloads to access this section.

The SETUP message that the FortiGate unit sends when you enable push updates includes the IP address of the FortiGate interface to which the FDN connects. The Use override push option is used when your FortiGate unit is behind a NAT device. This option creates a policy that will redirect the incoming FDS traffic to the FortiGate unit. The FortiGate unit sends the FDS the IP and port numbers of the NAT device. However, the NAT device must also be configured to forward the FDS traffic to the FortiGate unit on port 9443.

Availability
The availability of this service on this FortiGate unit, dependent on your service subscription. The status displayed can be one of: Unreachable, Not Registered, Valid License, or Valid Contract.
The option to Subscribe will be displayed if Availability is Not Registered.
The option to Renew will be displayed if Availability is Expired.

Status Icon
Icon shown indicates the status of the subscription service. The icon corresponds to the availability description.
- grey - Unreachable - FortiGate unit is not able to connect to service
- yellow - Not Registered - FortiGate unit can connect, but has no support registered for this service
- yellow - Expired - FortiGate unit had a valid license that expired
- green - Valid license - FortiGate unit can connect to FDN and has a registered support contract
If the Status Icon is green, the expiry date is displayed.

Version
The version number of the definition file currently installed on the FortiGate unit for this service.

(Last update date and method)
The date of the last update and method used for last attempt to download definition updates for this service.

[Update]
Select to manually update this service on your FortiGate unit. This will prompt you to download the update file from your local computer. To download updates from FDN directly, use the Update Now control.

(Date)
Local system date when the FortiGate unit last checked for updates for this service.

AntiVirus and IPS Downloads
Select the blue arrow to display or hide this section. See "AntiVirus and IPS Downloads" on page 190.

Web Filtering and AntiSpam Options
Select the blue arrow to display or hide this section. See "Web Filtering and AntiSpam Options" on page 192.

IPS Options
Select the blue arrow to display or hide this section.
Select to send attack details to FSN to improve IPS signature quality.
Fortinet recommends that you enable this feature.

Management & Analysis Service Options
Select the blue arrow to display or hide this section.
Enter your Account ID that you were given when you registered for this service.
If you are not connected to a FortiGuard FortiAnalyzer unit or subscribed to the FortiGuard Analysis Service, there will be no content in this section.
If you do not have an account ID, register for the FortiGuard Management Service with customer service.
For more information, see “Enabling push updates through a NAT device” on page 196.

Figure 110: AntiVirus and IPS Options section

- **Use override server address**: Select to configure an override server if you cannot connect to the FDN or if your organization provides updates using their own FortiGuard server. When selected, enter the IP address or domain name of a FortiGuard server and select Apply. If the FDN Status still indicates no connection to the FDN, see “Troubleshooting FDN connectivity” on page 193.

- **Allow Push Update**: Select to allow push updates. Updates will be sent to your FortiGate unit when they are available without you checking if they are available. Push Update Status Icon shows the status of the push update service.

- **Push Update Status Icon**: The status of the FortiGate unit for receiving push updates:
  - grey - unreachable: FortiGate unit is not able to connect to push update service
  - yellow - not available: push update service is not available with current support license
  - green - available: push update service is allowed. See “To enable push updates” on page 195.

  If the icon is either grey or yellow, see “Troubleshooting FDN connectivity” on page 193.

- **Use override push**: Enable if there is a NAT device between the FortiGate unit and the FDS. Override push allows you to create a forwarding policy that redirects incoming FDS push updates to your FortiGate unit. The NAT device must be configured to forward the FDS traffic to the FortiGate unit, including UDP port 9443. See “Enabling push updates through a NAT device” on page 196. Available only if Allow Push Update is selected.

- **IP**: Enter the IP address of the NAT device in front of your FortiGate unit. FDS will connect to this device when attempting to reach the FortiGate unit. Available only if Use override push is enabled.

- **port**: Select the port on the NAT device that will receive the FDS push updates. This port must be forwarded to UDP port 9443 on the FortiGate unit. Available only if Use override push is enabled.

- **Scheduled Update**: Select this check box to enable scheduled updates.

  - **Every**: Attempt to update once every 1 to 23 hours. Select the number of hours between each update request.

  - **Daily**: Attempt to update once a day. You can specify the hour of the day to check for updates. The update attempt occurs at a randomly determined time within the selected hour.
Weekly  Attempt to update once a week. You can specify the day of the week and the hour of the day to check for updates. The update attempt occurs at a randomly determined time within the selected hour.

Update Now  Select Update Now to manually initiate an FDN update.

Web Filtering and AntiSpam Options

Select the blue arrow next to Web Filtering and AntiSpam Options to access this section.

Figure 111: Web Filtering and AntiSpam Options section

Enable Web Filter  Select to enable FortiGuard Web Filter service.
Enable Cache  Select to enable caching FortiGuard Services information. This improves performance by reducing FortiGate unit requests to the FortiGuard server. The cache uses 6% of the FortiGate memory. When the cache is full, the least recently used IP address or URL is deleted. Available only if Enable Web Filter is selected.
TTL  Time to live. The number of seconds to store blocked IP addresses and URLs in the cache before contacting the server again. Available only if both Enable Web Filter and Enable Cache are selected.

Enable Anti Spam  Select to enable FortiGuard AntiSpam service.
Enable Cache  Select to enable caching FortiGuard Services information. This improves performance by reducing FortiGate unit requests to the FortiGuard server. The cache uses 6% of the FortiGate memory. When the cache is full, the least recently used IP address or URL is deleted. Available only if Enable Anti Spam is selected.
TTL  Time to live. The number of seconds to store blocked IP addresses and URLs in the cache before contacting the server again.

Use Default Port (53)  Select to use port 53 to communicate with FortiGuard Antispam servers.
Use Alternate Port (8888)  Select to use port 8888 to communicate with FortiGuard Antispam servers.
Test Availability  Select to test the connection to the FortiGuard Antispam server. Results are shown below the button and on the Status indicators.
please click here  Select to re-evaluate a URL’s category rating on the FortiGuard Web Filter service.
Management & Analysis Service Options

This section displays your configuration options for the FortiGuard Management and Log & Analysis services.

Select the blue arrow next to Log & Analysis Options to access this section.

Figure 112: FDN Log & Analysis options

Enter the Account ID you were given when you registered for your service or services with Fortinet Support.

This section provides links to “Logging to a FortiGuard Analysis server” on page 479 where you can configure your settings, and to purge your logs.

To configure how often to purge your logs, select how old the logs should be in months before being purged.

Troubleshooting FDN connectivity

If your FortiGate unit is unable to connect to the FDN, check your configuration. For example, you may need to add routes to the FortiGate routing table or configure your network to allow the FortiGate unit to use HTTPS on port 443 to connect to the Internet.

You might have to connect to an override FortiGuard server to receive updates. See “To add an override server” on page 194. If this is not successful, check your configuration to make sure you can connect to the override FortiGuard server from the FortiGate unit.

Push updates might be unavailable if:

• you have not registered the FortiGate unit (To register your FortiGate unit, go to Product Registration and follow the instructions.)
• there is a NAT device installed between the FortiGate unit and the FDN (see “Enabling push updates through a NAT device” on page 196)
• your FortiGate unit connects to the Internet using a proxy server (see “To enable scheduled updates through a proxy server” on page 195).

Updating antivirus and attack definitions

Use the following procedures to configure the FortiGate unit to connect to the FortiGuard Distribution Network (FDN) to update the antivirus (including grayware) definitions and attack definitions.

To make sure the FortiGate unit can connect to the FDN

1 Go to System > Status and select Change on the System Time line in the System Information section.

2 Make sure that the time zone is set correctly for the region in which your FortiGate unit is located.

3 Go to System > Maintenance > FortiGuard Center.
4 Select Refresh.
   The FortiGate unit tests its connection to the FDN. The test results are displayed at the top of the System Update page.

**To update antivirus and attack definitions**

1 Go to System > Maintenance > FortiGuard Center.
2 Select Update Now to update the antivirus and attack definitions.
   If the connection to the FDN or override server is successful, the web-based manager displays a message similar to the following:
   
   Your update request has been sent. Your database will be updated in a few minutes. Please check your update page for the status of the update.

   After a few minutes, if an update is available, the System Update Center page lists new version information for antivirus definitions and attack definitions. The System Status page also displays new dates and version numbers for antivirus, attack and IPS definitions. Messages are recorded to the event log indicating whether the update was successful or not.

   **Note:** Updating antivirus and attack definitions can cause a very short disruption in traffic currently being scanned while the FortiGate unit applies the new signature database. To minimize this possibility, schedule updates for times of light traffic.

**To enable scheduled updates**

1 Go to System > Maintenance > FortiGuard Center.
2 Select the Scheduled Update check box.
3 Select one of the following to check for and download updates.

   - **Every** Once every 1 to 23 hours. Select the number of hours and minutes between each update request.
   - **Daily** Once a day. You can specify the time of day to check for updates.
   - **Weekly** Once a week. You can specify the day of the week and the time of day to check for updates.

4 Select Apply.
   The FortiGate unit starts the next scheduled update according to the new update schedule.

   Whenever the FortiGate unit runs a scheduled update, the event is recorded in the FortiGate event log.

**To add an override server**

If you cannot connect to the FDN, or if your organization provides antivirus and attack updates using their own FortiGuard server, you can use the following procedure to add the IP address of an override FortiGuard server.

1 Go to System > Maintenance > FortiGuard Center.
2 Select the Use override server address check box.
3 Type the fully qualified domain name or IP address of a FortiGuard server.
4 Select Apply.

The FortiGate unit tests the connection to the override server.

If the FortiGuard Distribution Network availability icon changes from grey, the FortiGate unit has successfully connected to the override server.

If the FortiGuard Distribution Network availability icon stays gray, the FortiGate unit cannot connect to the override server. Check the FortiGate configuration and network configuration for settings that would prevent the FortiGate unit from connecting to the override FortiGuard server.

To enable scheduled updates through a proxy server

If your FortiGate unit must connect to the Internet through a proxy server, you can use the `config system autoupdate tunneling` command to allow the FortiGate unit to connect (or tunnel) to the FDN using the proxy server. For more information, see the FortiGate CLI Reference.

### Enabling push updates

The FDN can push updates to FortiGate units to provide the fastest possible response to critical situations. You must register the FortiGate unit before it can receive push updates. To register your FortiGate unit, go to Product Registration and follow the instructions.

When you configure a FortiGate unit to allow push updates, the FortiGate unit sends a SETUP message to the FDN. The next time new antivirus or attack definitions are released, the FDN notifies all FortiGate units that are configured for push updates that a new update is available. Within 60 seconds of receiving a push notification, the FortiGate unit requests an update from the FDN.

**Note:** Push updates are not supported if the FortiGate unit must use a proxy server to connect to the FDN. For more information, see “To enable scheduled updates through a proxy server” on page 195.

When the network configuration permits, configuring push updates is recommended in addition to configuring scheduled updates. On average the FortiGate unit receives new updates sooner through push updates than if the FortiGate unit receives only scheduled updates. However, scheduled updates make sure that the FortiGate unit receives the latest updates.

Enabling push updates is not recommended as the only method for obtaining updates. The FortiGate unit might not receive the push notification. Also, when the FortiGate unit receives a push notification it makes only one attempt to connect to the FDN and download updates.

**To enable push updates**

1 Go to **System > Maintenance > FortiGuard Center**.
2 Select Allow Push Update.
3 Select Apply.
Push updates when FortiGate IP addresses change

The SETUP message that the FortiGate unit sends when you enable push updates includes the IP address of the FortiGate interface to which the FDN connects. The interface used for push updates is the interface configured in the default route of the static routing table.

The FortiGate unit sends the SETUP message if you change the IP address of this interface manually or if you have set the interface addressing mode to DHCP or PPPoE and your DHCP or PPPoE server changes the IP address.

The FDN must be able to connect to this IP address for your FortiGate unit to be able to receive push update messages. If your FortiGate unit is behind a NAT device, see “Enabling push updates through a NAT device” on page 196.

If you have redundant connections to the Internet, the FortiGate unit also sends the SETUP message when one Internet connection goes down and the FortiGate unit fails over to the other Internet connection.

In Transparent mode if you change the management IP address, the FortiGate unit also sends the SETUP message to notify the FDN of the address change.

Enabling push updates through a NAT device

If the FDN can only connect to the FortiGate unit through a NAT device, you must configure port forwarding on the NAT device and add the port forwarding information to the push update configuration. Using port forwarding, the FDN connects to the FortiGate unit using UDP on either port 9443 or an override push port that you specify.

Note: You cannot receive push updates through a NAT device if the external IP address of the NAT device is dynamic (for example, set using PPPoE or DHCP).
General procedure

Use the following steps to configure the FortiGate unit on the internal network and the NAT device so that the FortiGate unit on the internal network can receive push updates:

1. Register and license the FortiGate unit on the internal network so that it can receive push updates.
2. Configure the FortiGuard Center of the FortiGate unit on the internal network.
   - Allow push updates
   - Add an override push update IP. Usually this would be the IP address of the external interface of the NAT device
   - If required, change the override push update port
3. Add a port forwarding virtual IP to the NAT device.
   - Set the external IP address of the virtual IP to match the override push update IP. Usually this would be the IP address of the external interface of the NAT device.
4. Add a firewall policy to the FortiGate NAT device that includes the port forwarding virtual IP.

To configure the FortiGuard Center of the FortiGate unit on the internal network

1. Go to System > Maintenance > FortiGuard Center.
2. Select Allow Push Update.
3 Select Use override push IP and enter the IP address of the external interface of the NAT device.

4 Do not change the push update port unless UDP port 9443 is blocked or used by other services on your network.

5 Select Apply.

The FortiGate unit sends the override push IP address and port to the FDN. The FDN now uses this IP address and port for push updates to the FortiGate unit on the internal network. Push updates will not actually work until you add a virtual IP to the NAT device so that the NAT device accepts push update packets and forwards them to the FortiGate unit on the internal network.

**Note:** If the external IP address or external service port changes, add the changes to the Use override push configuration and select Apply to update the push information on the FDN.

---

### To add a port forwarding virtual IP to the FortiGate NAT device

Configure the NAT device to use port forwarding to forward push update connections from the FDN to the FortiGate unit on the internal network.

1 Go to **Firewall > Virtual IP** and select **Create New**.

2 Add a port forwarding virtual IP that maps the external interface of the NAT device to the IP address of the FortiGate unit on the internal network using the push update UDP port.

   - **Name**: Add a name for the Virtual IP.
   - **External Interface**: The interface on the NAT device that connects to the Internet.
   - **Type**: Static NAT.
   - **External IP Address/Range**: The IP address that the FDN connects to send push updates to the FortiGate unit on the Internal network. This would usually be the IP address of the external interface of the NAT device. This IP address must be the same as the FortiGuard Center push update override IP of the FortiGate unit on the internal network.
   - **Mapped IP Address/Range**: The IP address of the FortiGate unit on the Internal network.
   - **Port Forwarding**: Select Port Forwarding.
   - **Protocol**: UDP
   - **External Service Port**: The external service port that the FDN connects to. The external service port for push updates is usually 9443. If you changed the push update port in the FortiGuard Center configuration of the FortiGate unit on the internal network, you must set the external service port to the changed push update port.
   - **Map to Port**: The map to port must be the same as the external service port.

3 Select OK.

---

### To add a firewall policy to the FortiGate NAT device

1 Add a new external to internal firewall policy.

2 Configure the policy with the following settings:

3 Select OK.
To confirm that push updates to the FortiGate unit on the internal network are working

1. Go to **System > Maintenance > FortiGuard Center**.
2. Select Refresh.

   The Push Update indicator should change to solid green.

### License

If your FortiGate unit is model 3000 or higher, you can purchase a license key from Fortinet to increase the maximum number of VDOMs to 25, 50, 100 or 250. By default, FortiGate units support a maximum of 10 VDOMs.

The license key is a 32-character string supplied by Fortinet. Fortinet requires your unit serial number to generate the license key.

Go to **System > Maintenance > License** to enter your license key.

**Figure 114: License key for additional VDOMs**

<table>
<thead>
<tr>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current License</strong></td>
</tr>
<tr>
<td><strong>Input License Key</strong></td>
</tr>
<tr>
<td><strong>Apply</strong></td>
</tr>
</tbody>
</table>

**Current License**  The current maximum number of Virtual Domains.

**Input License Key**  Enter the license key supplied by Fortinet and select Apply.
System Chassis (FortiGate-5000 series)

For FortiGate-5000 series modules installed in a FortiGate-5050 or FortiGate-5140 chassis, you can go to System > Chassis to view real-time operating status information about the hardware components installed in the chassis.

From the system chassis pages you can view information about all of the hardware components in the chassis. You can use the `get chassis status` command to display similar chassis information from the FortiGate CLI.

Information displayed by the system chassis pages and by the `get chassis status` command depends on the FortiGate-5000 series chassis and the FortiGate-5000 series modules installed in the chassis and not on the FortiGate-5000 module that you are connecting to.

The system chassis pages display information received from the chassis shelf manager. The system chassis pages only display information if at least one shelf manager is functioning in the chassis and only if the FortiGate-5000 module that you have connected to can communicate with a shelf manager.

This section describes:
- SMC (shelf manager card)
- Blades (FortiGate-5000 chassis slots)
- Chassis monitoring event log messages

SMC (shelf manager card)

Go to System > Chassis > SMC to view the status of the shelf manager cards (SMCs) installed in the FortiGate-5000 series chassis. The SMC list is the same for the FortiGate-5140 chassis and the FortiGate-5050 chassis. The SMC list shows basic status information about the shelf manager cards in the chassis.

![Figure 115: Shelf manager card (SMC) list](image)

- **Refresh interval**: Set how often the web-based manager refreshes the information displayed on the SMC list.
- **Refresh**: Manually refresh the information displayed on the SMC list.
- **SMC #**: Shelf manager card slot number: SMC 1 or SCM 2.
- **Status**: Current status of the shelf manager card in each chassis slot. The status can be Present if a shelf manager card is installed in the slot and Empty if a shelf manager card is not installed.
- **Active/Standby**: The mode of the shelf manager card in each chassis slot. Shelf managers can operate in active or standby mode. In active mode the shelf manager is operating the chassis. In standby mode the shelf manager is waiting to switch to active mode if it detects that the active shelf manager is not operating. If status is empty, active/standby is blank.
Blades (FortiGate-5000 chassis slots)

Go to System > Chassis > Blades to display a list of the slots in the FortiGate-5000 chassis that the FortiGate-5000 series module is installed in. The list of slots shows whether the slot is empty or contains a FortiGate-5000 module. If a slot contains a module, the display shows the type of module in the slot. Slots can contain node cards such as the FortiGate-5001SX module and switch cards such as the FortiSwitch-5003 module. The slot containing the FortiGate-5000 module that you are connecting to is highlighted in yellow.

If the FortiGate-5000 series module that you are connecting to is installed in a FortiGate-5050 chassis, the blades list contains 5 rows. For a FortiGate-5140 chassis the blades list contains 14 rows.

For each slot that contains a module, the blades list indicates if the monitored temperatures and voltages for the module in that slot are within acceptable ranges. If temperature and voltage show good, the module is operating with acceptable ranges. If temperature or voltage show alarm, the shelf manager has registered an alarm because a temperature or voltage is outside of the acceptable range.

If you have SNMP enabled and have selected the Temperature too high and Voltage out of range SNMP events, when the shelf manager registers a temperature or voltage alarm, the FortiGate-5000 module SNMP agent sends an SNMP trap.

Figure 116: Example FortiGate-5050 blades list

<table>
<thead>
<tr>
<th>Slot #</th>
<th>Blade Type</th>
<th>Temperature</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Empty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Empty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Node Card</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>2</td>
<td>Switch Card</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>1</td>
<td>Empty</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Refresh interval Set how often the web-based manager refreshes the information displayed on the blades list.

Refresh Manually refresh the information displayed on the blades list.

Slot # The slot number in the chassis. Slots 1 to 5 are listed for the FortiGate-5050 chassis and slots 1 to 14 are listed for the FortiGate-5140 chassis.

Blade Type Indicates whether the slot contains a node card (for example, a FortiGate-5001SX module) or a switch card (for example, a FortiSwitch-5003 module).
Temperature

Indicates if the temperature sensors for the module in each slot are detecting a temperature within an acceptable range. Good indicates that all monitored temperatures are within acceptable ranges. Alarm indicates that a monitored temperature is too high (usually about 75°C) or too low (below 10°C).

You can mouse over the temperature indicator to view the temperatures being read by each sensor on the module. The mouse over display includes the name of the temperature sensor and the temperature reading.

The temperatures that are displayed depend on the FortiGate or FortiSwitch module. For example:

For FortiGate-5005FA2 modules:
- Incoming Air-Flow: 37°C
- CPU Board Temp: 49°C
- CPU1 Temp: 65°C
- CPU2 Temp: 66°C

For FortiGate-5001SX and FortiGate-5001FA2 modules:
- TEMP1: 37°C
- TEMP2: 30°C

And for FortiSwitch-5003 modules:
- Baseboard Temp: 35°C
- Board (BRD) Top Temp: 33°C
- BRD Bottom Temp: 33°C
- BRD Center Temp: 38°C
Chassis monitoring event log messages

FortiGate-5000 series modules can send the log messages shown in Table 31 when chassis monitoring detects temperatures, voltages, or fan speeds that are outside of normal operating parameters. The messages in Table 31 all have the chassis log type and a severity of warning or critical. Warning messages are recorded when non-critical thresholds are reached. Critical messages are recorded when critical thresholds are reached.
Table 31: Chassis monitoring warning and critical event log messages

<table>
<thead>
<tr>
<th>ID</th>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>99503</td>
<td>Chassis fan anomaly: Fan &lt;fan_integer&gt;, &lt;rpm_integer&gt; RPM</td>
<td>A chassis fan is operating at an RPM value outside of the normal operating range. &lt;fan_integer&gt; is the number of the fan tray. For the FortiGate-5140 &lt;fan_integer&gt; can be 0, 1, or 2. The FortiGate-5050 only has one fan tray. &lt;rpm_integer&gt; is the RPM at which the fan is operating.</td>
</tr>
<tr>
<td></td>
<td>Chassis fan anomaly</td>
<td></td>
</tr>
<tr>
<td>99504</td>
<td>Chassis temperature anomaly: T &lt;sensor_integer&gt;, &lt;temp_integer&gt; Celsius</td>
<td>A temperature sensor has reported a temperature outside of the normal operating range for this sensor. A typical operating range is between 10 and 75 degrees Celsius. &lt;temp_integer&gt; identifies the temperature sensor. &lt;temp_integer&gt; is the temperature being reported by the sensor.</td>
</tr>
<tr>
<td>99505</td>
<td>Chassis voltage anomaly: V&lt;design_voltage&gt;, &lt;monitored_voltage&gt; V</td>
<td>A chassis voltage sensor has detected a voltage level outside of the operating range for the sensor. &lt;design_voltage&gt; is the voltage the circuit should have at the sensor location during normal operation. For example, &lt;design_voltage&gt; could be 3.3, 5, and so on. &lt;monitored_voltage&gt; is the actual voltage measured by the sensor.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>99506</td>
<td>Blade fan anomaly: Fan &lt;fan_integer&gt;, &lt;rpm_integer&gt; RPM</td>
<td>A blade fan is operating at an RPM value outside of the normal operating range. &lt;fan_integer&gt; identifies the fan. &lt;rpm_integer&gt; is the RPM at which the fan is operating.</td>
</tr>
<tr>
<td>99507</td>
<td>Blade temperature anomaly: Blade &lt;temp_integer&gt;, &lt;temp_integer&gt; Celsius</td>
<td>A temperature sensor on a FortiGate-5000 or FortiSwitch-5000 series module has reported a temperature outside of the normal operating range for this sensor. A typical operating range is between 10 and 75 degrees Celsius. &lt;temp_integer&gt; identifies the module temperature sensor. &lt;temp_integer&gt; is the temperature being reported by the sensor.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>99508</td>
<td>Blade voltage anomaly: Blade &lt;design_voltage&gt;, &lt;monitored_voltage&gt; V</td>
<td>A voltage sensor on a FortiGate-5000 or FortiSwitch-5000 series module has detected a voltage level outside of the operating range for the sensor. &lt;design_voltage&gt; is the voltage the circuit should have at the sensor location during normal operation. For example, &lt;design_voltage&gt; could be 3.3, 5, and so on. &lt;monitored_voltage&gt; is the actual voltage measured by the sensor.</td>
</tr>
</tbody>
</table>
Switch (FortiGate-224B only)

This section describes how to configure the switch portion of your FortiGate-224B unit. The following topics are included in this section:

- Overview
- Enabling switch view
- Viewing WAN ports and WAN VLAN interfaces
- Viewing switch-LAN ports
- Viewing switch VLANs
- Configuring port monitoring
- Using Spanning-Tree Protocol
- Configuring IGMP snooping
- Configuring QoS
- Configuring port quarantine
- Configuring dynamic policies
- Configuring 802.1X authentication
- Viewing switch status

Overview

The FortiGate-224B unit contains all of the functionality of the Fortinet FortiGate product family plus it can provide security and enhanced functionality for your local switched LAN.

The FortiGate-224B firmware has two views:

- firewall view - the unit is the same as other FortiGate models, except that it has 28 network interfaces. This is the default mode.
- switch mode - port1 through port26 are switch ports on the swlan interface. The web-based manager Switch menu is available, providing access to enhanced security features. HA is not supported.

The switch portion of the FortiGate-224B unit is by default a single FortiGate interface, native. You can configure firewall policies to permit communication with other interfaces, applying antivirus and IPS scanning as needed.

For security within the native network, you have several options:

- Create switch VLANs. Configure firewall policies from each switch VLAN to other switch VLANs and other interfaces to control and protect traffic.
- Create secure ports on native and its switch VLANs. A secure switch port is subject to FortiGate firewall policies and protection profiles. Configure firewall policies to control and protect traffic between switch ports.
Enabling switch view

You must enable switch view to make the switch features available and to enable you to create intra-VLAN firewall policies. You must use the CLI to enable switch view.

To enable switch view

In the CLI, enter the following commands:

```
config system global
    set switch-view enable
end
```

When asked if you want to continue, respond y. The system resets and restores factory default values. You might have to use the console to restore the appropriate IP address and enable administrative access for the web-based manager.

To return to firewall mode, use the CLI commands shown above, but set `switch-view` to disable.

Viewing WAN ports and WAN VLAN interfaces

FortiGate-224B WAN1 and WAN2 ports are the same as network interfaces on other FortiGate models. Go to System > Network > Interface to view and configure the WAN ports and WAN VLAN interfaces. See "Interface" on page 79.

Note: Virtual Domain (VDOM) and Transparent mode do not apply to the FortiGate-224B.
Viewing switch-LAN ports

Go to **Switch > Port > Interface** to view and configure the Switch LAN ports. You can also view and configure WAN ports from this page.

**Figure 117: Viewing the switch-LAN ports**

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>VLAN Membership (VID)</th>
<th>Status</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe01</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe02</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe03</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe04</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe05</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe06</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe07</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe08</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe09</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe10</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe11</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe12</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe13</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe14</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe15</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe16</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe17</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe18</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe19</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe20</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe21</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe22</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe23</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>fe24</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>ge25</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
<tr>
<td>ge26</td>
<td>Access</td>
<td>1</td>
<td>🟠</td>
<td>100Half</td>
</tr>
</tbody>
</table>

**Port**
The switch port. fe01-fe24 or ge25-ge26.

**Type**
Access or Trunk

**VLAN Membership (VID)**
The VLAN to which this port belongs, identified by VLAN ID.

**Status**
Green upwards arrow - port is up
Red downwards arrow - port disabled
S - port is a secure port and subject to firewall policies
Type-inconsistent - the port is a trunk, not an access port
PVID-Inconsistent - native VLAN different at other end of trunk

**Speed**
10 or 100 Mb/s, full or half duplex, e.g., 100Full.

**Edit icon**
Edit the settings for this port.

**Refresh**
Update displayed Switch-LAN port information.
Configuring a switch-LAN interface

To configure a switch-LAN interface go to **Switch > Port > Interface** and select the Edit icon for the Switch-LAN interface you want to reconfigure.

**Figure 118: Switch-LAN interface settings**

<table>
<thead>
<tr>
<th>Edit Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Mode</td>
</tr>
<tr>
<td>Native VLAN</td>
</tr>
<tr>
<td>Speed</td>
</tr>
<tr>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>Edge Port</td>
</tr>
</tbody>
</table>
| Link Type      | Select one of the following:  
|                | Shared LAN - a typical LAN with multiple devices  
|                | Point-to-Point LAN - a point-to-point link  
|                | Auto - type of link is determined automatically |
| 802.1x          | Enable or disable 802.1X authentication on this port. For complete 802.1X configuration, see “Configuring 802.1X authentication” on page 226. |
| RADIUS VLAN assignment |
| Secure Port    | Enable Secure Port if you want to create firewall policies to govern the intra-VLAN traffic to and from this port. For information about intra-VLAN firewall policies, see “Configuring intra-VLAN firewall policies (FortiGate-224B only)” on page 275. |
Viewing switch VLANs

A switch VLAN is similar to a VLAN on any other interface, but applies only to selected ports on the native interface. Go to **Switch > Port > VLAN** to view a list of the current switch VLANs and to create new switch VLANs.

**Figure 119: Viewing list of switch VLANs**

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>Member Ports</th>
<th>SVI IP/Mask</th>
<th>Root Port</th>
<th>STP</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>VLAN04</td>
<td>fe02, 10, 21, 22</td>
<td>10.12.1.1/255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>VLAN07</td>
<td>fe14, 15, 16, 17, 18, 19, 20</td>
<td>10.11.1.1/255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>VLAN100</td>
<td>fe03, 4</td>
<td>10.16.1.1/255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>VLAN33</td>
<td>fe07, 8, 9, 11, 12</td>
<td>11.20.20.0/255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>native</td>
<td>fe01, 5, 6, 13, 20, 24, ge25, ge26</td>
<td>190.160.5.99/255.255.255.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Create New**
Create a new switch VLAN interface. See “Configuring a switch VLAN” on page 212.

**VLAN ID**
The VLAN identifier.

**Name**
The name of this VLAN.

**Member Ports**
A list of the ports that belong to this VLAN. For trunk ports, “(N)” indicates the native VLAN, “(t)” indicates the tagged VLAN.

**SVI IP/Mask**
The Switch Virtual Interface used for routing.

**Root Port**
The current root port for the VLAN when Spanning Tree Protocol is in effect.

**STP**
Enable Spanning Tree Protocol on this VLAN. This is available only when STP mode is PVST+.
To configure STP settings, see “Configuring Spanning-Tree settings” on page 214.

**Delete icon**
Delete the VLAN. You cannot delete VLAN 1.

**Edit icon**
Edit the settings for a VLAN. See “Configuring a switch VLAN” on page 212.
Configuring a switch VLAN

Go to Switch > Port > VLAN and select Create New to create a new switch VLAN. You can also modify an existing VLAN by selecting its Edit icon.

Figure 120: Creating a new VLAN

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for this VLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Enter the VLAN ID for this switch VLAN. Do not use any of the reserved VLAN IDs. By default, VLAN IDs 4020 through 4044 are reserved.</td>
</tr>
<tr>
<td>Virtual Interface</td>
<td>Enable or disable having a virtual address for this port.</td>
</tr>
<tr>
<td>Virtual IP/Netmask</td>
<td>If you enable Virtual Interface, enter the Virtual IP address and netmask.</td>
</tr>
<tr>
<td>Available Ports</td>
<td>A list of the switch ports that do not already belong to a VLAN. To add a port to the Member Ports list, select it and then select the right-pointing arrow button.</td>
</tr>
<tr>
<td>Member Ports</td>
<td>A list of the switch ports that belong to this VLAN. To remove a port from the list, select it and then select the left-pointing arrow button.</td>
</tr>
<tr>
<td>Administrative Access</td>
<td>Select the types of administrative access permitted on this port. Ping access enables response to ping requests for testing.</td>
</tr>
</tbody>
</table>
Configuring port monitoring

Switch Port Analysis (SPAN) enables you to analyze network traffic passing through switch ports by sending a copy of the traffic to a port connected to remote monitoring equipment.

FortiGate-224B supports two Span sessions: Ingress (traffic to the port) and Egress (traffic from the port). You configure ports to receive the Ingress and Egress SPAN session data. You can use one port for both sessions or use two different ports. For the remaining ports, you choose whether to monitor them in the Ingress or Egress session or both, or not to monitor them at all.

Note: Egress traffic is stripped of its VLAN ID tag if the Egress port has a different VLAN ID than the monitored traffic.

Go to Switch > Port > SPAN to configure port monitoring.

Figure 121: Monitoring ports

### MTU
This field is available only on physical interfaces. To improve network performance, you can change the maximum transmission unit (MTU) of the packets that the FortiGate unit transmits. Ideally, the MTU should be the same as the smallest MTU of all the networks between the FortiGate unit and the destination of the packets. If the packets that the FortiGate unit sends are larger, they are broken up or fragmented, which slows down transmission. Experiment by lowering the MTU to find an MTU size for best network performance.

To change the MTU, select Override default MTU value (1500) and enter the maximum packet size. The MTU size range is 68 to 1500 bytes for manual mode, 576 to 1500 bytes for DHCP mode, and 576 to 1492 bytes for PPPoE mode.

### Log
Select Log to record logs for any traffic to or from the interface. To record logs you must also enable traffic log for a logging location and set the logging severity level to Notification or lower. Go to Log & Report > Log Config to configure logging locations and types.

### IGMP snooping
Enable to limit flooding of multicast packets to those ports where clients have joined the relevant groups.
Using Spanning-Tree Protocol

Spanning Tree Protocol (STP) is a Layer-2 protocol that ensures that only one active path exists between any two network interfaces. This prevents loops, but if there are multiple paths, it can provide redundancy to protect against link failures.

Using information exchanged amongst switches, spanning tree protocol defines a root switch and a loop-free path from the root to each switch in the network. Redundant data paths are blocked. If a network segment fails and a redundant path exists, the spanning-tree algorithm activates the standby path. The network topology is continuously recalculated and updated.

When two interfaces on a switch are part of a loop, spanning tree protocol uses port priority and path cost settings to determine which interface is used and which is blocked.

FortiGate-224B supports three STP modes:

- **STP**: This is the traditional STP protocol defined in IEEE 802.1D-1998. In this mode, FortiGate-224B can interoperate with other switches running traditional STP.

- **RSTP**: Rapid STP as defined in IEEE 802.1D-2004. FortiGate-224B creates a single STP network that spans all VLANs. This is also referred to as Common Spanning Tree (CSTP). In this mode, FortiGate-224B can interoperate with other switches running either RSTP or traditional STP on a port-by-port basis. RSTP is the default STP mode for FortiGate-224B.

- **PVST+**: Per-VLAN STP. FortiGate-224B creates a CSTP network that covers all VLANs plus an STP network for each VLAN. In this mode, FortiGate-224B can interoperate with other switches running PVST+ that are connected by access links and 802.1Q trunks.

**Configuring Spanning-Tree settings**

Go to **Switch > Protocols > Spanning-Tree** to configure Spanning Tree settings.

**Figure 122: Spanning Tree Protocol settings - STP or RSTP**
Enable Spanning-Tree

Select one of:
- STP Basic Spanning Tree Protocol
- RSTP Rapid Spanning Tree Protocol (default)
- PVST+ Per-VLAN Spanning Tree Protocol

Table of STP Instances

In STP and RSTP mode, there is only one row in the table to describe the Common Spanning Tree (CST).
In PVST+ mode, the table lists the per-VLAN STP instances.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Root Port</th>
<th>Root Path Cost</th>
<th>Priority</th>
<th>Root</th>
<th>Max Age</th>
<th>Hello Time</th>
<th>Forward Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>fo0/5</td>
<td>200000</td>
<td>02760</td>
<td>00:66:17:de:66:40</td>
<td>20</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>160</td>
<td>fo0/5</td>
<td>28672</td>
<td>00:69:06:ee:00:33</td>
<td>20</td>
<td>2</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>260</td>
<td>fo0/5</td>
<td>200000</td>
<td>02766</td>
<td>00:66:17:6b:64:44</td>
<td>20</td>
<td>2</td>
<td>15</td>
</tr>
</tbody>
</table>
Configuring Spanning-Tree VLAN settings

Go to **Switch > Protocols > Spanning-Tree** and select the Edit icon for a VLAN to configure Spanning Tree settings.

Figure 124: Spanning Tree Protocol VLAN settings

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>CST in STP and RSTP mode, otherwise the VLAN ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello Time</td>
<td>The interval in seconds between hello message broadcasts to other switches. The range is 1 to 10 seconds. The default is 2 seconds.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>The duration in seconds of the listening and learning states before the interface begins forwarding. The range is 4 to 30 seconds. The default is 15 seconds.</td>
</tr>
<tr>
<td>Max Age</td>
<td>The interval in seconds that the FortiGate-224B unit waits without receiving spanning-tree configuration messages before it attempts a reconfiguration. The range is 6 to 40 seconds. The default is 20.</td>
</tr>
<tr>
<td>Priority</td>
<td>The bridge priority of the root switch. The lower the value, the higher the priority. Range 0 to 61440. Default 36864. This is used for spanning tree calculations.</td>
</tr>
<tr>
<td>Port</td>
<td>fe01-24, ge25-26</td>
</tr>
<tr>
<td>State</td>
<td>One of: Disabled Not operational. This applies only to STP mode.</td>
</tr>
</tbody>
</table>
Viewing Spanning-Tree VLAN information

Go to Switch > Protocols > Spanning-Tree and select the View icon for a VLAN to view spanning-tree information about the VLAN.
Configuring Spanning-Tree VLAN port settings

Go to Switch > Protocols > Spanning-Tree, select the Edit icon for a VLAN, and then select the Edit icon for a port to configure Spanning Tree port settings.

Figure 125: Spanning Tree VLAN port settings

<table>
<thead>
<tr>
<th>Port</th>
<th>Priority</th>
<th>Path Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe01</td>
<td>224</td>
<td>0</td>
</tr>
</tbody>
</table>

Priority: Range 0 to 240 in steps of 16. Lower number is higher priority.
Path Cost: Enter the path cost or 0 to derive cost from port speed.

Configuring IGMP snooping

When IGMP snooping is enabled, the FortiGate-224B unit monitors multicast traffic and dynamically configures ports so that multicast packets are sent only to ports with clients interested in this traffic. This can help control traffic through the switch.

Go to Switch > Protocols > IGMP Snooping to configure IGMP settings.

Figure 126: IGMP settings

Enable IGMP snooping: Enable IGMP snooping. You must also enable IGMP Snooping on switch-VLANs. See “Configuring a switch VLAN” on page 212.

Configuring QoS

Quality of Service (QoS) settings enable you to prioritize network traffic by type. Inter-Switch Link (ISL) trunk frames carry IEEE 802.1P Class of Service (CoS) information. You can use this to set priorities and rate limiting for traffic by type. FortiGate-224B also supports the use of Layer-3 Differentiated Services Code Point (DSCP) values to prioritize traffic.

Configuring QoS settings

Go to Switch > Qos > Config to configure QoS settings.

Figure 127: QoS queue settings
Configuring CoS-Map settings

Go to Switch > QoS > CoS-Map to configure CoS-Map settings.

For each 802.1p priority, you can select CoS Queue-1 through Queue-4.

Configuring DSCP-Map settings

Differentiated Services Code Point (DSCP)

Go to Switch > QoS > DSCP-Map to configure DSCP-Map settings.

Enter the DSCP value, select the queue and then select Add to create a new entry in the table. In the table, you can remove an entry by selecting the Delete icon.

Viewing QoS rate limits

Go to Switch > QoS > Rate Limiting to configure rate limits.

Create New Add a rate limit entry. See “Adding a QoS rate limit” on page 220.

Port Port number: fe01-fe24, ge25-26.
Configuring port quarantine

Access control pre-screens clients to determine the security of their computers. When the client connects to the switch port using a web browser, FortiGate-224B downloads an ActiveX control to perform security checks on the computer. Depending on the client profile that applies to this port, this host check can check for

- antivirus software
- firewall software
- up-to-date operating system software

If the client passes the host check, the computer is granted access to the network. If the client fails the host check, there are several optional actions:

- Deny access.

Adding a QoS rate limit

Go to Switch > QoS > Rate Limiting and select Create New to configure rate limits.

Figure 131: Adding a QoS rate limit

<table>
<thead>
<tr>
<th>Port</th>
<th>fe01-fe24, ge25-26</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Mode</td>
<td>Select one of:</td>
</tr>
<tr>
<td></td>
<td>Broadcast + Multicast + Flooded Unicast</td>
</tr>
<tr>
<td></td>
<td>Broadcast + Multicast</td>
</tr>
<tr>
<td></td>
<td>Broadcast</td>
</tr>
<tr>
<td></td>
<td>All</td>
</tr>
<tr>
<td>Ingress Limit</td>
<td>Select desired maximum rate</td>
</tr>
<tr>
<td>Egress Limit</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>
- Quarantine the switch port to which the user is connected. Allow a re-check of the computer after installing or activating the required software. For information about quarantine, see “Configuring dynamic policies” on page 224.
- Dynamic profile. Provide access to the network using a specified protection profile. The FortiGate-224B unit applies antivirus scanning, IPS and content filtering as specified in the protection profile. Optionally, you can make the client’s port a secure port. It is then subject to firewall policies. For information about dynamic policies, see “Viewing access policies” on page 222.
- Allow. Permit network access in spite of failed host check.

Viewing client profiles

The FortiGate-224B host check uses an ActiveX control to determine the security of the client computer. When the user connects to the port with a web browser, the ActiveX control is downloaded and checks the client system’s AV software, firewall software and operating system, depending on the detection settings.

Go to Switch > Port Quarantine > Client Profile to configure access control host checks.

Figure 132: Client profile list

| Create New | Create a new client profile. See “Configuring a client profile” on page 221. |
| Name | The name of the client profile. |
| Detect Items | The types of host check this profile includes: Antivirus (AV), Firewall, OS check. See “Configuring a client profile” on page 221. |
| Delete icon | Delete the profile. You cannot delete a profile that is used in a Strict or Dynamic policy. |
| Edit icon | Edit the profile. |

Configuring a client profile

Go to Switch > Port Quarantine > Client Profile and select Create New to create a client profile or select the Edit icon of an existing profile to modify it.

Figure 133: Configuring a client profile
Viewing access policies

Go to Switch > Port Quarantine > Strict Policy to view, modify or create new access policies for switch ports. These policies perform host checking according to the selected profile and apply the selected action if the client fails the host check.

Dynamic profile applies an existing protection profile to the user and monitors the port. The port is quarantined if a virus or other form of attack is detected.

Figure 134: Viewing and editing access policies

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the detection rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable any of the following as needed:</td>
<td></td>
</tr>
<tr>
<td>FortiClient AV Check</td>
<td>Check that FortiClient Host Security is installed and running.</td>
</tr>
<tr>
<td>FortiClient Firewall Check</td>
<td>Check that the FortiClient Host Security firewall is enabled.</td>
</tr>
<tr>
<td>Enable OS Check</td>
<td>Check for operating system version. Select acceptable operating systems. For Windows XP and Windows 2000 you can select the minimum acceptable service pack.</td>
</tr>
<tr>
<td>Third-Party AV Check</td>
<td>Check that one of the following products is installed:</td>
</tr>
<tr>
<td>Third-Party Firewall Check</td>
<td>• Norton Internet Security 2006</td>
</tr>
<tr>
<td></td>
<td>• Trend Micro PC-cillin</td>
</tr>
<tr>
<td></td>
<td>• Mcafee</td>
</tr>
<tr>
<td></td>
<td>• Sophos anti-virus (antivirus only)</td>
</tr>
<tr>
<td></td>
<td>• Panda Platinum 2006 Internet Security</td>
</tr>
<tr>
<td></td>
<td>• F-Secure</td>
</tr>
<tr>
<td></td>
<td>• Secure Resolution (antivirus only)</td>
</tr>
<tr>
<td></td>
<td>• Cat Computer Services</td>
</tr>
<tr>
<td></td>
<td>• AHN LAB</td>
</tr>
<tr>
<td></td>
<td>• Kaspersky</td>
</tr>
<tr>
<td></td>
<td>• ZoneAlarm</td>
</tr>
</tbody>
</table>

Name

The name of this strict policy.

Client Profile

The client profile (a set of host checks) that applies to this strict policy.

Action

Action if the client fails access host check.

• Allow - access allowed anyway
• Deny - no further access allowed
• Quarantine - port is quarantined
• Dynamic-Profile - user traffic to other VLANs is scanned according to the protection profile selected in the access policy

Ports

The ports to which this strict policy applies.
Configuring an access policy

Go to Switch > Port Quarantine > Strict Policy and select Create New to configure an access policy for selected switch ports.

Figure 135: Configuring a strict access policy

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for this policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Profile</td>
<td>Select the client profile to apply with this policy.</td>
</tr>
<tr>
<td>Action</td>
<td>Select the action to take if a client fails the host check. One of:</td>
</tr>
<tr>
<td></td>
<td>• Allow - allow access anyway</td>
</tr>
<tr>
<td></td>
<td>• Deny - do not allow further access</td>
</tr>
<tr>
<td></td>
<td>• Quarantine - quarantine the port</td>
</tr>
<tr>
<td></td>
<td>• Dynamic-Profile - apply dynamic profile</td>
</tr>
<tr>
<td>Protection profile</td>
<td>If Action is Dynamic-Profile, select the protection profile to apply. Dynamic profile applies the selected protection profile and monitors the port. The port is quarantined if a virus or other form of attack is detected.</td>
</tr>
<tr>
<td>Secure port</td>
<td>Enable Secure Port on the interface automatically when the dynamic profile is in effect. You must create firewall policies to allow traffic to pass between this switch port and other interfaces.</td>
</tr>
<tr>
<td>Available Ports</td>
<td>A list of the switch ports that do not already have an access policy. To add ports to the Member Ports list for this policy, select the ports and then select the right-pointing arrow button.</td>
</tr>
<tr>
<td>Member Ports</td>
<td>A list of the switch ports that belong to this policy. To remove ports from the list, select the ports and then select the left-pointing arrow button.</td>
</tr>
</tbody>
</table>
Configuring dynamic policies

The FortiGate-224B unit can protect the network from a potential security threat by moving the affected switch port to the quarantine VLAN. This isolates devices on that switch port from the rest of the network.

The FortiGate-224B unit can quarantine a port for several different reasons:

- The host computer failed access host-check. For more information, see "Configuring port quarantine" on page 220.
- The antivirus or IPS system triggered an alert based on the activity on the port. For more information, see "Configuring a dynamic policy" on page 224.
- The administrator assigned the port to the quarantine VLAN

From the quarantine VLAN, only the quarantine web portal and selected third-party URLs are accessible. All other URL requests are redirected to the web portal. The web portal provides downloadable FortiClient Host Security or other security software. Optionally, the user can request a new host-check. If the host-check passes, the port is removed from the quarantine VLAN.

Viewing quarantine policies

Go to Switch > Port Quarantine > Dynamic Policy to configure dynamic policies for the switch ports.

Figure 136: Viewing Dynamic policies

<table>
<thead>
<tr>
<th>Name</th>
<th>AV/IPS Alert</th>
<th>Ports</th>
<th>Quarantine Portal</th>
<th>Client Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest</td>
<td>AV Bridge</td>
<td>Fe12, 13, 14, 15, 16, 17, 18</td>
<td>HostCheck</td>
<td>aa</td>
</tr>
<tr>
<td>Workstation</td>
<td>AV IPS</td>
<td>Fe01, 2, 3, 4, 5, 6</td>
<td>FortiClient URLS</td>
<td></td>
</tr>
</tbody>
</table>

Name: The name of the dynamic policy.
AV/IPS Alert: Shows whether antivirus (AV) and/or IPS protection are enabled in this dynamic policy. See "Configuring a dynamic policy" on page 224.
Ports: The ports to which this policy applies.
Quarantine Portal: Lists the Quarantine web portal settings for this policy. See "Configuring a dynamic policy" on page 224.
Client Profile: The name of the client profile. For more information, see "Configuring a client profile" on page 221.
Delete icon: Delete this dynamic policy.
Edit icon: Edit this dynamic policy.

Configuring a dynamic policy

Go to Switch > Port Quarantine > Dynamic Policy and select Create New to configure a dynamic policy. You can configure dynamic web portal page settings for selected switch ports.

Note: A dynamic policy is effective only if there is a firewall policy for the port.
Figure 137: Creating a dynamic policy

### New Dynamic Policy

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for this dynamic policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Min. Alert</td>
<td>Select the minimum IPS alert level that will trigger quarantine, or None if IPS protection is not required.</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Select to trigger quarantine if there is an antivirus alert.</td>
</tr>
</tbody>
</table>

#### Available Ports

- A list of the switch ports that do not already have a dynamic policy.
- To add a port to the Member Ports list, select it and then select the right-pointing arrow button.

#### Member Ports

- A list of the switch ports that belong to this policy.
- To remove a port from the list, select it and then select the left-pointing arrow button.

#### Portal...

- Enable FortiClient Image Download
- Allow to access third-party URLs

#### Allowed URLs

| Name | Enter the text for the link. |
| URL | Enter the URL for the link. |
| Delete icon | Select to remove link. |
| Add button | Select to add link to list. |

#### Host check and Auto-Recover

- Select to show a “Check my computer” link on the web portal page. The user selects this link to re-run the host check specified in the Client Profile.

#### Client Profile

- Select the access client profile to apply with this policy.

---

See “Configuring a client profile” on page 221.
Configuring 802.1X authentication

FortiGate-224B supports device authentication using the IEEE 802.1X standard. When 802.1X is enabled, no communication, even ARP or DHCP, is permitted until authentication is successful. Authentication is valid only on one port. If the device is moved to a different port, it must reauthenticate.

FortiGate-224B unit acts as a proxy between the host 802.1X client, called a supplicant, and the RADIUS server. When the RADIUS server replies with an authentication success message, the FortiGate-224B permits the host device to access the network.

For information about configuring the 802.1X supplicant, refer to the documentation for the supplicant. For information about configuring the RADIUS server, refer to the documentation for the RADIUS server.

You must configure the FortiGate-224B unit to access a RADIUS server to perform authentication before you configure 802.1X authentication. See “Configuring a RADIUS server” on page 381.

Go to Switch > 802.1X.

Figure 138: 802.1X settings

<table>
<thead>
<tr>
<th>Configure 802.1X</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Radius Server</strong></td>
</tr>
<tr>
<td><strong>Supplicant Timeout (sec.)</strong></td>
</tr>
<tr>
<td><strong>Server Timeout (sec.)</strong></td>
</tr>
<tr>
<td><strong>Max Re-Authentication</strong></td>
</tr>
<tr>
<td><strong>Re-Authentication Period (sec.)</strong></td>
</tr>
</tbody>
</table>

- **Radius Server**: Select the RADIUS authentication server. If needed, select Create New or go to User > RADIUS to set up a RADIUS server.
- **Supplicant Timeout (sec.)**: Enter the maximum time in seconds that the FortiGate-224B unit waits for a response from the client. The default is 30 seconds.
- **Server Timeout (sec.)**: Enter the maximum time in seconds that the FortiGate-224B unit waits for a response from the RADIUS server. The default is 15 seconds.
- **Max Re-Authentication**: Enter the maximum number of incomplete authentication attempts the FortiGate-224B unit permits from one client. The default is 2. After this number of attempts, the client’s status is unauthorized.
- **Re-Authentication Period (sec.)**: Enter the time period in seconds after which the client must reauthenticate. The default is 3600 seconds.

The table shows the authenticated clients:

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC Address</th>
<th>PAE State</th>
<th>BE State</th>
<th>Status</th>
</tr>
</thead>
</table>

- **Port**: The switch port to which the client is connected.
- **MAC Address**: The client’s MAC address.
- **PAE State**: Port Access Entity authentication status
- **BE State**: Back End state
- **Status**: Port status: Authorized or Unauthorized
Viewing switch status

You can monitor the operation of the FortiGate-224B unit switch functionality. While doing this, there are some limited actions you can take. You can:

• View access activity. You can clear the results of the host check to force a re-test of the host computer. See “Monitoring access results” on page 227.

• View the status of quarantined ports. You can remove a port from quarantine or manually quarantine a port. See “Viewing quarantine port information” on page 227.

• View the MAC table. You can add MAC table entries. See “Viewing the MAC table” on page 228.

• View traffic statistics. You can reset the statistical counters for any port. See “Viewing statistics” on page 229.

Monitoring access results

Go to Switch > Status > Strict Quarantine Result to see the results of access policies.

Figure 139: Access results

<table>
<thead>
<tr>
<th>Port</th>
<th>Detected Result</th>
<th>Remedy Action</th>
<th>Reset</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa02</td>
<td>AV: fail, FW: fail</td>
<td>Dynamic-Profiles, Dynamic-Secure Port</td>
<td>()</td>
</tr>
<tr>
<td>fa03</td>
<td>FW: fail</td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa04</td>
<td>OS: fail</td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa05</td>
<td>AV: fail, FW: fail, OS: Pass</td>
<td>Dynamic-Profiles, Dynamic-Secure Port</td>
<td>()</td>
</tr>
<tr>
<td>fa06</td>
<td></td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa07</td>
<td></td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa08</td>
<td></td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa09</td>
<td></td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa10</td>
<td></td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa11</td>
<td></td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa12</td>
<td></td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa13</td>
<td></td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa14</td>
<td></td>
<td></td>
<td>()</td>
</tr>
<tr>
<td>fa15</td>
<td></td>
<td></td>
<td>()</td>
</tr>
</tbody>
</table>

Port: The switch port.
Detected Result: The list of checks performed and the results. The tests are:
- AV - antivirus software
- FW - firewall software
- OS - operating system
The result can be either Pass or Fail.
Remedy Action: The remedy that was applied.
Reset: Clear the result for this port.

Viewing quarantine port information

Go to Switch > Status > Dynamic Quarantine Result to view information about quarantined switch ports.

Figure 140: Dynamic quarantine info

<table>
<thead>
<tr>
<th>Manually Quarantine Port(s):</th>
<th>Quarantine Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe02, fe03, fe04, fe05, fe06, fe07, fe08, fe09, fe10, fe11, fe12, fe13, fe14, fe15, fe16, fe17, fe18, fe19, fe21, fe22, fe23, fe24, fe25, fe26, fe27, fe28</td>
<td></td>
</tr>
</tbody>
</table>

Quarantined Ports:

<table>
<thead>
<tr>
<th>port</th>
<th>VLAN ID</th>
<th>Trigger</th>
<th>Time</th>
<th>Details</th>
<th>Host-Check</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>03</td>
<td>Manual</td>
<td>2006-4-13 14:53:44</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Manually Quarantine Ports

Port

To quarantine a switch port, click on its link.

VLAN ID

The switch port.

The VLAN from which the port was removed.

Trigger

The reason for the port being quarantined:

Time

The time when the port was quarantined. One of: AV (antivirus), FW (firewall), OS (Operating System), or Manual (administrator action).

Details

If the trigger is AV, this field lists the virus name.
If the trigger is IPS, this field lists the IPS anomaly.

Host-check

The host checks that were performed and the results.
Host checks are one or more of: AV (antivirus), FW (firewall) and OS (Operating System). Result is Pass or Fail.

Action

Select the Delete icon to remove the port from quarantine.

Viewing the MAC table

Go to Switch > Status > MAC-Table to view the switch MAC table.

Figure 141: Viewing the switch MAC table

<table>
<thead>
<tr>
<th>Create New</th>
<th>MAC</th>
<th>Port</th>
<th>VLAN/DBNUM</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:09:6f:00:00:01</td>
<td>fe04</td>
<td>db:1</td>
<td>dynamic</td>
</tr>
<tr>
<td>2</td>
<td>00:09:6f:00:00:02</td>
<td>db:1</td>
<td>dynamic</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>00:09:6f:00:00:03</td>
<td>fe04</td>
<td>db:220</td>
<td>dynamic</td>
</tr>
<tr>
<td>4</td>
<td>00:09:6f:00:00:04</td>
<td>fe04</td>
<td>db:220</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

Create New  Create a MAC table entry.

ID  Entry number

MAC  MAC address

Port  Switch VLAN port

VLAN/DBNUM  VLAN ID

Status  Dynamic or Static.

Creating a MAC table entry

Go to Switch > Status > MAC-Table and select Create New to add an entry to the switch MAC table.

Figure 142: Adding a MAC table entry

MAC

VLAN-ID

Port

Enter the MAC address, VLAN-ID and switch port for the MAC table entry and then select OK.
Viewing statistics

Go to Switch > Status > Statistics to view information about switch traffic.

**Figure 143: Viewing switch statistics**

<table>
<thead>
<tr>
<th>Port</th>
<th>InGood(B)</th>
<th>InBad(B)</th>
<th>InUnicast</th>
<th>InMulticast</th>
<th>InBroadcast</th>
<th>OutGood(B)</th>
<th>OutBad(B)</th>
<th>OutUnicast</th>
<th>OutMulticast</th>
<th>OutBroadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe01</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe02</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe03</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe04</td>
<td>3336</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3332</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe05</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe06</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe07</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe08</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe09</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3709</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>fe11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe14</td>
<td>253</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3332</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>fe15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe22</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fe24</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge01</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6464</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>52</td>
</tr>
</tbody>
</table>

**Port** Switch port fe01-24, ge25-26

**InGood(B)** Number of good bytes inbound.

**InBad(B)** Number of bad bytes inbound.

**InUnicast** Number of inbound unicast bytes.

**InMulticast** Number of inbound multicast bytes.

**InBroadcast** Number of inbound broadcast bytes.

**OutGood(B)** Number of good bytes outbound.

**OutBad(B)** Number of collisions.

**OutUnicast** Number of outbound unicast bytes.

**OutMulticast** Number of outbound multicast bytes.

**OutBroadcast** Number of outbound broadcast bytes.

**Delete icon** Reset the statistical counts for this port.
Router Static

This section explains some general routing concepts, how to define static routes and route policies. A route provides the FortiGate unit with the information it needs to forward a packet to a particular destination on the network. A static route causes packets to be forwarded to a destination other than the factory configured default gateway.

The factory configured static default route provides you with a starting point to configure the default gateway. You must either edit the factory configured static default route to specify a different default gateway for the FortiGate unit, or delete the factory configured route and specify your own static default route that points to the default gateway for the FortiGate unit. See “Default route and default gateway” on page 236.

You define static routes manually. Static routes control traffic exiting the FortiGate unit—you can specify through which interface the packet will leave and to which device the packet should be routed.

As an option, you can define route policies. Route policies specify additional criteria for examining the properties of incoming packets. Using route policies, you can configure the FortiGate unit to route packets based on the IP source and/or destination addresses in packet headers and other criteria such as on which interface the packet was received and which protocol (service) and/or port is being used to transport the packet.

This section describes:

• Routing concepts
• Static Route
• Policy Route

Routing concepts

Routing is a complex topic. Because the FortiGate unit works as a security device on a network and packets must pass through the FortiGate unit, you need to understand a number of basic routing concepts in order to configure the FortiGate unit appropriately.

Whether you administer a small or large network, this module will help you understand how the FortiGate unit performs routing functions.

The following topics are covered in this section:

• How the routing table is built
• How routing decisions are made
• Multipath routing and determining the best route
• How route sequence affects route priority
• Equal Cost Multipath (ECMP) Routes
• Blackhole Routing
How the routing table is built

In the factory default configuration, the FortiGate routing table contains a single static default route. You can add routing information to the routing table by defining additional static routes. The table may include several different routes to the same destination—the IP addresses of the next-hop router specified in those routes or the FortiGate interfaces associated with those routes may vary.

The FortiGate unit selects the “best” route for a packet by evaluating the information in the routing table. The best route to a destination is typically associated with the shortest distance between the FortiGate unit and the closest next-hop router. In some cases, the next best route may be selected if the best route is unavailable for some reason. The best routes are installed in the FortiGate forwarding table, which is a subset of the FortiGate routing table. Packets are forwarded according to the information in the forwarding table.

How routing decisions are made

Whenever a packet arrives at one of the FortiGate unit’s interfaces, the FortiGate unit determines whether the packet was received on a legitimate interface by doing a reverse lookup using the source IP address in the packet header. If the FortiGate unit cannot communicate with the computer at the source IP address through the interface on which the packet was received, the FortiGate unit drops the packet as it is likely an hacking attempt.

If the destination address can be matched to a local address (and the local configuration permits delivery), the FortiGate unit delivers the packet to the local network. If the packet is destined for another network, the FortiGate unit forwards the packet to a next-hop router according to a route policy and/or the information stored in the FortiGate forwarding table. See "Policy Route" on page 239.

Multipath routing and determining the best route

Multipath routing occurs when more than one entry to the same destination is present in the routing table. When multipath routing happens, the FortiGate unit may have several possible destinations for an incoming packet, forcing the FortiGate unit to decide which next-hop is the best one.

Two methods to manually resolve multiple routes to the same destination are to lower the administrative distance of one route or to set the priority of both routes. For the FortiGate unit to select a primary (preferred) route, manually lower the administrative distance associated with one of the possible routes. The administrative distance can be from 1 to 255.

Another method is to manually change the priority of both of the routes. If the next-hop administrative distances of two routes on the FortiGate unit are equal it may not be clear which route the packet will take. Configuring the priority for each of those routes will make it clear which next-hop will be used in the case of a tie. The priority for a route can only be set from the CLI. Lower priorities are preferred.
All entries in the routing table are associated with an administrative distance. If the routing table contains several entries that point to the same destination (the entries may have different gateways or interface associations), the FortiGate unit compares the administrative distances of those entries, selects the entries having the lowest distances, and installs them as routes in the FortiGate forwarding table. As a result, the FortiGate forwarding table only contains routes having the lowest distances to every possible destination. For information about how to change the administrative distance associated with a static route, see “Adding a static route to the routing table” on page 238.

**How route sequence affects route priority**

After the FortiGate unit selects static routes for the forwarding table based on their administrative distances, the sequence numbers of those routes determines routing priority. When two routes to the same destination exist in the forwarding table, the route having the lowest sequence number is the best choice.

As of FortiOS v3.0, a priority field has been added for routes that are configured using the CLI. The priority field overrides route sequence for resolving two routes with the same administrative distance. The route with the lowest value in the priority field is considered the best route. When the priority value is a tie or is not used, the best route is the route with the lowest sequence number in the routing table. The best route is also the primary route. The command to set the priority field is: `set priority <integer>` under the `config route static` command. For more information see the FortiGate CLI Reference.

When you add a static route to the Static Route list through the web-based manager, the FortiGate unit assigns the next unassigned sequence number to the new entry automatically. For example, in Figure 144, two static routes to the same destination (1.1.1.0/24) were created to illustrate how entry numbers and sequence numbers are assigned through the web-based manager. The two routes specify the same gateway, but in one case, the packet would leave the FortiGate unit through the interface named “port1”, and in the second case, the packet would leave the FortiGate unit through the interface named “port2”.

**Figure 144: Static routes created through the web-based manager**

<table>
<thead>
<tr>
<th>IP</th>
<th>Mask</th>
<th>Gateway</th>
<th>Device</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>172.20.128.2</td>
<td>port1</td>
<td>10</td>
</tr>
<tr>
<td>1.1.1.0</td>
<td>255.255.255.0</td>
<td>192.168.100.1</td>
<td>port1</td>
<td>2</td>
</tr>
<tr>
<td>1.1.1.0</td>
<td>255.255.255.0</td>
<td>192.168.100.1</td>
<td>port2</td>
<td>2</td>
</tr>
</tbody>
</table>

Entry number 2 was created first and entry number 3 was created second, so their sequence numbers in the routing table are 2 and 3 respectively. When the FortiGate unit evaluates these two routes to the same destination, both will be added to the forwarding table because they have low administrative distances. After a route has been added to the forwarding table, its sequence number determines the priority of the route unless its priority was set in the CLI with the `set priority` command. Because entry number 2 has the lowest sequence number, it is the preferred route.
Routing concepts

Note: You can display the sequence numbers of static routes in the routing table through the CLI: type `config router static, and then `get`. The sequence number of a route is equivalent to the `edit <ID_integer>` value that one enters when defining a static route through the CLI. For more information, see `config router static` in the FortiGate CLI Reference.

The order of entries in the Static Route list typically mirrors the sequence of static routes in the routing table when all static routes are configured through the web-based manager. However, because you can specify the sequence number of a static route when you add the route through the CLI, the sequence number of a route may not always match its entry number in the Static Route list. Sequence numbers can be specified for static routes through the CLI only. In summary, if a route in the routing table has a lower sequence number than another route to the same destination, the FortiGate unit will choose the route with the lower sequence number before choosing the other route. Because you can use the CLI to specify which sequence numbers or priority field settings to use when defining static routes, routes to the same destination can be prioritized according to their sequence numbers and priority field settings. For a static route to be the preferred route, you must create the route using the `config router static CLI` command and specify a low sequence number or low priority for the route.

Equal Cost Multipath (ECMP) Routes

When there is more than one route to the same destination, it can be confusing which route or routes will be installed and used. This is based on distance and priority, as explained earlier. If the distance of both routes is the same and both priorities are the same, then they are an Equal Cost Multipath (ECMP) route. If you have load balancing enabled with ECMP routes, then different sessions will use different routes to the same address to load balance traffic.

Blackhole Routing

Blackhole routing is a route that drops all traffic sent to it. It is very much like `/dev/null` in Linux programming.

Blackhole routing is used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator will not discover any information from the target system.

Blackhole routing can also be used to limit traffic on a subnet. If some addresses are not in use, traffic to those addresses (traffic which may be valid or malicious) can be directed to a blackhole for added security and lowering traffic on the subnet.

The loopback interface was added to enable easier configuration of blackhole routing. It is a virtual interface that does not forward traffic. It can only be configured from the CLI, the same way as a normal interface, but it has fewer parameters to configure and all traffic sent to it stops there. It does not suffer from hardware connection or link status problems, so it is always available. This can be useful for other dynamic routing roles. Once configured, a loopback interface can be used in firewall policies, routing, and other places that refer to interfaces. For more information see the system chapter of the FortiGate CLI Reference.
Static Route

You configure static routes by defining the destination IP address and netmask of packets that the FortiGate unit is intended to intercept, and specifying a (gateway) IP address for those packets. The gateway address specifies the next-hop router to which traffic will be routed.

Note: You can use the `config router static6` CLI command to add, edit, or delete static routes for IPv6 traffic. For more information, see the “router” chapter of the FortiGate CLI Reference.

Working with static routes

The Static Route list displays information that the FortiGate unit compares to packet headers in order to route packets. Initially, the list contains the factory configured static default route. See "Default route and default gateway" on page 236. Additional entries can be added manually.

When you add a static route to the Static Route list, the FortiGate unit evaluates the information to determine if it represents a different route compared to any other route already present in the FortiGate routing table. If no route having the same destination exists in the routing table, the FortiGate unit adds the route to the routing table.

To view the list of static routes, go to Router > Static > Static Route. To edit an existing static route entry, go to Router > Static > Static Route and select the Edit icon beside the entry that you want to edit.

Figure 145 shows the static route list belonging to a FortiGate unit that has interfaces named "external" and "internal". The names of the interfaces on your FortiGate unit may be different.

**Figure 145: Static Route list**

Create New Add a static route to the Static Route list. See "Adding a static route to the routing table" on page 238.

IP The destination IP addresses of packets that the FortiGate unit intercepts.

Mask The network masks associated with the IP addresses.

Gateway The IP addresses of the next-hop routers to which intercepted packets are forwarded.

Device The names of the FortiGate interfaces through which intercepted packets are received and sent.

Distance The administrative distances associated with each route. The values represent distances to next-hop routers.

Delete and Edit icons Delete or edit an entry in the list.
Default route and default gateway

In the factory default configuration, entry number 1 in the Static Route list is associated with a destination address of 0.0.0.0/0.0.0.0, which means any/all destinations. This route is called the “static default route”. If no other routes are present in the routing table and a packet needs to be forwarded beyond the FortiGate unit, the factory configured static default route causes the FortiGate unit to forward the packet to the default gateway.

To prevent this you must either edit the factory configured static default route to specify a different default gateway for the FortiGate unit, or delete the factory configured route and specify your own static default route that points to the default gateway for the FortiGate unit.

For example, consider Figure 146, which shows a FortiGate unit connected to a router. To ensure that all outbound packets destined to any network beyond the router are routed to the correct destination, you must edit the factory default configuration and make the router the default gateway for the FortiGate unit.

Figure 146: Making a router the default gateway

To route outbound packets from the internal network to destinations that are not on network 192.168.20.0/24, you would edit the default route and include the following settings:

- Destination IP/mask: 0.0.0.0/0.0.0.0
- Gateway: 192.168.10.1
• Device: Name of the interface connected to network 192.168.10.0/24 (for example, external).
• Distance: 10

The Gateway setting specifies the IP address of the next hop router interface to the FortiGate external interface. The interface behind the router (192.168.10.1) is the default gateway for FortiGate_1.

In some cases, there may be routers behind the FortiGate unit. If the destination IP address of a packet is not on the local network but is on a network behind one of those routers, the FortiGate routing table must include a static route to that network. For example, in Figure 147, the FortiGate unit must be configured with static routes to interfaces 192.168.10.1 and 192.168.11.1 in order to forward packets to Network_1 and Network_2 respectively.

**Figure 147: Destinations on networks behind internal routers**

To route packets from Network_1 to Network_2, Router_1 must be configured to use the FortiGate internal interface as its default gateway. On the FortiGate unit, you would create a new static route with these settings:

- Destination IP/mask: 192.168.30.0/24
- Gateway: 192.168.11.1
- Device: dmz
- Distance: 10

To route packets from Network_2 to Network_1, Router_2 must be configured to use the FortiGate dmz interface as its default gateway. On the FortiGate unit, you would create a new static route with these settings:

- Destination IP/mask: 192.168.20.0/24
- Gateway: 192.168.10.1
- Device: internal
- Distance: 10
Changing the gateway for the default route

The default gateway determines where packets matching the default route will be forwarded.

**To change the gateway for the default route**

1. Go to **Router > Static > Static Route**.
2. Select the Edit icon in row 1.
3. In the Gateway field, type the IP address of the next-hop router to which outbound traffic may be directed.
4. If the FortiGate unit reaches the next-hop router through a different interface (compared to the interface that is currently selected in the Device field), select the name of the interface from the Device field.
5. In the Distance field, optionally adjust the administrative distance value.
6. Select OK.

Adding a static route to the routing table

A route provides the FortiGate unit with the information it needs to forward a packet to a particular destination. A static route causes packets to be forwarded to a destination other than the default gateway.

You define static routes manually. Static routes control traffic exiting the FortiGate unit—you can specify through which interface the packet will leave and to which device the packet should be routed.

To add a static route entry, go to **Router > Static > Static Route** and select Create New.

When you add a static route through the web-based manager, the FortiGate unit assigns the next unassigned sequence number to the route automatically and adds the entry to the Static Route list.

Figure 148 shows the Edit Static Route dialog box belonging to a FortiGate unit that has an interface named “internal”. The names of the interfaces on your FortiGate unit may be different.

**Figure 148: Edit Static Route**

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>Gateway</th>
<th>Device</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.0/255.255.255.0</td>
<td>192.168 20.1</td>
<td>internal</td>
<td>10 (1-255)</td>
</tr>
</tbody>
</table>

**Destination** Type the destination IP address and network mask of packets that the FortiGate unit has to intercept. The value 0.0.0.0/0.0.0.0 is reserved for the default route.

**Gateway** Type the IP address of the next-hop router to which the FortiGate unit will forward intercepted packets.

**Device** Select the name of the FortiGate interface through which the intercepted packets may be routed to the next-hop router.

**Distance** Type an administrative distance for the route. The distance value is arbitrary and should reflect the distance to the next-hop router. A lower value indicates a more preferred route. The value can be an integer from 1 to 255.
Policy Route

Whenever a packet arrives at a FortiGate unit interface, the FortiGate unit determines whether the packet was received on a legitimate interface by doing a reverse lookup using the source IP address in the packet header. If the FortiGate unit cannot communicate with the computer at the source IP address through the interface on which the packet was received, the FortiGate unit drops the packet.

If the destination address can be matched to a local address (and the local configuration permits delivery), the FortiGate unit delivers the packet to the local network. If the packet is destined for another network, the FortiGate unit forwards the packet to a next-hop router according to a route policy and/or the information stored in the FortiGate forwarding table (see “Routing concepts” on page 231).

When routing policies exist and a packet arrives at the FortiGate unit, the FortiGate unit starts at the top of the Policy Route list and attempts to match the packet with a policy. If a match is found and the policy contains enough information to route the packet (the IP address of the next-hop router must be specified as well as the FortiGate interface for forwarding packets to the next-hop router), the FortiGate unit routes the packet using the information in the policy. If no route policy matches the packet, the FortiGate unit routes the packet using the routing table.

Note: Because most policy settings are optional, a matching policy alone might not provide enough information for the FortiGate unit to forward the packet. The FortiGate unit may refer to the routing table in an attempt to match the information in the packet header with a route in the routing table.

For example, if the outgoing interface is the only item given in the policy, the FortiGate unit looks up the IP address of the next-hop router in the routing table. This situation could happen when the FortiGate interfaces are dynamic (the interface receives an IP address through DHCP or PPPoE) and you do not want or are unable to specify the IP address of the next-hop router because the IP address changes dynamically.

To view the list of route policies, go to **Router > Static > Policy Route**. To edit an existing route policy, go to **Router > Static > Policy Route** and select the Edit icon beside the policy that you want to edit.

Figure 149 shows the policy route list belonging to a FortiGate unit that has interfaces named “external” and “internal”. The names of the interfaces on your FortiGate unit may be different.

**Figure 149: Policy Route list**

<table>
<thead>
<tr>
<th>#</th>
<th>Incoming</th>
<th>Outgoing</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>port2</td>
<td>port4</td>
<td>192.168.10.0 / 255.255.255.0</td>
<td>192.168.20.0 / 255.255.255.0</td>
</tr>
<tr>
<td>1</td>
<td>lan</td>
<td>lan</td>
<td>10.1.1.0 / 255.255.255.0</td>
<td>10.1.1.0 / 255.255.255.0</td>
</tr>
</tbody>
</table>

Create New  Add a route policy. See “Adding a route policy” on page 240.

#  The ID numbers of configured route policies. These numbers are sequential unless policies have been moved within the table.

Incoming  The interfaces on which packets subjected to route policies are received.

Outgoing  The interfaces through which policy routed packets are routed.
Source

The IP source addresses and network masks that cause policy routing to occur.

Destination

The IP destination addresses and network masks that cause policy routing to occur.

Delete icon

Select to delete a policy route.

Edit icon

Select to edit a policy route.

Move To icon

Select to move policy route up or down in the policy route table. Selecting this icon will bring up the Move Policy Route screen where you can specify the new location in the Policy Route table. See “Moving a route policy”.

Adding a route policy

Route policy options define which attributes of an incoming packet cause policy routing to occur. If the attributes of a packet match all the specified conditions, the FortiGate unit routes the packet through the specified interface to the specified gateway.

To add a route policy, go to Router > Static > Policy Route and select Create New.

Figure 150 shows the New Routing Policy dialog box belonging to a FortiGate unit that has interfaces named “external” and “internal”. The names of the interfaces on your FortiGate unit may be different.

Figure 150: New Routing Policy

<table>
<thead>
<tr>
<th>New Routing Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>If incoming traffic matches:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Force traffic to:</td>
</tr>
<tr>
<td>Gateway Address</td>
</tr>
</tbody>
</table>

Protocol

To perform policy routing based on the value in the protocol field of the packet, type the protocol number to match. The range is from 0 to 255. A value of 0 disables the feature.

Incoming Interface

Select the name of the interface through which incoming packets subjected to the policy are received.

Source Address / Mask

To perform policy routing based on the IP source address of the packet, type the source address and network mask to match. A value of 0.0.0.0/0.0.0.0 disables the feature.

Destination Address / Mask

To perform policy routing based on the IP destination address of the packet, type the destination address and network mask to match. A value of 0.0.0.0/0.0.0.0 disables the feature.

Destination Ports

To perform policy routing based on the port on which the packet is received, type the same port number in the From and To fields. If you want policy routing to apply to a range of ports, type the starting port number in the From field and the ending port number in the To field. Zero values disable this feature.
Moving a route policy

A routing policy is added to the bottom of the routing table when it is created. If you want one policy to be used in preference to another, you may want to move it to a different location in the routing policy table.

The option to use one of two routes happens when both routes are a match, say 172.20.0.0/255.255.0.0 and 172.20.120.0/255.255.255.0. If both of these routes are in the policy table, both can match a route to 172.20.120.112 but the second one is a better match. In that case the best match route should be positioned before the other route in the policy table.

Using the CLI, you can assign priorities to routes. In the case of two matches in the routing table, the priority will determine which route is used. This feature is only available through the CLI.

Figure 151: Move Policy Route

<table>
<thead>
<tr>
<th>Policy route ID</th>
<th>Move to</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

**Before / After**

Select before to place the selected Policy Route before the indicated route. Select After to place it following the indicated route.

**Policy route ID**
Enter the Policy route ID of the route in the Policy route table to move the selected route before or after.
Router Dynamic

This section explains how to configure dynamic protocols to route traffic through large or complex networks. Dynamic routing protocols enable the FortiGate unit to automatically share information about routes with neighboring routers and learn about routes and networks advertised by neighboring routers. The FortiGate unit supports these dynamic routing protocols:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)

**Note:** Basic RIP, OSPF, and BGP routing options can be configured through the web-based manager. Many additional options may be configured through CLI commands only. For complete descriptions and examples of how to use CLI commands to configure RIP, OSPF, and BGP settings, see the “router” chapter of *FortiGate CLI Reference*.

The FortiGate unit selects routes and updates its routing table dynamically based on the rules you specify. Given a set of rules, the FortiGate unit can determine the best route or path for sending packets to a destination. You can also define rules to suppress the advertising of routes to neighboring routers and/or change FortiGate routing information before it is advertised.

**Note:** A FortiGate unit can operate as a Protocol Independent Multicast (PIM) version 2 router in the root virtual domain. FortiGate units support PIM sparse mode and dense mode and can service multicast servers or receivers on the network segment to which a FortiGate interface is connected. PIM can use static routes, RIP, OSPF, or BGP to forward multicast packets to their destinations.

Bi-Directional Forwarding (BFD) is a protocol that works with BGP and OSPF to quickly discover routers on the network that can not be contacted, and re-route traffic accordingly until those routers can be contacted.

This section describes:

- RIP
- OSPF
- BGP
- Multicast
- Bi-directional Forwarding Detection (BFD)
RIP

RIP is a distance-vector routing protocol intended for small, relatively homogeneous, networks. The FortiGate implementation of RIP supports RIP version 1 (see RFC 1058) and RIP version 2 (see RFC 2453).

Note: Basic routing options can be configured through the web-based manager. Many additional options may be configured through CLI commands only. For complete descriptions and examples of how to use CLI commands to configure RIP settings, see the “router” chapter of the FortiGate CLI Reference.

How RIP works

When RIP is enabled, the FortiGate unit broadcasts requests for RIP updates from each of its RIP-enabled interfaces. Neighboring routers respond with information from their routing tables. The FortiGate unit adds routes from neighbors to its own routing table only if those routes are not already recorded in the routing table. When a route already exists in the routing table, the FortiGate unit compares the advertised route to the recorded route and chooses the shortest route for the routing table.

RIP uses hop count as the metric for choosing the best route. A hop count of 1 represents a network that is connected directly to the FortiGate unit, while a hop count of 16 represents a network that the FortiGate unit cannot reach. Each network that a packet travels through to reach its destination usually counts as one hop. When the FortiGate unit compares two routes to the same destination, the route having the lowest hop count is added to the routing table.

Similarly, when RIP is enabled on an interface, the FortiGate unit sends RIP responses to neighboring routers on a regular basis. The updates provide information about the routes in the FortiGate routing table, subject to the rules that you specify for advertising those routes. You can specify how often the FortiGate unit sends updates, how long a route can be kept in the FortiGate routing table without being updated, and for routes that are not updated regularly, how long the FortiGate unit advertises the route as unreachable before it is removed from the FortiGate routing table.

Viewing and editing basic RIP settings

When you configure RIP settings, you have to specify the networks that are running RIP and specify any additional settings needed to adjust RIP operation on the FortiGate interfaces that are connected to the RIP-enabled network.

To configure basic settings for a FortiGate unit connected to a RIP network, go to Router > Dynamic > RIP. To edit the operating parameters of a RIP-enabled interface, go to Router > Dynamic > RIP and select the Edit icon in the row that corresponds to the RIP-enabled interface.

Figure 152 shows the basic RIP settings on a FortiGate unit that has interfaces named “dmz” and “external”. The names of the interfaces on your FortiGate unit may be different.
Figure 152: Basic RIP settings

RIP Version

Select the level of RIP compatibility needed at the FortiGate unit. You can enable global RIP settings on all FortiGate interfaces connected to RIP-enabled networks:

- Select 1 to send and receive RIP version 1 packets.
- Select 2 to send and receive RIP version 2 packets.

You can override the global settings for a specific FortiGate interface if required (see “Overriding the RIP operating parameters on an interface” on page 247).

Advanced Options

Select advanced RIP options. See “Selecting advanced RIP options” on page 246.

Networks

The IP addresses and network masks of major networks (connected to the FortiGate unit) that run RIP. When you add a network to the Networks list, the FortiGate interfaces that are part of the network are advertised in RIP updates. You can enable RIP on all FortiGate interfaces whose IP addresses match the RIP network address space.

IP/Netmask

Enter the IP address and netmask that defines the RIP-enabled network.

Add

Select to add the network information to the Networks list.

Interfaces

Any additional settings needed to adjust RIP operation on a FortiGate interface.

Create New

Select to configure RIP operating parameters for an interface. These parameters will override the global RIP settings for that interface. See “Overriding the RIP operating parameters on an interface” on page 247.

Interface

Select the interface to configure RIP operating parameters for.

Send Version

Select the version of RIP used to send updates through each interface: 1, 2, or both.

Receive Version

Select the versions of RIP used to listen for updates on each interface: 1, 2, or both.

Authentication

Select the type of authentication used on this interface: None, Text or MD5.

Passive

Select to block RIP broadcasts on this interface.

Delete and Edit icons

Delete or edit a RIP network entry or a RIP interface definition.
Selecting advanced RIP options

Advanced RIP options let you specify settings for RIP timers and define metrics for redistributing routes that the FortiGate unit learns through some means other than RIP updates. For example, if the FortiGate unit is connected to an OSPF or BGP network or you add a static route to the FortiGate routing table manually, you can configure the FortiGate unit to advertise those routes on RIP-enabled interfaces.

To select advanced RIP options, go to Router > Dynamic > RIP and expand Advanced Options. After you select the options, select Apply.

Note: Additional advanced options can be configured through the CLI. For example, you can filter incoming or outgoing updates using a route map, an access list, or a prefix list. The FortiGate unit also supports offset lists, which add the specified offset to the metric of a route. For more information, see the “router” chapter of the FortiGate CLI Reference.

Figure 153: Advanced Options (RIP)

**Default Metric**

Enter the default hop count that the FortiGate unit should assign to routes that are added to the Fortinet routing table. The range is from 1 to 16. This value also applies to Redistribute unless otherwise specified.

**Enable Default-information-originate**

Select to generate and unconditionally advertise a default route into the FortiGate unit’s RIP-enabled networks. The generated route may be based on routes learned through a dynamic routing protocol, routes in the routing table or both.

**RIP Timers**

Override the default RIP timer settings. The default settings are effective in most configurations — if you change these settings, take care to ensure that the new settings are compatible with local routers and access servers.

- **Update**
  Enter the amount of time (in seconds) that the FortiGate unit will wait between sending RIP updates.

- **Timeout**
  Enter the maximum amount of time (in seconds) that a route is considered reachable while no updates are received for the route. This is the maximum time the FortiGate unit will keep a reachable route in the routing table while no updates for that route are received. If the FortiGate unit receives an update for the route before the timeout period expires, the timer is restarted. The Timeout period should be at least three times longer than the Update period.
Overriding the RIP operating parameters on an interface

RIP interface options enable you to override the global RIP settings that apply to all Fortinet interfaces connected to RIP-enabled networks. For example, if you want to suppress RIP advertising on an interface that is connected to a subnet of a RIP-enabled network, you can enable the interface to operate passively. Passive interfaces listen for RIP updates but do not respond to RIP requests.

If RIP version 2 is enabled on the interface, you can optionally choose password authentication to ensure that the FortiGate unit authenticates a neighboring router before accepting updates from that router. The FortiGate unit and the neighboring router must both be configured with the same password. Authentication guarantees the authenticity of the update packet, not the confidentiality of the routing information in the packet.

To set specific RIP operating parameters for a RIP-enabled interface, go to Router > Dynamic > RIP and select Create New.

**Note:** Additional options such as split-horizon and key-chain settings can be configured per interface through the CLI. For more information, see the “router” chapter of the FortiGate CLI Reference.

Figure 154 shows the New/Edit RIP Interface dialog box belonging to a FortiGate unit that has an interface named “internal”. The names of the interfaces on your FortiGate unit may be different.
OSPF

Open shortest path first (OSPF) is a link-state routing protocol that is most often used in large heterogeneous networks to share routing information among routers in the same Autonomous System (AS). FortiGate units support OSPF version 2 (see RFC 2328).

**Note:** Basic OSPF routing options can be configured through the web-based manager. Many additional options may be configured through CLI commands only. For complete descriptions and examples of how to use CLI commands to configure OSPF settings, see the "router" chapter of the *FortiGate CLI Reference*.

**OSPF autonomous systems**

An OSPF AS is typically divided into logical areas linked by area border routers. An area comprises a group of contiguous networks. An area border router links one or more areas to the OSPF network backbone (area ID 0). To specify the characteristics of an OSPF AS, see "Defining an OSPF AS" on page 249.

When the FortiGate unit has an interface to an OSPF area, it can participate in OSPF communications. The FortiGate unit uses the OSPF Hello protocol to acquire neighbors in an area. A neighbor is any router that has an interface to the same area as the FortiGate unit. After initial contact, the FortiGate unit exchanges Hello packets with its OSPF neighbors regularly to confirm that the neighbors can be reached.
OSPF-enabled routers generate link-state advertisements and send them to their neighbors whenever the status of a neighbor changes or a new neighbor comes online. As long as the OSPF network is stable, link-state advertisements between OSPF neighbors do not occur. A Link-State Advertisement (LSA) identifies the interfaces of all OSPF-enabled routers in an area, and provides information that enables OSPF-enabled routers to select the shortest path to a destination. All LSA exchanges between OSPF-enabled routers are authenticated.

The FortiGate unit maintains a database of link-state information based on the advertisements that it receives from OSPF-enabled routers. To calculate the best route (shortest path) to a destination, the FortiGate unit applies the Shortest Path First (SPF) algorithm to the accumulated link-state information. OSPF uses relative cost as a basic metric for choosing the best route. Cost imposes a penalty on the outgoing direction of a FortiGate interface. The cost of a route is calculated by adding together all of the costs associated with the outgoing interfaces along the path to a destination. The lowest overall cost indicates the best route.

The FortiGate unit updates its routing table dynamically based on the results of the SPF calculation to ensure that an OSPF packet will be routed using the shortest path to its destination. Depending on the network topology, the entries in the FortiGate routing table may include:

- the addresses of networks in the local OSPF area (to which packets are sent directly)
- routes to OSPF area border routers (to which packets destined for another area are sent)
- if the network contains OSPF areas and non-OSPF domains, routes to AS boundary routers, which reside on the OSPF network backbone and are configured to forward packets to destinations outside the OSPF AS

The number of routes that a FortiGate unit can learn through OSPF depends on the network topology. A single FortiGate unit can support tens of thousands of routes if the OSPF network is configured properly.

**Defining an OSPF AS**

Defining an OSPF AS, involves:

- Defining the characteristics of one or more OSPF areas.
- Creating associations between the OSPF areas that you defined and the local networks to include in the OSPF AS.
- If required, adjusting the settings of OSPF-enabled interfaces.

For more information about how to perform these tasks using the web-based manager, follow the procedure given below.

**To define an OSPF AS**

1. Go to **Router > Dynamic > OSPF**.
2. Under Areas, select Create New.
3. Define the characteristics of one or more OSPF areas. See “Defining OSPF areas” on page 253.
5. Create associations between the OSPF areas that you defined and the local networks to include in the OSPF AS. See “Specifying OSPF networks” on page 254.
6 If you need to adjust the default settings of an OSPF-enabled interface, select Create New under Interfaces.

7 Select the OSPF operating parameters for the interface. See “Selecting operating parameters for an OSPF interface” on page 255.

8 Repeat Steps 6 and 7 if required for additional OSPF-enabled interfaces.

9 Optionally select advanced OSPF options for the OSPF AS. See “Selecting advanced OSPF options” on page 252.

10 Select Apply.

**Viewing and editing basic OSPF settings**

When you configure OSPF settings, you have to define the AS in which OSPF is enabled and specify which of the FortiGate interfaces participate in the AS. As part of the AS definition, you specify the AS areas and specify which networks to include those areas. You may optionally adjust the settings associated with OSPF operation on the FortiGate interfaces.

To view and edit OSPF settings, go to **Router > Dynamic > OSPF**.

Figure 155 shows the basic OSPF settings on a FortiGate unit that has an interface named “port1”. The names of the interfaces on your FortiGate unit may be different.

**Figure 155: Basic OSPF settings**

<table>
<thead>
<tr>
<th>Router ID</th>
<th>10.0.0.1</th>
<th>Apply</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Options</strong></td>
<td>Default, Redistribution</td>
<td></td>
</tr>
<tr>
<td><strong>Areas</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Area</strong></td>
<td><strong>Type</strong></td>
<td><strong>Authentication</strong></td>
</tr>
<tr>
<td>6.0.0.0</td>
<td>Regular</td>
<td>Text</td>
</tr>
<tr>
<td>6.0.0.1</td>
<td>Regular</td>
<td>Text</td>
</tr>
<tr>
<td>6.0.0.2</td>
<td>Regular</td>
<td>MD5</td>
</tr>
<tr>
<td><strong>Networks</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td><strong>Area</strong></td>
<td></td>
</tr>
<tr>
<td>10.0.0.0</td>
<td>9.0.0.0</td>
<td></td>
</tr>
<tr>
<td>172.16.0.0/255.255.255.0</td>
<td>9.0.0.1</td>
<td></td>
</tr>
<tr>
<td>192.168.0.0/255.255.255.0</td>
<td>9.0.0.2</td>
<td></td>
</tr>
</tbody>
</table>

| **Interfaces** |
| **Name** | **Interface** | **IP** | **Authentication** |
| OSPF_evenida_on_port1 | port1 | 172.20.128.140 | Text |

**Router ID** Enter a unique router ID to identify the FortiGate unit to other OSPF routers. By convention, the router ID is the numerically highest IP address assigned to any of the FortiGate interfaces in the OSPF AS. Do not change the router ID while OSPF is running.

**Advanced Options** Select advanced OSPF settings. See “Selecting advanced OSPF options” on page 252.

**Areas** Information about the areas making up an OSPF AS. The header of an OSPF packet contains an area ID, which helps to identify the origination of a packet inside the AS.

**Create New** Select to define an OSPF area and add the new area to the Areas list. See “Defining OSPF areas” on page 253.
### Area
The unique 32-bit identifiers of areas in the AS, in dotted decimal notation. Area ID 0.0.0.0 references the backbone of the AS and cannot be changed or deleted.

### Type
The types of areas in the AS:
- If an area is a normal OSPF area, “Regular” is displayed.
- If an area is not so stubby, “NSSA” is displayed.
- If an area is a stub, “Stub” is displayed.

For more information, see "Defining OSPF areas" on page 253.

### Authentication
The methods for authenticating OSPF packets sent and received through all FortiGate interfaces linked to each area:
- When authentication is disabled, “None” is displayed.
- When text-based password authentication is enabled, “Text” is displayed.
- When MD5 authentication is enabled, “MD5” is displayed.

A different authentication setting may apply to some of the interfaces in an area, as displayed under Interfaces. For example, if an area employs simple passwords for authentication, you can configure a different password for one or more of the networks in that area.

### Networks
The networks in the OSPF AS and their area IDs. When you add a network to the Networks list, all FortiGate interfaces that are part of the network are advertised in OSPF link-state advertisements. You can enable OSPF on all FortiGate interfaces whose IP addresses match the OSPF network address space.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Select to add a network to the AS, specify its area ID, and add the definition to the Networks list. See “Specifying OSPF networks” on page 254.</td>
</tr>
<tr>
<td>Network</td>
<td>The IP addresses and network masks of networks in the AS on which OSPF runs. The FortiGate unit may have physical or VLAN interfaces connected to the network.</td>
</tr>
<tr>
<td>Area</td>
<td>The area IDs that have been assigned to the OSPF network address space.</td>
</tr>
</tbody>
</table>

### Interfaces
Any additional settings needed to adjust OSPF operation on a FortiGate interface.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Select to add additional/different OSPF operating parameters for a FortiGate interface and add the configuration to the Interfaces list. See “Selecting operating parameters for an OSPF interface” on page 255.</td>
</tr>
<tr>
<td>Name</td>
<td>The names of OSPF interface definitions.</td>
</tr>
<tr>
<td>Interface</td>
<td>The names of FortiGate physical or VLAN interfaces having OSPF settings that differ from the default values assigned to all other interfaces in the same area.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP addresses of the OSPF-enabled interfaces having additional/different settings.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The methods for authenticating LSA exchanges sent and received on specific OSPF-enabled interfaces. These settings override the area Authentication settings.</td>
</tr>
</tbody>
</table>

Delete and Edit icons
Select to delete or edit an OSPF area entry, network entry, or interface definition.
Selecting advanced OSPF options

Advanced OSPF options let you specify metrics for redistributing routes that the FortiGate unit learns through some means other than OSPF link-state advertisements. For example, if the FortiGate unit is connected to a RIP or BGP network or you add a static route to the FortiGate routing table manually, you can configure the FortiGate unit to advertise those routes on OSPF-enabled interfaces.

To select advanced RIP options, go to Router > Dynamic > RIP and expand Advanced Options. After you select the options, select Apply.

Figure 156: Advanced Options (OSPF)

**Default Information**

- **None**: Disable the generation of a default route.
- **Regular**: Generate a default route into the OSPF AS and advertise the route to neighboring autonomous systems only if the route is stored in the FortiGate routing table.
- **Always**: Generate a default route into the OSPF AS and advertise the route to neighboring autonomous systems unconditionally, even if the route is not stored in the FortiGate routing table.

**Redistribute**

- **Connected**: Select to redistribute routes learned from directly connected networks.
  - If you want to specify a cost for those routes, enter the cost in the Metric field. The range is from 1 to 16,777,214.
- **Static**: Select to redistribute routes learned from static routes.
  - If you want to specify a cost for those routes, enter the cost in the Metric field. The range is from 1 to 16,777,214.
- **RIP**: Select to redistribute routes learned through RIP.
  - If you want to specify a cost for those routes, enter the cost in the Metric field. The range is from 1 to 16,777,214.
- **BGP**: Select to redistribute routes learned through BGP.
  - If you want to specify a cost for those routes, enter the cost in the Metric field. The range is from 1 to 16,777,214.

**Note:** Many additional advanced OSPF options can be configured through the CLI. For details, see the “router” chapter of the FortiGate CLI Reference.
Defining OSPF areas

An area logically defines part of the OSPF AS. Each area is identified by a 32-bit area ID expressed in decimal dot notation. Area ID 0.0.0.0 is reserved for the OSPF network backbone. You can classify the remaining areas of an AS in one of three ways:

- Regular
- Stub
- NSSA

A regular area contains more than one router, each having at least one OSPF-enabled interface to the area.

To reach the OSPF backbone, the routers in a stub area must send packets to an area border router. Routes leading to non-OSPF domains are not advertised to the routers in stub areas. The area border router advertises to the OSPF AS a single default route (destination 0.0.0.0) into the stub area, which ensures that any OSPF packet that cannot be matched to a specific route will match the default route. Any router connected to a stub area is considered part of the stub area.

In a Not-So-Stubby Area (NSSA), routes that lead out of the area into a non-OSPF domain are made known to OSPF AS. However, the area itself continues to be treated like a stub area by the rest of the AS.

Regular areas and stub areas (including not-so-stubby areas) are connected to the OSPF backbone through area border routers.

To define an OSPF area, go to Router > Dynamic > OSPF, and then under Areas, select Create New. To edit the attributes of an OSPF area, go to Router > Dynamic > OSPF and select the Edit icon in the row that corresponds to the area.

Note: If required, you can define a virtual link to an area that has lost its physical connection to the OSPF backbone. Virtual links can only be set up between two FortiGate units that act as area border routers. For more information, see “config virtual-link” under the OSPF “config area” subcommand in the FortiGate CLI Reference.

Figure 157: New/Edit OSPF Area

<table>
<thead>
<tr>
<th>Area</th>
<th>Type</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Regular</td>
<td>None</td>
</tr>
</tbody>
</table>

Area

Type a 32-bit identifier for the area. The value must resemble an IP address in decimal-dot notation. Once the OSPF area has been created, the area IP value cannot be changed.
OSPF Router Dynamic

Specifying OSPF networks

OSPF areas group a number of contiguous networks together. When you assign an area ID to a network address space, the attributes of the area are associated with the network.

To assign an OSPF area ID to a network, go to Router > Dynamic > OSPF, and then under Networks, select Create New. To change the OSPF area ID assigned to a network, go to Router > Dynamic > OSPF and select the Edit icon in the row that corresponds to the network.

Figure 158: New/Edit OSPF Network

<table>
<thead>
<tr>
<th>New/Edit OSPF Network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP/Netmask</strong></td>
</tr>
<tr>
<td><strong>Area</strong></td>
</tr>
</tbody>
</table>

IP/Netmask: Enter the IP address and network mask of the local network that you want to assign to an OSPF area.

Area: Select an area ID for the network. The attributes of the area must match the characteristics and topology of the specified network. You must define the area before you can select the area ID. See “Defining OSPF areas” on page 253.
Selecting operating parameters for an OSPF interface

An OSPF interface definition contains specific operating parameters for a FortiGate OSPF-enabled interface. The definition includes the name of the interface (for example, external or VLAN_1), the IP address assigned to the interface, the method for authenticating LSA exchanges through the interface, and timer settings for sending and receiving OSPF Hello and dead-interval packets.

You can enable OSPF on all FortiGate interfaces whose IP addresses match the OSPF-enabled network space. For example, define an area of 0.0.0.0 and the OSPF network is defined as 10.0.0.0/16. Then define vlan1 as 10.0.1.1/24, vlan2 as 10.0.2.1/24 and vlan3 as 10.0.3.1/24. All three VLANs will run OSPF in area 0.0.0.0. To enable all interfaces, you would create OSPF network 0.0.0.0/0 having an area that matches a specific IP address.

You can configure different OSPF parameters for the same FortiGate interface when more than one IP address has been assigned to the interface. For example, the same FortiGate interface could be connected to two neighbors through different subnets. You could configure an OSPF interface definition containing one set of Hello and dead-interval parameters for compatibility with one neighbor’s settings, and a second OSPF interface definition for the same interface to ensure compatibility with the second neighbor’s settings.

To select OSPF operating parameters for a FortiGate interface, go to Router > Dynamic > OSPF, and then under Interfaces, select Create New. To edit the operating parameters of an OSPF-enabled interface, go to Router > Dynamic > OSPF and select the Edit icon in the row that corresponds to the OSPF-enabled interface.

Figure 159 shows the New/Edit OSPF Interface dialog box belonging to a FortiGate unit that has an interface named “port1”. The interface names on your FortiGate unit may differ.

Figure 159: New/Edit OSPF Interface

| Name | Enter a name to identify the OSPF interface definition. For example, the name could indicate to which OSPF area the interface will be linked. |
| Interface | Select the name of the FortiGate interface to associate with this OSPF interface definition (for example, port1, external, or VLAN_1). The FortiGate unit can have physical, VLAN, virtual IPSec or GRE interfaces connected to the OSPF-enabled network. |
**BGP**

Border Gateway Protocol (BGP) is an Internet routing protocol typically used by ISPs to exchange routing information between different ISP networks. For example, BGP enables the sharing of network paths between the ISP network and an autonomous system (AS) that uses RIP and/or OSPF to route packets within the AS. The FortiGate implementation of BGP supports BGP-4 and complies with RFC 1771.

**How BGP works**

When BGP is enabled, the FortiGate unit sends routing table updates to neighboring autonomous systems whenever any part of the FortiGate routing table changes. Each AS, including the local AS of which the FortiGate unit is a member, is associated with an AS number. The AS number references a particular destination network.

**IP**

Enter the IP address that has been assigned to the OSPF-enabled interface. The interface becomes OSPF-enabled because its IP address matches the OSPF network address space.

For example, if you defined an OSPF network of 172.20.120.0/24 and port1 has been assigned the IP address 172.20.120.140, type 172.20.120.140.

**Authentication**

Select an authentication method for LSA exchanges on the specified interface:

- Select None to disable authentication.
- Select Text to authenticate LSA exchanges using a plain-text password. The password can be up to 35 characters, and is sent in clear text over the network.
- Select MD5 to use one or more keys to generate an MD5 hash.

This setting overrides the area Authentication setting.

**Password**

Enter the plain-text password. Enter an alphanumeric value of up to 15 characters. The OSPF neighbors that send link-state advertisements to this FortiGate interface must be configured with an identical password.

This field is available only if you selected plain-text authentication.

**MD5 Keys**

Enter the key identifier for the (first) password in the ID field (the range is from 1 to 255) and then type the associated password in the Key field. The password is an alphanumeric string of up to 16 characters. The OSPF neighbors that send link-state advertisements to this FortiGate interface must be configured with an identical MD5 key. If the OSPF neighbor uses more than one password to generate MD5 hash, select the Add icon to add additional MD5 keys to the list. This field is available only if you selected MD5 authentication.

**Hello Interval**

Optionally, set the Hello Interval to be compatible with Hello Interval settings on all OSPF neighbors.

This setting defines the period of time (in seconds) that the FortiGate unit waits between sending Hello packets through the interface.

**Dead Interval**

Optionally, set the Dead interval to be compatible with Dead Interval settings on all OSPF neighbors.

This setting defines the period of time (in seconds) that the FortiGate unit waits to receive a Hello packet from an OSPF neighbor through the interface. If the FortiGate unit does not receive a Hello packet within the specified amount of time, the FortiGate unit declares the neighbor inaccessible.

By convention, the Dead Interval value is usually four times greater than the Hello Interval value.
BGP updates advertise the best path to a destination network. When the FortiGate unit receives a BGP update, the FortiGate unit examines the Multi-Exit Discriminator (MED) attributes of potential routes to determine the best path to a destination network before recording the path in the FortiGate routing table.

BGP has the capability to gracefully restart. This capability limits the effects of software problems by allowing forwarding to continue when the control plane of the router fails. It also reduces routing flaps by stabilizing the network.

**Note:** Graceful restarting and other advanced settings cannot be configured through the web-based manager, only through CLI commands. For complete descriptions and examples of how to use CLI commands to configure BGP settings, see the “router” chapter of the FortiGate CLI Reference.

### Viewing and editing BGP settings

When you configure BGP settings, specify the AS that includes the FortiGate unit as a member and enter a router ID to identify the FortiGate unit to other BGP routers. You must also identify the FortiGate unit’s BGP neighbors and specify which of the networks local to the FortiGate unit should be advertised to BGP neighbors.

To view and edit BGP settings, go to **Router > Dynamic > BGP**. The web-based manager offers a simplified user interface to configure basic BGP options. A large number of advanced BGP options can be configured through the CLI. For more information, see the “router” chapter of the FortiGate CLI Reference.

### Figure 160: Basic BGP options

| Local AS | Enter the number of the local AS that the FortiGate unit is a member of. |
| Router ID | Enter a unique router ID to identify the FortiGate unit to other BGP routers. The router ID is an IP address written in dotted-decimal format. If you change the router ID while BGP is running, all connections to BGP peers will be broken temporarily until they are re-established. |
| Neighbors | The IP addresses and AS numbers of BGP peers in neighboring autonomous systems. |
| IP | Enter the IP address of the neighbor interface to the BGP-enabled network. |
| Remote AS | Enter the number of the AS that the neighbor belongs to. |
| Add/Edit | Select to add the neighbor information to the Neighbors list, or edit an entry in the list. |
| Neighbor | The IP addresses of BGP peers. |
| Remote AS | The numbers of the autonomous systems associated with the BGP peers. |
Multicast

A FortiGate unit can operate as a Protocol Independent Multicast (PIM) version 2 router in the root virtual domain. FortiGate units support PIM sparse mode (RFC 2362) and PIM dense mode (RFC 3973) and can service multicast servers or receivers on the network segment to which a FortiGate interface is connected.

Multicast server applications use a (Class D) multicast address to send one copy of a packet to a group of receivers. The PIM routers throughout the network ensure that only one copy of the packet is forwarded through the network until it reaches an end-point destination. At the end-point destination, copies of the packet are made only when required to deliver the information to multicast client applications that request traffic destined for the multicast address.

Note: To support PIM communications, the sending/receiving applications and all connecting PIM routers in between must be enabled with PIM version 2. PIM can use static routes, RIP, OSPF, or BGP to forward multicast packets to their destinations. To enable source-to-destination packet delivery, either sparse mode or dense mode must be enabled on all the PIM-router interfaces. Sparse mode routers cannot send multicast messages to dense mode routers. In addition, if a FortiGate unit is located between a source and a PIM router, two PIM routers, or is connected directly to a receiver, you must create a firewall policy manually to pass encapsulated (multicast) packets or decapsulated data (IP traffic) between the source and destination.

A PIM domain is a logical area comprising a number of contiguous networks. The domain contains at least one Boot Strap Router (BSR). If sparse mode is enabled, the domain also contains a number of Rendezvous Points (RPs) and Designated Routers (DRs). When PIM is enabled on a FortiGate unit, the FortiGate unit can perform any of these functions at any time as configured. If required for sparse mode operation, you can define static RPs.

Note: Basic options can be configured through the web-based manager. Many additional options may be configured through CLI commands only. For complete descriptions and examples of how to use CLI commands to configure PIM settings, see “multicast” in the “router” chapter of the FortiGate CLI Reference.

Viewing and editing multicast settings

When multicast (PIM) routing is enabled, you can configure sparse mode or dense mode operation on any FortiGate interface.
To view and edit PIM settings, go to Router > Dynamic > Multicast. The web-based manager offers a simplified user interface to configure basic PIM options. Advanced PIM options can be configured through the CLI. For more information, see the "router" chapter of the FortiGate CLI Reference.

**Figure 161: Basic Multicast options**

![Multicast options interface](image)

**Enable Multicast Routing** Select to enable PIM version 2 routing. A firewall policy must be created on PIM-enabled interfaces to pass encapsulated packets and decapsulated data between the source and destination.

**Add Static RP** If required for sparse mode operation, enter the IP address of a Rendezvous Point (RP) that may be used as the root of a packet distribution tree for a multicast group. Join messages from the multicast group are sent to the RP, and data from the source is sent to the RP.

If an RP for the specified IP's multicast group is already known to the Boot Strap Router (BSR), the RP known to the BSR is used and the static RP address that you specify is ignored.

**Apply** Select to save the specified static RP addresses.

**Create New** Select to create a new multicast entry for an interface. This will allow you to fine-tune PIM operation on a specific FortiGate interface or override the global PIM settings on a particular interface. See "Overriding the multicast settings on an interface" on page 260.

**Interface** The names of FortiGate interfaces having specific PIM settings.

**Mode** The mode of PIM operation (Sparse or Dense) on that interface.

**Status** The status of parse-mode RP candidacy on the interface.

To enable or disable RP candidacy on an interface, select the Edit icon in the row that corresponds to the interface.

**Priority** The priority number assigned to RP candidacy on that interface. Only available when RP candidacy is enabled.

**DR Priority** The priority number assigned to Designated Router (DR) candidacy on the interface. Only available when sparse mode is enabled.

**Delete and Edit icons** Select to delete or edit the PIM settings on the interface.
Overriding the multicast settings on an interface

Multicast (PIM) interface options enable you to set operating parameters for FortiGate interfaces connected to PIM domains. For example, you can enable dense mode on an interface that is connected to a PIM-enabled network segment. When sparse mode is enabled, you can adjust the priority number that is used to advertise Rendezvous Point (RP) and/or Designated Router (DR) candidacy on the interface.

Figure 162: Multicast interface settings

![Multicast interface settings](image)

Interface | Select the name of the root VDOM FortiGate interface to which these settings apply. The interface must be connected to a PIM version 2 enabled network segment.
---
PIM Mode | Select the mode of operation: Sparse Mode or Dense Mode. All PIM routers connected to the same network segment must be running the same mode of operation. If you select Sparse Mode, adjust the remaining options as described below.
---
DR Priority | Enter the priority number for advertising DR candidacy on the FortiGate interface. The range is from 1 to 4,294,967,295. This value is compared to the DR interfaces of all other PIM routers on the same network segment, and the router having the highest DR priority is selected to be the DR.
---
RP Candidate | Select to enable or disable RP candidacy on the interface.
---
RP Candidate Priority | Enter the priority number for advertising RP candidacy on the FortiGate interface. The range is from 1 to 255.

Multicast destination NAT

Multicast destination NAT (DNAT) allows you translate externally received multicast destination addresses to addresses that conform to an organization's internal addressing policy.

Using this feature, users do not need to redistribute routes at the translation boundary into their network infrastructure for Reverse Path Forwarding (RPF) to work properly, and users can receive identical feeds from two ingress points in the network and route them independently.

Multicast DNAT is configured in the CLI using the following command:

```
config firewall multicast-policy
edit pl
    set dnat <dnatted-multicast-group>
    set ...
next
end
```

For more information, see the “firewall” chapter of the FortiGate CLI Reference.
Bi-directional Forwarding Detection (BFD)

Bi-directional Forwarding Detection (BFD) protocol is designed to deal with dynamic routing protocols’ problem of not having a fine granularity for detecting device failures on the network and re-routing around those failures. BFD can detect these failures on a millisecond timer, where the routing protocols can only detect them on a second timer taking much longer to react to failures.

Your FortiGate unit supports BFD as part of OSPF and BGP dynamic networking. It is only configurable from the CLI.

How it works

When you enable BFD on your FortiGate unit, BFD starts trying to connect to other routers on the network. You can limit where BFD looks for routers by only enabling one interface, and enabling BFD for specific neighboring routers on the network.

Once the connection has been made, BFD will continue to send periodic packets to the router to make sure it is still operational. These small packets are sent frequently.

If BFD never connects to the router on the network, it can’t report on that router being up or down. In this situation, BFD will continue to try and connect to the router. Until that connection is made, the device may go down and up without notice.

If there is no response from the neighboring router within the set period of time, BFD on your FortiGate unit declares that router down and changes routing accordingly. BFD continues to try and reestablish a connection.

Once that connection is reestablished, routes are reset to include the router once again.

Configuring BFD

BFD is intended for networks that use BGP or OSPF routing protocols. This generally excludes smaller networks.

You can enable BFD for your FortiGate unit, and turn it off for one or two interfaces. Alternatively you can specifically enable BFD for each neighbor router, or interface. Which method you choose will be determined by the amount of configuring for your network.

The size of your timeout period is very important. There is no easy number, as it varies for each network and FortiGate unit. High end FortiGate models will respond very quickly unless loaded down with traffic. Also the size of the network will slow down the response time - packets need to make more hops than on a smaller network. Those two factors (CPU load and network traversal time) affect how long the timeout you select should be. With too short a timeout period, BFD will not connect to the network device but it will keep trying. This state generates unnecessary network traffic, and leaves the device unmonitored. If this happens to you, try setting a longer timeout period to allow BFD more time to discover the device on the network.
Configuring BFD on your FortiGate unit

For this example BFD is enabled on the FortiGate unit using the default values. This means that once a connection is established, your FortiGate unit will wait for up to 150 milliseconds (50 x 3) for a reply from a BFD router before declaring that router down and rerouting traffic. The port that BFD traffic originates from will be checked for security purposed.

```
config system settings
    set bfd enable
    set bfd-desired-min-tx 50
    set bfd-required-min-rx 50
    set bfd-detect-mult 3
    set bfd-dont-enforce-src-port disable
end
```

Note: The minimum receive interval (bfd-required-min-rx) and the detection multiplier (bfd-detect-mult) combine to determine how long a period your FortiGate unit will wait for a reply before declaring the neighbor down. The correct value for your situation will vary based on the size of your network and the speed of your FortiGate unit’s CPU. The number used in this example may not work for your network.

Configure BFD off on a specific interface

The above example configured BFD to be on for your FortiGate unit. If there is an interface that is not connected to any BFD enabled routers, you can reduce network traffic by turning BFD off just for that interface. For this example, BFD is turned off for the internal interface using CLI commands. It could just as easily have been turned on (enable) or set to use the FortiGate unit’s default settings (global).

```
config system interface
    edit internal
        set bfd disable
end
```

Configuring BFD on BGP

Configuring BFD on a BGP network is very straight forward - turn it on. In BGP, you enable BFD for each neighbor that is running the protocol. This allows a two-way communication to be established.

Configuring BFD on OSPF

Configuring BFD on an OSPF network is very much like enabling BFD on your FortiGate unit - you can enable it globally, and you can override the global settings at the interface level.
Router Monitor

This section explains how to interpret the Routing Monitor list. The list displays the entries in the FortiGate routing table.

This section describes:

- Displaying routing information
- Searching the FortiGate routing table

Displaying routing information

By default, all routes are displayed in the Routing Monitor list. The default static route is defined as 0.0.0.0/0, which matches the destination IP address of “any/all” packets.

To display the routes in the routing table, go to **Router > Monitor**.

**Figure 163** shows the Routing Monitor list belonging to a FortiGate unit that has interfaces named “port1”, “port4”, and “lan”. The names of the interfaces on your FortiGate unit may be different.

**Figure 163:** Routing Monitor list

<table>
<thead>
<tr>
<th>Type</th>
<th>Subtype</th>
<th>Network</th>
<th>Distance</th>
<th>Metric</th>
<th>Gateway</th>
<th>Interface</th>
<th>Up Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>0.0.0.0/0</td>
<td>10 6</td>
<td>172.16.7.1</td>
<td>vlan_483</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>4.4.4.4/32</td>
<td>110 11</td>
<td>136.1.1.4</td>
<td>lan</td>
<td>00:37:37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>5.5.5.5/32</td>
<td>110 11</td>
<td>136.1.1.5</td>
<td>lan</td>
<td>00:37:37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIPv2</td>
<td>12.0.0.0/8</td>
<td>120 2</td>
<td>26.1.0.12</td>
<td>vlan_550</td>
<td>00:39:16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPF NESA 1</td>
<td>12.1.1.0/24</td>
<td>110 30</td>
<td>136.1.1.1</td>
<td>vlan_402</td>
<td>00:37:10</td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPF NESA 2</td>
<td>12.1.1.0/24</td>
<td>130 999</td>
<td>136.1.1.1</td>
<td>vlan_402</td>
<td>00:37:10</td>
<td></td>
</tr>
<tr>
<td>RIPv2</td>
<td>12.1.3.0/24</td>
<td>120 2</td>
<td>26.1.0.12</td>
<td>vlan_550</td>
<td>00:39:31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIPv2</td>
<td>12.1.3.0/24</td>
<td>120 2</td>
<td>26.1.0.12</td>
<td>vlan_550</td>
<td>00:39:31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td>19.1.1.0/24</td>
<td>0 6</td>
<td>0.0.0.0</td>
<td>vlan_402</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td>19.1.1.0/24</td>
<td>0 6</td>
<td>0.0.0.0</td>
<td>port1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td>19.1.1.0/24</td>
<td>0 6</td>
<td>0.0.0.0</td>
<td>lan</td>
<td>00:33:34</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td>19.1.1.0/24</td>
<td>0 6</td>
<td>0.0.0.0</td>
<td>lan</td>
<td>00:33:34</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BGP</td>
<td>160.1.1.0/24</td>
<td>200 6</td>
<td>136.1.1.5</td>
<td>lan</td>
<td>00:49:34</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BGP</td>
<td>160.1.1.0/24</td>
<td>200 6</td>
<td>136.1.1.5</td>
<td>lan</td>
<td>00:49:34</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPF inter</td>
<td>160.1.1.0/24</td>
<td>110 11</td>
<td>136.1.1.5</td>
<td>lan</td>
<td>00:35:13</td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPF External 1</td>
<td>160.1.1.0/24</td>
<td>110 10</td>
<td>136.1.1.5</td>
<td>lan</td>
<td>00:26:56</td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPF External 1</td>
<td>160.1.1.0/24</td>
<td>110 10</td>
<td>136.1.1.5</td>
<td>lan</td>
<td>00:26:56</td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPF External 2</td>
<td>160.1.1.0/24</td>
<td>110 13</td>
<td>136.1.1.5</td>
<td>lan</td>
<td>00:26:55</td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td>172.16.7.0/24</td>
<td>0 6</td>
<td>0.0.0.0</td>
<td>vlan_483</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td>192.168.1.0/24</td>
<td>0 6</td>
<td>0.0.0.0</td>
<td>port1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Displaying routing information

Router Monitor

Type
Select one of these route types to search the routing table and display routes of the selected type only:

- All displays all routes recorded in the routing table.
- Connected displays all routes associated with direct connections to FortiGate interfaces.
- Static displays the static routes that have been added to the routing table manually.
- RIP displays all routes learned through RIP.
- OSPF displays all routes learned through OSPF.
- BGP displays all routes learned through BGP.
- HA displays RIP, OSPF, and BGP routes synchronized between the primary unit and the subordinate units of a high availability (HA) cluster. HA routes are maintained on subordinate units and are only visible if you are viewing the router monitor from a virtual domain that is configured as a subordinate virtual domain in a virtual cluster. For details about HA routing synchronization, see the FortiGate High Availability User Guide.

Network
Enter an IP address and netmask (for example, 172.16.14.0/24) to search the routing table and display routes that match the specified network.

Gateway
Enter an IP address and netmask (for example, 192.168.12.1/32) to search the routing table and display routes that match the specified gateway.

Apply Filter
Select to search the entries in the routing table based on the specified search criteria and display any matching routes.

Type
The type values assigned to FortiGate routes (Static, Connected, RIP, OSPF, or BGP).

Subtype
If applicable, the subtype classification assigned to OSPF routes.

- An empty string implies an intra-area route. The destination is in an area to which the FortiGate unit is connected.
- OSPF inter area means the destination is in the OSPF AS, but the FortiGate unit is not connected to that area.
- External 1 means the destination is outside the OSPF AS. The metric of a redistributed route is calculated by adding the external cost and the OSPF cost together.
- External 2 means the destination is outside the OSPF AS. In this case, the metric of the redistributed route is equivalent to the external cost only, expressed as an OSPF cost.
- OSPF NSSA 1 has the same meaning as External 1, but the route was received through a not-so-stubby area.
- OSPF NSSA 2 has the same meaning as External 2, but the route was received through a not-so-stubby area.

Network
The IP addresses and network masks of destination networks that the FortiGate unit can reach.

Distance
The administrative distance associated with the route. A value of 0 means the route is preferable compared to routes to the same destination.

To modify the administrative distance assigned to static routes, see “Adding a static route to the routing table” on page 238. Refer to the FortiGate CLI Reference for dynamic routes.
Searching the FortiGate routing table

You can apply a filter to search the routing table and display certain routes only. For example, you can display static routes, connected routes, routes learned through RIP, OSPF, or BGP, and/or routes associated with the network or gateway that you specify.

If you want to search the routing table by route type and further limit the display according to network or gateway, all of the values that you specify as search criteria must match corresponding values in the same routing table entry in order for that entry to be displayed (an implicit AND condition is applied to all of the search parameters you specify).

For example, if the FortiGate unit is connected to network 172.16.14.0/24 and you want to display all directly connected routes to network 172.16.14.0/24, you must select Connected from the Type list, type 172.16.14.0/24 in the Network field, and then select Apply Filter to display the associated routing table entry or entries. Any entry that contains the word "Connected" in its Type field and the specified value in the Gateway field will be displayed.

To search the FortiGate routing table

1. Go to Router > Monitor > Routing Monitor.
2. From the Type list, select the type of route to display. For example, select Connected to display all connected routes, or select RIP to display all routes learned through RIP.
3. If you want to display routes to a specific network, type the IP address and netmask of the network in the Networks field.
4. If you want to display routes to a specific gateway, type the IP address of the gateway in the Gateway field.
5. Select Apply Filter.

Note: All of the values that you specify as search criteria must match corresponding values in the same routing table entry in order for that entry to be displayed.
Firewall Policy

Firewall policies control all traffic passing through the FortiGate unit. Add firewall policies to control connections and traffic between FortiGate interfaces, zones, and VLAN subinterfaces.

This section describes:

- About firewall policies
- Viewing the firewall policy list
- Configuring firewall policies
- Firewall policy examples

About firewall policies

Firewall policies are instructions the FortiGate unit uses to decide what to do with a connection request. When the firewall receives a connection request in the form of a packet, it analyzes the packet to extract its source address, destination address, and service (by port number).

For the packet to be connected through the FortiGate unit, the source address, destination address, and service of the packet must match a firewall policy. The policy directs the firewall action on the packet. The action can be to allow the connection, deny the connection, require authentication before the connection is allowed, or process the packet as an IPSec VPN packet.

Each policy can be configured to route connections or apply network address translation (NAT) to translate source and destination IP addresses and ports. Add IP pools to use dynamic NAT when the firewall translates source addresses. Use policies to configure port address translation (PAT) through the FortiGate unit.

Add protection profiles to firewall policies to apply different protection settings for the traffic that is controlled by firewall policies. For details about protection profiles, see “Firewall Protection Profile” on page 329.

Enable traffic logging for a firewall policy so the FortiGate unit logs all connections that use this policy.

The firewall matches policies by searching for a match starting at the top of the policy list and moving down until it finds the first match. Arrange policies in the policy list from more specific to more general. For example, the default policy is a very general policy because it matches all connection attempts. Exceptions to that policy are added to the policy list above the default policy. No policy below the default policy will ever be matched.

Policy options are configurable when creating or editing a firewall policy. Depending on the type of action selected, a different set of options is presented.
Multicast policies

The FortiGate unit supports multicast policies. You can configure and create multicast policies using the following CLI command:

```
config firewall multicast-policy
```

For details, see the FortiGate CLI Reference.

How policy matching works

When the FortiGate unit receives a connection attempt at an interface, it selects a policy list to search through for a policy that matches the connection attempt. The FortiGate unit chooses the policy list based on the source and destination addresses of the connection attempt.

The FortiGate unit then starts at the top of the selected policy list and searches down the list for the first policy that matches the connection attempt source and destination addresses, service port, and time and date at which the connection attempt was received. The first policy that matches is applied to the connection attempt. If no policy matches, the connection is dropped. As a general rule, always order firewall policies from most specific to most general.

General policies are policies that can accept connections from multiple source and destination addresses or from address ranges. General policies can also accept connections from multiple service ports or have schedules that mean the policy can be matched over a wide range of times and dates. If you want to add policies that are exceptions to general policies, then these specific exception policies should be added to the policy list above the general policies.

For example, you may have a general policy that allows all users on your internal network to access all services on the Internet. If you want to block access to FTP servers on the Internet, you should add a policy that denies FTP connections above the general policy. The deny policy blocks FTP connections, but connection attempts for all other kinds of services do not match the FTP policy but do match the general policy. Therefore, the firewall still accepts all connections from the internal network to the Internet other than FTP connections.

Also note the following about policy matching:

- Policies that require authentication must be added to the policy list above matching policies that do not; otherwise, the policy that does not require authentication is selected first.
- IPSec VPN tunnel mode policies must be added to the policy list above matching accept or deny policies
- SSL VPN policies must be added to the policy list above matching accept or deny policies

Viewing the firewall policy list

If virtual domains are enabled on the FortiGate unit, firewall policies are configured separately for each virtual domain. To access policies, select a virtual domain from the main menu.

You can add, delete, edit, and re-order policies in the policy list.

To view the policy list, go to Firewall > Policy.
Figure 164: Sample policy list

The policy list displays the following information. Note that some of the columns are not displayed by default. Use Column Settings to add or remove table columns.

Create New
Select to add a firewall policy. See “Adding a firewall policy” on page 270. Select the down arrow beside Create New to choose to either add a firewall policy or firewall policy section. A firewall policy section is a way of grouping firewall policies.

Column Settings
Select to customize the table view. You can select the columns to show and specify the column displaying order in the table.
By default, the Status, From, To, VPN Tunnel, Authentication, Comments, Label, Count, Log and Index columns are not displayed.

Filter icon
Select to edit the column filters, which allow you to filter or sort the policy list according to the criteria you specify. For details, see “Adding filters to web-based manager lists” on page 43.

ID
The policy identifier. Policies are numbered in the order they are added to the policy list.

Source
The source address or address group to which the policy applies. See “Firewall Address” on page 289. Address information can also be edited from the policy list. Clicking on the address opens the Edit Address dialog box.

Destination
The destination address or address group to which the policy applies. See “Firewall Address” on page 289. Address information can also be edited from the policy list. Clicking on the address opens the Edit Address dialog box.

Schedule
The schedule that controls when the policy should be active. See “Firewall Schedule” on page 301.

Service
The service to which the policy applies. See “Firewall Service” on page 293.

Profile
The protection profile that is associated with the policy.

Action
The response to make when the policy matches a connection attempt.

Status
Either enabled or disabled.

From
The source interface.

To
The destination interface.

VPN Tunnel
The VPN tunnel the VPN policy uses.

Authentication
The user authentication method the policy uses.

Comments
Comments entered when creating or editing the policy.

Label
The firewall section title.

Log
A green check mark indicates traffic logging is enabled for the policy; a grey cross mark indicates traffic logging is disabled for the policy.
**Adding a firewall policy**

Use the following steps to add a firewall policy to a firewall policy list.

1. Go to **Firewall > Policy**.
2. Select Create New or select the Insert Policy before icon beside a policy in the list to add the new policy above that policy.
3. Select the source and destination interfaces.
4. Select the source and destination addresses.
5. Configure the policy.
   For information about configuring policies, see “Configuring firewall policies” on page 271.
6. Select OK.
7. Arrange policies in the policy list so they have the expected results.
   For information about arranging policies in a policy list, see “How policy matching works” on page 268 and “Moving a policy to a different position in the policy list”.

**Moving a policy to a different position in the policy list**

You can move a policy in the list to influence how policies are evaluated. When more than one policy has been defined for the same interface pair, the policy that is first in the list is evaluated first.

The ordering of firewall encryption policies is important to ensure that they take effect as expected—firewall encryption policies must be evaluated before regular firewall policies.

Moving a policy in the list does not change its policy ID number.

**Figure 165: Move Policy**

1. Go to **Firewall > Policy**.
2. Select the Move To icon in the row beside the policy that you want to move.
3. Specify the position for the policy.
4. Select OK.
Configuring firewall policies

Use firewall policies to define how a firewall policy is selected to be applied to a communication session and to define how the FortiGate unit process the packets in that communication session.

To add or edit a firewall policy go to Firewall > Policy.

You can add ACCEPT policies that accept communication sessions. Using an accept policy you can apply FortiGate features such as virus scanning and authentication to the communication session accepted by the policy. An ACCEPT policy can enable interface-mode IPSec VPN traffic if either the source or the destination is an IPSec virtual interface. For more information, see “Overview of IPSec interface mode” on page 343.

You can add DENY policies to deny communication sessions.

You can also add IPSec encryption policies to enable IPSec tunnel mode VPN traffic and SSL VPN encryption policies to enable SSL VPN traffic. Firewall encryption policies determine which types of IP traffic will be permitted during an IPSec or SSL VPN session. If permitted by the firewall encryption policy, a tunnel may be initiated automatically whenever an IP packet of the specified type arrives at the FortiGate interface to the local private network. For more information, see “IPSec firewall policy options” on page 280 and/or “SSL-VPN firewall policy options” on page 281.

Figure 166: Policy options - NAT/Route mode ACCEPT policy

The source and destination Interface/Zone match the firewall policy with the source and destination of a communication session. The Address Name matches the source and destination address of the communication session. Schedule defines when the firewall policy is enabled.
Configuring firewall policies

Service matches the firewall policy with the service used by a communication session.

Action defines how the FortiGate unit processes traffic. Specify an action to accept or deny traffic or configure a firewall encryption policy.

You can use the remaining firewall policy options (NAT, Protection Profile, Log Allowed Traffic, Log Violation Traffic, Authentication, and Traffic shaping) to set additional features. Log Violation Traffic can be applied to policies that deny traffic. Differentiated services can be configured through CLI commands (see the “firewall” chapter of the FortiGate CLI Reference).

Firewall policy options

Go to Firewall > Policy and select Create New to add a firewall policy. You can configure the following firewall policy options:

Intra-VLAN Policy

(FortiGate model 224B only) This is available only in switch view. Enable to create a policy governing traffic between switch ports on a switch VLAN. There must be at least one secure port available. See “Configuring intra-VLAN firewall policies (FortiGate-224B only)” on page 275.

Source Interface/Zone

Select the name of the FortiGate interface or zone on which IP packets are received. Interfaces and zones are configured on the System Network page. See “Interface” on page 79 for information about interfaces. See “Zone” on page 98 for information about zones.

If Action is set to IPSEC, the interface is associated with the local private network.

If Action is set to SSL-VPN, the interface is associated with connections from remote SSL VPN clients.

Source Address

Select the name of a previously defined IP address to associate with the source interface or zone, or select Create New to define a new IP address or address group.

If you want to associate multiple addresses or address groups to the interface/zone, select Multiple beside Source Address. In the pop-up window, move the addresses or address groups from the Available Addresses box to the Members box, then select OK.

A packet must have the associated IP address in its header to be subject to the policy. Addresses can be created in advance. See “Configuring addresses” on page 291.

If Action is set to IPSEC, the address is the private IP address of the host, server, or network behind the FortiGate unit.

If Action is set to SSL-VPN and the policy is for web-only mode clients, select all.

If Action is set to SSL-VPN and the policy is for tunnel mode clients, select the name of the address that you reserved for tunnel mode clients.
Firewall Policy

Configuring firewall policies

Destination Interface/Zone
Select the name of the FortiGate interface or zone to which IP packets are forwarded. Interfaces and zones are configured on the System Network page. See “Interface” on page 79 for information about interfaces. See “Zone” on page 98 for information about zones.
If Action is set to IPSEC, the interface is associated with the entrance to the VPN tunnel.
If Action is set to SSL-VPN, the interface is associated with the local private network.

Destination Address
Select the name of a previously defined IP address to associate with the destination interface or zone, or select Create New to define a new IP address.
If you want to associate multiple addresses or address groups to the interface/zone, select Multiple beside Destination Address. In the pop-up window, move the addresses or address groups from the Available Addresses box to the Members box, then select OK.
A packet must have the associated IP address in its header to be subject to the policy. Addresses can be created in advance.
If Action is set to IPSEC, the address is the private IP address to which packets may be delivered at the remote end of the VPN tunnel.
If Action is set to SSL-VPN, select the name of the IP address that corresponds to the host, server, or network that remote clients need to access behind the FortiGate unit.

Schedule
Select a one-time or recurring schedule that controls when the policy is available to be matched with communication sessions. Schedules can be created in advance by going to Firewall > Schedule. See “Firewall Schedule” on page 301.
You can also select Create New to create a Recurring or One-time schedule during policy configuration. Add the information required for the recurring or one-time schedule and select OK. The new schedule is added to the Schedule list.

Service
Select the name of a service or service group that matches the service or protocol of the packets to be matched with this policy. Select from a wide range of predefined services. Custom services can be created in advance by going to Firewall > Service > Custom. Service groups can be created in advance by going to Firewall > Service > Group. See “Configuring custom services” on page 297 and “Configuring service groups” on page 300.
You can select Create New to create a custom service or a service group during policy configuration. Add the information required for the custom service or service group and select OK. The new custom service or service group is added to the Service list.
By selecting the Multiple button beside Service, you can select multiple services or service groups.

Action
Select how you want the firewall to respond when a packet matches the conditions of the policy.

ACCEPT
Accept traffic matched by the policy. You can configure NAT, protection profiles, log traffic, shape traffic, set authentication options, or add a comment to the policy.

DENY
Reject traffic matched by the policy. The only other configurable policy options are to log traffic (to log the connections denied by this policy) or add a comment.

IPSEC
Configure an IPSec firewall encryption policy, which causes the FortiGate unit to process IPSec VPN packets. See “IPSec firewall policy options” on page 280.

SSL-VPN
Configure an SSL-VPN firewall encryption policy, which causes the FortiGate unit to accept SSL VPN traffic. This option is available only after you have added a SSL-VPN user group. See “SSL-VPN firewall policy options” on page 281.
Configuring firewall policies

**NAT**
Enable Network Address Translation for the policy. NAT translates the source address and port of packets accepted by the policy. When NAT is selected, Dynamic IP Pool and Fixed Port can be configured.

**Dynamic IP Pool**
Select to translate the source address to an address randomly selected from an IP Pool. An IP Pool can be a single IP address or an IP address range. An IP pool list appears if IP Pool addresses have been added to the destination interface.

Select the name of an IP Pool added to the destination interface to cause the FortiGate unit to translate the source address to one of the addresses defined by this IP Pool.

Dynamic IP Pool cannot be selected if the destination interface, VLAN subinterface, or one of the interfaces or VLAN subinterfaces in the destination zone is configured using DHCP or PPPoE.

You cannot use IP pools when using zones. An IP pool can only be associated with an interface. For information about adding IP Pools, see "IP pools" on page 324.

**Fixed Port**
Select Fixed Port to prevent NAT from translating the source port.

Some applications do not function correctly if the source port is changed. In most cases, if Fixed Port is selected, Dynamic IP pool is also selected. If Dynamic IP pool is not selected, a policy with Fixed Port selected can only allow one connection at a time.

**Protection Profile**
Select a protection profile to configure how antivirus, web filtering, web category filtering, spam filtering, IPS, content archiving, and logging are applied to a firewall policy. Protection profiles can be created in advance or during profile configuration. Profiles created at this point appear in the protection profile list. For information about adding and configuring Protection profiles, see "Firewall Protection Profile" on page 329.

For authentication in the advanced settings, the protection profile option is disabled because the user group chosen for authentication is already tied to a protection profile. For more information about adding authentication to firewall policies, see "Adding authentication to firewall policies" on page 276.

**Log Allowed Traffic**
Select Log Allowed Traffic, for Accept, IPSEC or SSL-VPN policies to record messages to the traffic log whenever the policy processes a connection. Enable traffic log for a logging location (syslog, WebTrends, local disk if available, memory, or FortiAnalyzer) and set the logging severity level to Notification or lower. For information about logging, see "Log&Report" on page 469.

**Log Violation Traffic**
Select Log Violation Traffic, for Deny policies, to record messages to the traffic log whenever the policy processes a connection. Enable traffic log for a logging location (syslog, WebTrends, local disk if available, memory, or FortiAnalyzer) and set the logging severity level to Notification or lower. For information about logging, see "Log&Report" on page 469.

**Authentication**
Add users and a firewall protection profile to a user group before selecting Authentication. For information about adding and configuring user groups, see "User groups" on page 386. Authentication is available if Action is set to Accept or SSLVPN. For more information about adding authentication to firewall policies, see "Adding authentication to firewall policies" on page 276.

**Check FortiClient is Installed and Running**
On the FortiGate model 1000A, 3600A, and 5005FA2, firewall policies can deny access for hosts that do not have FortiClient Host Security software installed and operating. See "Options to check FortiClient on hosts" on page 282.
### Traffic Shaping

Traffic Shaping controls the bandwidth available to, and sets the priority of the traffic processed by, the policy.

- Be sure to enable traffic shaping on all firewall policies. If you do not apply any traffic shaping rule to a policy, the policy is set to high priority by default.
- Distribute firewall policies over all three priority queues (low, medium and high).
- Be sure that the sum of all Guaranteed Bandwidth in all firewall policies is significantly less than the bandwidth capacity of the interface.

For information about how to configure traffic shaping, see “Adding traffic shaping to firewall policies on page 278

### User Authentication Disclaimer

Display the Authentication Disclaimer page (a replacement message). The user must accept the disclaimer to connect to the destination. You can use the disclaimer in conjunction with authentication or a protection profile. This option is available on some models. It is not available for SSL-VPN policies.

### Redirect URL

If you enter a URL, the user is redirected to the URL after authenticating and/or accepting the user authentication disclaimer. This option is available on some models. It is not available for SSL-VPN policies.

### Comments

Add a description or other information about the policy. The comment can be up to 63 characters long, including spaces.

### Configuring intra-VLAN firewall policies (FortiGate-224B only)

In switch view, the FortiGate-224B unit can create firewall policies governing traffic between switch ports that are on the same switch VLAN. These are called switch VLAN-secure policies. If you want to create policies between VLANs, see “Firewall policy options on page 272.

An intra-VLAN policy must have at least one secure port as source or destination. It is not possible to create a firewall policy between two non-secure ports. For information about creating secure switch ports, see “Configuring a switch-LAN interface on page 210.

Go to **Firewall > Policy** and select Create New to configure a new firewall policy.
Adding authentication to firewall policies

Add users and a firewall protection profile to a user group before selecting Authentication. For information about adding and configuring user groups, see "User groups" on page 386. Authentication is available if Action is set to Accept or SSL VPN.

When you enable user authentication on a firewall policy, the end users using the firewall policy will be challenged to authenticate before they can use the policy.

In case of user ID and password authentication, the end users will be prompted to input their user name and password.

In case of certificate authentication (HTTPS or HTTP redirected to HTTPS only), you can install customized certificates on the FortiGate unit and the end users can also have customized certificates installed on their browsers. Otherwise, the end users will see a warning message and have to accept the default FortiGate certificate, which the end users’ web browsers may deem as invalid. For information about how to use certificates, see “VPN Certificates” on page 369.
User authentication supports the following protocols:

- HTTP
- HTTPS
- Telnet
- FTP

For information about configuring authentication protocols and other authentication settings, see “Authentication settings” on page 394.

You can specify which protocol will be used to issue the authentication challenge. The firewall policy must also include the authentication protocol for the end users to be able to get authenticated. For example, if you are creating a POP3 policy, and you have specified that HTTP protocol will be used for authentication, the firewall policy services must include at least HTTP and POP3.

**Figure 168: Selecting user groups for authentication**

Select Authentication and select one or more user groups to require users to enter a user name and password, or use certificates to authenticate, before the firewall accepts the connection.

- The Firewall authentication method includes locally defined user groups, as well as LDAP, and RADIUS users.
- Select Active Directory from the drop-down list to choose Active Directory groups defined in User > User Group. Authentication with Active Directory groups and other groups cannot be combined in the same policy.
- To use NTLM authentication, select NTLM from the drop-down list and choose Active Directory groups defined in User > User Group. You use AD groups as the members of the authentication group for NTLM.

**Note:** To allow the FortiGate unit to authenticate with an Active Directory server, the Fortinet Server Authentication Extensions (FSAE) must be installed on the Active Directory Domain Controller. FSAE is available from Fortinet Technical Support.

In most cases, ensure users can use DNS through the firewall without authentication. If DNS is not available, users cannot connect to a web, FTP, or Telnet server using a domain name.

**Note:** Policies that require authentication must be added to the policy list above matching policies that do not; otherwise, the policy that does not require authentication is selected first.
Adding traffic shaping to firewall policies

Traffic Shaping controls the bandwidth available to, and sets the priority of the traffic processed by, the policy. Traffic Shaping makes it possible to control which policies have the highest priority when large amounts of data are moving through the FortiGate device. For example, the policy for the corporate web server might be given higher priority than the policies for most employees' computers. An employee who needs unusually high-speed Internet access could have a special outgoing policy set up with higher bandwidth.

Traffic shaping is available for Accept, IPSEC, and SSL-VPN policies. It is also available for all supported services, including H.323, TCP, UDP, ICMP, and ESP.

Guaranteed and maximum bandwidth in combination with queuing ensures minimum and maximum bandwidth is available for traffic.

Traffic shaping cannot increase the total amount of bandwidth available, but it can be used to improve the quality of bandwidth-intensive and sensitive traffic.

Note: For more information about traffic shaping you can also see the FortiGate Traffic Shaping Technical Note.

Guaranteed bandwidth and maximum bandwidth

When you enter a value in the Guaranteed Bandwidth field of a firewall policy you guarantee the amount of bandwidth available for selected network traffic (in Kbytes/sec). For example, you may want to give a higher guaranteed bandwidth to your e-commerce traffic.

When you enter a value in the Maximum Bandwidth field of a firewall policy you limit the amount of bandwidth available for selected network traffic (in Kbytes/sec). For example, you may want to limit the bandwidth of IM traffic usage, so as to save some bandwidth for the more important e-commerce traffic.

The bandwidth available for traffic controlled by a policy is used for both the control and data sessions and is used for traffic in both directions. For example, if guaranteed bandwidth is applied to an internal to external FTP policy, and a user on an internal network uses FTP to put and get files, both the put and get sessions share the bandwidth available to the traffic controlled by the policy.

The guaranteed and maximum bandwidth available for a policy is the total bandwidth available to all traffic controlled by the policy. If multiple users start multiple communications session using the same policy, all of these communications sessions must share from the bandwidth available for the policy.

However, bandwidth availability is not shared between multiple instances of using the same service if these multiple instances are controlled by different policies. For example, you can create one FTP policy to limit the amount of bandwidth available for FTP for one network address and create another FTP policy with a different bandwidth availability for another network address.

Traffic Priority

Set traffic priority to manage the relative priorities of different types of traffic. Important and latency-sensitive traffic should be assigned a high priority. Less important and less sensitive traffic should be assigned a low priority.

The FortiGate Antivirus Firewall provides bandwidth to low-priority connections only when bandwidth is not needed for high-priority connections.
For example, you can add policies to guarantee bandwidth for voice and e-commerce traffic. Then you can assign a high priority to the policy that controls voice traffic and a medium priority to the policy that controls e-commerce traffic. During a busy time, if both voice and e-commerce traffic are competing for bandwidth, the higher priority voice traffic will be transmitted before the e-commerce traffic.

**Traffic shaping considerations**

Traffic shaping will by definition attempt to “normalize” traffic peaks/bursts and can be configured to prioritize certain flows over others. But there is a physical limitation to the amount of data which can be buffered and for how long. Once these thresholds have been surpassed, frames and packets will be dropped, and sessions will be affected. Incorrect traffic shaping configurations may actually further degrade certain network flows, since the excessive discarding of packets can create additional overhead at the upper layers, which may be attempting to recover from these errors.

A basic traffic shaping example would be to prioritize certain traffic flows at the detriment of other traffic which can be discarded. This would mean that you accept to sacrifice certain performance and stability on traffic X, in order to increase or guarantee performance and stability to traffic Y.

If for example you are applying bandwidth limitations to certain flows, you must accept the fact that these sessions can be limited and therefore negatively impacted.

Traffic shaping which is applied to a firewall policy, is enforced for traffic which may flow in either direction. Therefore a session which may be setup by an internal host to an external one, via a Internal -> External policy, will have Traffic shaping applied even if the data stream is then coming from external to internal. For example, an FTP “get” or a SMTP server connecting to an external one, in order to retrieve email.

Also note that traffic shaping is effective for normal IP traffic at normal traffic rates. Traffic shaping is not effective during extremely high-traffic situations where the traffic is exceeding the FortiGate unit’s capacity. Packets must be received by the FortiGate unit before they are subject to traffic shaping. If the FortiGate unit cannot process all of the traffic it receives, then dropped packets, delays, and latency are likely to occur.

To ensure that traffic shaping is working at its best, ensure that the interface ethernet statistics are clean of errors, collisions or buffer overruns. If these are not clean, then FortiGate and switch settings may require adjusting.

To make traffic shaping work efficiently, be sure to observe the following rules:

- Enable traffic shaping on all firewall policies. If you do not apply any traffic shaping rule to a policy, the policy is set to high priority by default.
- Distribute firewall policies over all three priority queues (low, medium and high).

Be sure that the sum of all Guaranteed Bandwidth in all firewall policies is significantly less than the bandwidth capacity of the interface. Configuring FortiGate traffic shaping

You enable and specify traffic shaping settings when you configure firewall policies.
To configure traffic shaping

1. Go to Firewall > Policy.
2. When you create a new policy or edit a policy, select the Traffic Shaping option.
3. Configure the following three options:

**Guaranteed Bandwidth**
Use traffic shaping to guarantee the amount of bandwidth available through the firewall for a policy. Guarantee bandwidth (in Kbytes) to ensure there is enough bandwidth available for a high-priority service. Be sure that the sum of all Guaranteed Bandwidth in all firewall policies is significantly less than the bandwidth capacity of the interface.

**Maximum Bandwidth**
Use traffic shaping to limit the amount of bandwidth available through the firewall for a policy. Limit bandwidth to keep less important services from using bandwidth needed for more important services.

**Traffic Priority**
Select High, Medium, or Low. Select Traffic Priority so the FortiGate unit manages the relative priorities of different types of traffic. For example, a policy for connecting to a secure web server needed to support e-commerce traffic should be assigned a high traffic priority. Less important services should be assigned a low priority. The firewall provides bandwidth to low-priority connections only when bandwidth is not needed for high-priority connections.

Be sure to enable traffic shaping on all firewall policies. If you do not apply any traffic shaping rule to a policy, the policy is set to high priority by default.

Distribute firewall policies over all three priority queues.

**Note:** If you set both guaranteed bandwidth and maximum bandwidth to 0 (zero), the policy does not allow any traffic.

**IPSec firewall policy options**

When Action is set to IPSEC, the following options are available:

**Figure 169:IPSEC encryption policy**

<table>
<thead>
<tr>
<th>VPN Tunnel</th>
<th>Auto Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow inbound</td>
<td></td>
</tr>
<tr>
<td>Allow outbound</td>
<td></td>
</tr>
</tbody>
</table>

**VPN Tunnel**
Select the VPN tunnel name defined in the phase 1 configuration. The specified tunnel will be subject to this firewall encryption policy.

**Allow Inbound**
Select to enable traffic from a dialup client or computers on the remote private network to initiate the tunnel.

**Allow outbound**
Select to enable traffic from computers on the local private network to initiate the tunnel.

**Inbound NAT**
Select to translate the source IP addresses of inbound decrypted packets into the IP address of the FortiGate interface to the local private network.

**Outbound NAT**
Select in combination with a natip CLI value to translate the source addresses of outbound cleartext packets into the IP address that you specify. Do not select Outbound NAT unless you specify a natip value through the CLI. When a natip value is specified, the source addresses of outbound IP packets are replaced before the packets are sent through the tunnel. For more information, see the "firewall" chapter of the FortiGate CLI Reference.
Note: For a route-based (interface mode) VPN, you do not configure an IPSEC firewall policy. Instead, you configure two regular ACCEPT firewall policies, one for each direction of communication, with the IPSec virtual interface as the source or destination interface as appropriate.

For more information, see the “Defining firewall policies” chapter of the *FortiGate IPSec VPN User Guide*.

### SSL-VPN firewall policy options

When Action is set to SSL-VPN, the following options are available:

**Note:** The SSL-VPN option is available from the Action list after one or more SSL VPN user groups have been created. To create user accounts and SSL VPN user groups, see “Configuring SSL VPN user group options” on page 392.

**Figure 170:** SSL-VPN encryption policy

- **SSL Client Certificate**
  - **Restrictive:** Allows traffic generated by holders of a (shared) group certificate. The holders of the group certificate must be members of an SSL VPN user group, and the name of that user group must be present in the Allowed field.

- **Cipher Strength**
  - Select one of the following options to determine the level of SSL encryption to use. The web browser on the remote client must be capable of matching the level that you select:
    - To use any cipher suite, select Any.
    - To use a 164-bit or greater cipher suite, select High >= 164.
    - To use a 128-bit or greater cipher suite, select Medium >= 128.

- **User Authentication Method**
  - Select one of the following options:
    - If the user group that will be bound to this firewall policy is a local user group, select Local.
    - If the remote clients will be authenticated by an external RADIUS server, select Radius.
    - If the remote clients will be authenticated by an external LDAP server, select LDAP.
    - Select Any to enable all of the above authentication methods. Local is attempted first, then Radius, then LDAP.

- **Available Groups**
  - Select the name of the user group requiring SSL VPN access, and then select the right-pointing arrow. Do not select more than one user group unless all members of the selected user groups have identical access requirements.

For information about how to create a firewall encryption policy for SSL VPN users, see the “SSL VPN administration tasks” chapter of the *FortiGate SSL VPN User Guide*.
Options to check FortiClient on hosts

On the FortiGate model 1000A, 3600A, and 5005FA2, firewall policies can deny access for hosts that do not have FortiClient Host Security software installed and operating. This feature can detect FortiClient software version 3.0 MR2 or later.

Figure 171: FortiClient Host Security check options

<table>
<thead>
<tr>
<th>Check FortiClient Installed and Running</th>
<th>Restrict Access for:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• FortiClient is Not Installed</td>
</tr>
<tr>
<td></td>
<td>• FortiClient is Not Licensed</td>
</tr>
<tr>
<td></td>
<td>• AV/IPS Database Out-of-Date</td>
</tr>
<tr>
<td></td>
<td>• AV Disabled</td>
</tr>
<tr>
<td></td>
<td>• Firewall Disabled</td>
</tr>
<tr>
<td></td>
<td>• Web Filter Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Redirect Restricted Users to FortiGate Download Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select to redirect denied users to the internal web portal which provides the reason for denial. On units that support it, users can download FortiClient Host Security software.</td>
</tr>
</tbody>
</table>

Firewall policy examples

FortiGate units are fully capable of meeting various network requirements from home use to SOHO, to large enterprises and ISPs. The following two scenarios will demonstrate the practical applications of firewall policies in the SOHO and large enterprise environments.

For more detail on these two examples please see the Example Library Network and SOHO and SMB Network Protection example guides in the FortiOS v3.0 MR2 documentation.

• Scenario one: SOHO sized business
• Scenario two: enterprise sized business

Scenario one: SOHO sized business

Company A is a small software company performing development and providing customer support. In addition to their internal network of 15 computers, they also have several employees that work from home all or some of the time.
With their current network topography, all 15 of the internal computers are behind a router and must go to an external source to access the IPS Mail and Web servers. All home based employees access the router through open/non secured connections.

Figure 172: Example SOHO network before FortiGate installation

Company A requires secure connections for home-based workers. Like many companies, they rely heavily on email and Internet access to conduct business. They want a comprehensive security solution to detect and prevent network attacks, block viruses, and decrease spam. They want to apply different protection settings for different departments. They also want to integrate web and email servers into the security solution.

To deal with their first requirement company A configures specific policies for each home-based worker to ensure secure communication between the home-based worker and the internal network.

1. Go to **Firewall > Policy**.
2. Select Create New and enter or select the following settings for Home_User_1:

<table>
<thead>
<tr>
<th>Interface / Zone</th>
<th>Source: internal</th>
<th>Destination: wan1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Source: CompanyA_Network</td>
<td>Destination: Home_User_1</td>
</tr>
<tr>
<td>Schedule</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>IPSEC</td>
<td></td>
</tr>
<tr>
<td>VPN Tunnel</td>
<td>Home1</td>
<td></td>
</tr>
<tr>
<td>Allow Inbound</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>
Firewall policy examples

3 Select OK

4 Select Create New and enter or select the following settings for Home_User_2:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow outbound</td>
<td>yes</td>
</tr>
<tr>
<td>Inbound NAT</td>
<td>yes</td>
</tr>
<tr>
<td>Outbound NAT</td>
<td>no</td>
</tr>
<tr>
<td>Protection Profile</td>
<td>Enable and select standard_profile</td>
</tr>
<tr>
<td>Interface / Zone</td>
<td>Source: internal Destination: wan1</td>
</tr>
<tr>
<td>Address</td>
<td>Source: CompanyA_network Destination: All</td>
</tr>
<tr>
<td>Schedule</td>
<td>Always</td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Action</td>
<td>IPSEC</td>
</tr>
<tr>
<td>VPN Tunnel</td>
<td>Home2_Tunnel</td>
</tr>
<tr>
<td>Allow Inbound</td>
<td>yes</td>
</tr>
<tr>
<td>Allow outbound</td>
<td>yes</td>
</tr>
<tr>
<td>Inbound NAT</td>
<td>yes</td>
</tr>
<tr>
<td>Outbound NAT</td>
<td>no</td>
</tr>
<tr>
<td>Protection Profile</td>
<td>Enable and select standard_profile</td>
</tr>
</tbody>
</table>

5 Select OK

Figure 173: SOHO network topology with FortiGate-100
The proposed network is based around a FortiGate 100A unit. The 15 internal computers are behind the FortiGate unit. They now access the email and web servers in a DMZ, which is also behind the FortiGate unit. All home based employees now access the office network through the FortiGate unit via VPN tunnels.

**Scenario two: enterprise sized business**

Located in a large city, the library system is anchored by a main downtown location serving most of the population, with more than a dozen branches spread throughout the city. Each branch is wired to the Internet but none are linked with each other by dedicated connections.

The current network topography at the main location consists of three user groups. The main branch staff and public terminals access the servers in the DMZ behind the firewall. The catalog access terminals directly access the catalog server without first going through the firewall.

The topography at the branch office has all three users accessing the servers at the main branch via non secured internet connections.

**Figure 174: The library system’s current network topology**

The library must be able to set different access levels for patrons and staff members.
The first firewall policy for main office staff members allows full access to the Internet at all times. A second policy will allow direct access to the DMZ for staff members. A second pair of policies are required to allow branch staff members the same access.

The staff firewall policies will all use a protection profile configured specifically for staff access. Enabled features include virus scanning, spam filtering, IPS, and blocking of all P2P traffic. FortiGuard web filtering is also used to block advertising, malware, and spyware sites.

A few users may need special web and catalog server access to update information on those servers, depending on how they’re configured. Special access can be allowed based on IP address or user.

The proposed topography has the main branch staff and the catalog access terminals going through a Fortigate HA cluster to the servers in a DMZ. The public access terminals first go through a FortiWiFi unit, where additional policies can be applied, to the HA Cluster and finally to the servers.

The branch office has all three users routed through a FortiWiFi unit to the main branch via VPN tunnels.

Figure 175: Proposed library system network topology

Policies are configured in **Firewall > Policy**. Protection Profiles are configured in **Firewall > Protection Profile**.
Main office ‘staff to Internet’ policy:

<table>
<thead>
<tr>
<th>Source Interface</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>All</td>
</tr>
<tr>
<td>Destination Interface</td>
<td>External</td>
</tr>
<tr>
<td>Destination Address</td>
<td>All</td>
</tr>
<tr>
<td>Schedule</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Accept</td>
</tr>
</tbody>
</table>

Main office ‘staff to DMZ’ policy:

<table>
<thead>
<tr>
<th>Source Interface</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>All</td>
</tr>
<tr>
<td>Destination Interface</td>
<td>DMZ</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Servers</td>
</tr>
<tr>
<td>Schedule</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Accept</td>
</tr>
</tbody>
</table>

Branches ‘staff to Internet’ policy:

<table>
<thead>
<tr>
<th>Source Interface</th>
<th>Branches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Branch Staff</td>
</tr>
<tr>
<td>Destination Interface</td>
<td>External</td>
</tr>
<tr>
<td>Destination Address</td>
<td>All</td>
</tr>
<tr>
<td>Schedule</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Accept</td>
</tr>
</tbody>
</table>

Branches ‘staff to DMZ’ policy:

<table>
<thead>
<tr>
<th>Source Interface</th>
<th>Branches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Branch Staff</td>
</tr>
<tr>
<td>Destination Interface</td>
<td>DMZ</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Servers</td>
</tr>
<tr>
<td>Schedule</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Accept</td>
</tr>
</tbody>
</table>

For more information regarding these examples, see:

- SOHO and SMB Configuration Example Guide
- FortiGate Enterprise Configuration Example
Firewall Address

Add, edit, and delete firewall addresses as required. Firewall addresses are added to the source and destination address fields of firewall policies. Firewall addresses are added to firewall policies to match the source or destination IP addresses of packets that are received by the FortiGate unit.

This section describes:
- About firewall addresses
- Viewing the firewall address list
- Configuring addresses
- Viewing the address group list
- Configuring address groups

About firewall addresses

A firewall address can be:
- The IP address of a single computer (for example, 192.45.46.45).
- The IP address of a subnetwork (for example, 192.168.1.0 for a class C subnet).
- 0.0.0.0 to represent all possible IP addresses

The netmask corresponds to the type of address being added. For example:
- The netmask for the IP address of a single computer should be 255.255.255.255.
- The netmask for a class A subnet should be 255.0.0.0.
- The netmask for a class B subnet should be 255.255.0.0.
- The netmask for a class C subnet should be 255.255.255.0.
- The netmask for all addresses should be 0.0.0.0

An IP Range address represents:
- A range of IP addresses in a subnet (for example, 192.168.20.1 to 192.168.20.10)

Note: IP address: 0.0.0.0 and Netmask: 255.255.255.255 is not a valid firewall address.

Organize related addresses into address groups to simplify policy creation.

A firewall address can be configured with a name, an IP address, and a netmask, or a name and IP address range. It can also be a fully qualified domain name (FQDN).

Enter an IP address and netmask using the following formats:
- x.x.x.x/x.x.x.x, for example 192.168.1.0/255.255.255.0
- x.x.x.x/x, for example 192.168.1.0/24
Viewing the firewall address list

Enter an IP address range using the following formats:

- `x.x.x.x-x.x.x.x`, for example `192.168.110.100-192.168.110.120`
- `x.x.x.[x-x]`, for example `192.168.110.[100-120]`
- `x.x.x.*`, for example `192.168.110.*` to represent all addresses on the subnet

An IP/Mask address can represent:

- The address of a subnet (for example, a class C subnet, IP address: 192.168.20.0 and Netmask: 255.255.255.0).
- A single IP address (for example, IP Address: 192.168.20.1 and Netmask: 255.255.255.255)
- All possible IP addresses (represented by IP Address: 0.0.0.0 and Netmask: 0.0.0.0)

Enter an FQDN using the following formats:

- `<host_name>.<second_level_domain_name>.<top_level_domain_name>`
- `<host_name>.<top_level_domain_name>`

An FQDN can be:

- `www.fortinet.com`
- `example.com`

Viewing the firewall address list

If virtual domains are enabled on the FortiGate unit, addresses are configured separately for each virtual domain. To access addresses, select a virtual domain from the list in the main menu.

Add addresses to the list and edit existing addresses. The FortiGate unit comes configured with the default ‘All’ address which represents any IP address on the network. Addresses in the list are sorted by type: IP/Mask, IP Range, and FQDN.

To view the address list, go to **Firewall > Address**.

Figure 176: Sample address list

<table>
<thead>
<tr>
<th>Name</th>
<th>Address / FQDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/Mask</td>
<td></td>
</tr>
<tr>
<td>Development</td>
<td>10.16.19.255/255.255.255.0</td>
</tr>
<tr>
<td>all</td>
<td>0.0.0.0/0.0.0.0</td>
</tr>
<tr>
<td>IP Range</td>
<td></td>
</tr>
<tr>
<td>Sales</td>
<td>192.168.10.[20-30]</td>
</tr>
<tr>
<td>Web_Sales</td>
<td>192.168.20.[50-75]</td>
</tr>
<tr>
<td>FQDN</td>
<td></td>
</tr>
<tr>
<td>Home</td>
<td><a href="http://www.fortinet.com">www.fortinet.com</a></td>
</tr>
</tbody>
</table>

The address list has the following icons and features:

- **Create New**: Select to add a firewall address.
- **Name**: The name of the firewall address.
- **Address/FQDN**: The IP address and mask, IP address range, or fully qualified domain name.
- **Delete icon**: Select to remove the address from the list. The Delete icon is only available if the address has not been used in a firewall policy.
- **Edit icon**: Select to edit the following information: Name, Type, Subnet/IP Range.
Configuring addresses

Addresses can also be created or edited during firewall policy configuration from the firewall policy window.

One FQDN may be mapped to multiple machines for load balancing and HA. A single FQDN firewall policy can be created in which the FortiGate unit automatically resolves and maintains a record of all addresses to which the FQDN resolves.

**Caution:** Using a fully qualified domain name in a firewall policy, while convenient, does present some security risks. Be very cautious when using this feature.

To add an IP address, IP range, or FQDN, go to Firewall > Address, select Create New.

**Figure 177:** New address or IP range options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Name</td>
<td>Enter a name to identify the firewall address. Addresses, address groups, and virtual IPs must have unique names to avoid confusion in firewall policies.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of address: Subnet/IP Range or FQDN.</td>
</tr>
<tr>
<td>Subnet/ IP Range</td>
<td>Enter the firewall IP address, forward slash, and subnet mask or enter an IP address range separated by a hyphen.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface or zone you want the IP address to associate with. Select Any if you want to associate the IP address with the interface/zone when you create the policy.</td>
</tr>
</tbody>
</table>

Viewing the address group list

If virtual domains are enabled on the FortiGate unit, address groups are configured separately for each virtual domain. To access address groups, select a virtual domain from the list in the main menu.

Organize related addresses into address groups to make it easier to configure policies. For example, after adding three addresses and configuring them in an address group, configure a single policy using all three addresses.

To view the address group list, go to Firewall > Address > Group.

**Note:** If an address group is included in a policy, it cannot be deleted unless it is first removed from the policy.
Configuring address groups

Address groups can be created during firewall configuration by selecting Create New from the Address dropdown list.

To organize addresses into an address group, go to Firewall > Address > Group.

The address group list has the following icons and features:

- **Create New**: Select to add an address group.
- **Group Name**: The name of the address group.
- **Members**: The addresses in the address group.
- **Delete icon**: Select to remove the group from the list. The Delete icon is only available if the address group has not been used in a firewall policy.
- **Edit icon**: Select to edit the following information: Group Name and Members.
Firewall Service

Use services to determine the types of communication accepted or denied by the firewall. Add any of the predefined services to a policy. Create custom services for each virtual domain and add services to service groups.

This section describes:

- Viewing the predefined service list
- Viewing the custom service list
- Configuring custom services
- Viewing the service group list
- Configuring service groups

Viewing the predefined service list

If virtual domains are enabled on the FortiGate unit, predefined services are available globally.

To view the predefined service list, on the main menu, select Global Configuration then go to Firewall > Service.

Figure 180: Predefined service list

<table>
<thead>
<tr>
<th>Name</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>AH</td>
<td>tcp/51</td>
</tr>
<tr>
<td>ANY</td>
<td>all</td>
</tr>
<tr>
<td>AOL</td>
<td>tcp/50-81,94</td>
</tr>
<tr>
<td>BGP</td>
<td>tcp/279</td>
</tr>
<tr>
<td>DHCP</td>
<td>udp/67-68</td>
</tr>
<tr>
<td>DNS</td>
<td>tcp/53, udp/53</td>
</tr>
<tr>
<td>ESP</td>
<td>ip/50</td>
</tr>
<tr>
<td>FINGER</td>
<td>tcp/23</td>
</tr>
<tr>
<td>FTP</td>
<td>tcp/21</td>
</tr>
<tr>
<td>FTP_GET</td>
<td>tcp/23</td>
</tr>
<tr>
<td>FTP_PUT</td>
<td>tcp/21</td>
</tr>
<tr>
<td>Gopher</td>
<td>tcp/76</td>
</tr>
<tr>
<td>GRE</td>
<td>tcp/47</td>
</tr>
<tr>
<td>HTTP</td>
<td>tcp/80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>tcp/443</td>
</tr>
<tr>
<td>ICMP</td>
<td>icmp/any</td>
</tr>
<tr>
<td>IMAP</td>
<td>tcp/143</td>
</tr>
</tbody>
</table>

The predefined services list has the following icons and features:

- **Name**: The name of the predefined service.
- **Detail**: The protocol for each predefined service.
Table 32 lists the FortiGate predefined firewall services. Add these services to any policy.

**Table 32: FortiGate predefined services**

<table>
<thead>
<tr>
<th>Service name</th>
<th>Description</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AH</strong></td>
<td>Authentication Header. AH provides source host authentication and data integrity, but not secrecy. This protocol is used for authentication by IPSec remote gateways set to aggressive mode.</td>
<td></td>
<td>51</td>
</tr>
<tr>
<td><strong>ANY</strong></td>
<td>Match connections on any port. A connection using any of the predefined services is allowed through the firewall.</td>
<td>all</td>
<td>all</td>
</tr>
<tr>
<td><strong>AOL</strong></td>
<td>AOL instant messenger protocol.</td>
<td>TCP</td>
<td>5190-5194</td>
</tr>
<tr>
<td><strong>BGP</strong></td>
<td>Border Gateway Protocol routing protocol. BGP is an interior/exterior routing protocol.</td>
<td>TCP</td>
<td>179</td>
</tr>
<tr>
<td><strong>DCE-RPC</strong></td>
<td>DCE/RPC stands for Distributed Computing Environment / Remote Procedure Calls. It is a means to call procedures from one application in another application, without having to know about what computer the other application is running on.</td>
<td>TCP</td>
<td>135</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>135</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>Dynamic Host Configuration Protocol (DHCP) allocates network addresses and delivers configuration parameters from DHCP servers to hosts.</td>
<td>UDP</td>
<td>53</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>Domain name service for translating domain names into IP addresses.</td>
<td>TCP</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>53</td>
</tr>
<tr>
<td><strong>ESP</strong></td>
<td>Encapsulating Security Payload. This service is used by manual key and AutoIKE VPN tunnels for communicating encrypted data. AutoIKE key VPN tunnels use ESP after establishing the tunnel using IKE.</td>
<td></td>
<td>50</td>
</tr>
<tr>
<td><strong>FINGER</strong></td>
<td>A network service providing information about users.</td>
<td>TCP</td>
<td>79</td>
</tr>
<tr>
<td><strong>FTP</strong></td>
<td>FTP service for transferring files.</td>
<td>TCP</td>
<td>21</td>
</tr>
<tr>
<td><strong>FTP_GET</strong></td>
<td>FTP service for uploading files.</td>
<td>TCP</td>
<td>21</td>
</tr>
<tr>
<td><strong>FTP_PUT</strong></td>
<td>FTP service for downloading files</td>
<td>TCP</td>
<td>21</td>
</tr>
<tr>
<td><strong>GOPHER</strong></td>
<td>Gopher communication service. Gopher organizes and displays Internet server contents as a hierarchically structured list of files.</td>
<td>TCP</td>
<td>70</td>
</tr>
<tr>
<td><strong>GRE</strong></td>
<td>Generic Routing Encapsulation. A protocol allowing an arbitrary network protocol to be transmitted over any other arbitrary network protocol, by encapsulating the packets of the protocol within GRE packets.</td>
<td></td>
<td>47</td>
</tr>
<tr>
<td><strong>H323</strong></td>
<td>H.323 multimedia protocol. H.323 is a standard approved by the International Telecommunication Union (ITU) defining how audiovisual conferencing data is transmitted across networks. For more information see the FortiGate Support for H.323 Technical Note.</td>
<td>TCP</td>
<td>1720, 1503</td>
</tr>
<tr>
<td>Service name</td>
<td>Description</td>
<td>Protocol</td>
<td>Port</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>HTTP</td>
<td>HTTP is the protocol used by the word wide web for transferring data for web pages.</td>
<td>TCP</td>
<td>80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HTTP with secure socket layer (SSL) service for secure communication with web servers.</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>ICMP_ANY</td>
<td>Internet Control Message Protocol is a message control and error-reporting protocol between a host and gateway (Internet).</td>
<td>ICMP</td>
<td></td>
</tr>
<tr>
<td>IKE</td>
<td>IKE is the protocol to obtain authenticated keying material for use with ISAKMP for IPSEC.</td>
<td>UDP</td>
<td>500</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol is a protocol used for retrieving email messages.</td>
<td>TCP</td>
<td>143</td>
</tr>
<tr>
<td>INFO_ADDRESS</td>
<td>ICMP information request messages.</td>
<td>ICMP</td>
<td>17</td>
</tr>
<tr>
<td>INFO_REQUEST</td>
<td>ICMP address mask request messages.</td>
<td>ICMP</td>
<td>15</td>
</tr>
<tr>
<td>IRC</td>
<td>Internet Relay Chat allows people connected to the Internet to join live discussions.</td>
<td>TCP</td>
<td>6660-6669</td>
</tr>
<tr>
<td>Internet-Locator-Service</td>
<td>Internet Locator Service includes LDAP, User Locator Service, and LDAP over TLS/SSL.</td>
<td>TCP</td>
<td>389</td>
</tr>
<tr>
<td>L2TP</td>
<td>L2TP is a PPP-based tunnel protocol for remote access.</td>
<td>TCP</td>
<td>1701</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol is a set of protocols used to access information directories.</td>
<td>TCP</td>
<td>389</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System allows network users to access shared files stored on computers of different types.</td>
<td>TCP</td>
<td>111, 2049</td>
</tr>
<tr>
<td>NNTP</td>
<td>Network News Transport Protocol is a protocol used to post, distribute, and retrieve USENET messages.</td>
<td>TCP</td>
<td>119</td>
</tr>
<tr>
<td>NTP</td>
<td>Network time protocol for synchronizing a computer’s time with a time server.</td>
<td>TCP</td>
<td>123</td>
</tr>
<tr>
<td>NetMeeting</td>
<td>NetMeeting allows users to teleconference using the Internet as the transmission medium.</td>
<td>TCP</td>
<td>1720</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First (OSPF) routing protocol. OSPF is a common link state routing protocol.</td>
<td></td>
<td>89</td>
</tr>
<tr>
<td>PC-Anywhere</td>
<td>PC-Anywhere is a remote control and file transfer protocol.</td>
<td>UDP</td>
<td>5632</td>
</tr>
<tr>
<td>PING</td>
<td>ICMP echo request/reply for testing connections to other devices.</td>
<td>ICMP</td>
<td>8</td>
</tr>
<tr>
<td>PING6</td>
<td>PING6 sends ICMPv6 ECHO_REQUEST packets to network hosts.</td>
<td></td>
<td>58</td>
</tr>
<tr>
<td>POP3</td>
<td>Post office protocol is an email protocol for downloading email from a POP3 server.</td>
<td>TCP</td>
<td>110</td>
</tr>
</tbody>
</table>
### Table 32: FortiGate predefined services (Continued)

<table>
<thead>
<tr>
<th>Service name</th>
<th>Description</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol is a protocol allowing corporations to extend their own corporate network through private tunnels over the public Internet.</td>
<td>TCP</td>
<td>1723</td>
</tr>
<tr>
<td>QUAKE</td>
<td>For connections used by the popular Quake multi-player computer game.</td>
<td>UDP</td>
<td>26000, 27000, 27910, 27960</td>
</tr>
<tr>
<td>RAUDIO</td>
<td>For streaming real audio multimedia traffic.</td>
<td>UDP</td>
<td>7070</td>
</tr>
<tr>
<td>REXEC</td>
<td>This command executes the specified command on a remote host. The remote host must be running a rexecd service (or daemon) for rexec to connect to.</td>
<td>TCP</td>
<td>512</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol is a common distance vector routing protocol.</td>
<td>UDP</td>
<td>520</td>
</tr>
<tr>
<td>RLOGIN</td>
<td>Rlogin service for remotely logging into a server.</td>
<td>TCP</td>
<td>513</td>
</tr>
<tr>
<td>RSH</td>
<td>Remote Shell, a UNIX command-line utility for remotely executing commands.</td>
<td>TCP</td>
<td>514</td>
</tr>
<tr>
<td>SAMBA</td>
<td>Samba allows Microsoft Windows clients to utilize file and print services from TCP/IP-enabled hosts.</td>
<td>TCP</td>
<td>139</td>
</tr>
<tr>
<td>SCCP</td>
<td>Skinny Client Control Protocol (SCCP) is a Cisco proprietary standard for terminal control for use with voice over IP (VoIP).</td>
<td>TCP</td>
<td>2000</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol defines how audiovisual conferencing data is transmitted across networks. For more information see the FortiGate SIP Support Technical Note.</td>
<td>UDP</td>
<td>5060</td>
</tr>
<tr>
<td>SIP-MSNmessenger</td>
<td>Session Initiation Protocol is used by Microsoft Messenger to initiate an interactive, possibly multimedia session.</td>
<td>TCP</td>
<td>1863</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol is used to send mail between email servers on the Internet.</td>
<td>TCP</td>
<td>25</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol is a set of protocols for managing complex networks</td>
<td>TCP</td>
<td>161-162</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>161-162</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell is a service for secure connections to computers for remote management.</td>
<td>TCP</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>22</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>Syslog service for remote logging.</td>
<td>UDP</td>
<td>514</td>
</tr>
<tr>
<td>TALK</td>
<td>A protocol supporting conversations between two or more users.</td>
<td>UDP</td>
<td>517-518</td>
</tr>
<tr>
<td>TCP</td>
<td>All TCP ports.</td>
<td>TCP</td>
<td>0-65535</td>
</tr>
<tr>
<td>TELNET</td>
<td>Telnet service for connecting to a remote computer to run commands.</td>
<td>TCP</td>
<td>23</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol is a simple file transfer protocol similar to FTP but with no security features.</td>
<td>UDP</td>
<td>69</td>
</tr>
<tr>
<td>TIMESTAMP</td>
<td>ICMP timestamp request messages.</td>
<td>ICMP</td>
<td>13</td>
</tr>
<tr>
<td>UDP</td>
<td>All UDP ports.</td>
<td>UDP</td>
<td>0-65535</td>
</tr>
</tbody>
</table>
Viewing the custom service list

If virtual domains are enabled on the FortiGate unit, custom services are configured separately for each virtual domain. To access custom services, select a virtual domain from the list in the main menu.

Add a custom service to create a policy for a service that is not in the predefined service list.

To view the custom service list, go to Firewall > Service > Custom.

Table 32: FortiGate predefined services (Continued)

<table>
<thead>
<tr>
<th>Service name</th>
<th>Description</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUCP</td>
<td>Unix to Unix copy utility, a simple file copying protocol.</td>
<td>UDP</td>
<td>540</td>
</tr>
<tr>
<td>VDOLIVE</td>
<td>For VDO Live streaming multimedia traffic.</td>
<td>TCP  7000-7010</td>
<td></td>
</tr>
<tr>
<td>WAIS</td>
<td>Wide Area Information Server is an Internet search protocol.</td>
<td>TCP</td>
<td>210</td>
</tr>
<tr>
<td>WINFRAME</td>
<td>For WinFrame communications between computers running Windows NT.</td>
<td>TCP</td>
<td>1494</td>
</tr>
<tr>
<td>X-WINDOWS</td>
<td>For remote communications between an X-Window server and X-Window clients.</td>
<td>TCP  6000-6063</td>
<td></td>
</tr>
</tbody>
</table>

Configuring custom services

Custom services can be created during firewall policy configuration by selecting Create New from the Service dropdown list.

To add a custom TCP or UDP service

1. Go to Firewall > Service > Custom.
2. Set Protocol Type to TCP/UDP.
3. Configure the following.
To add a custom ICMP service

1. Go to Firewall > Service > Custom.
2. Set Protocol Type to ICMP.
3. Configure the following.

To add a custom IP service

1. Go to Firewall > Service > Custom.
2. Set Protocol Type to IP.
3. Configure the following.
Viewing the service group list

If virtual domains are enabled on the FortiGate unit, service groups are created separately for each virtual domain. To access service groups, select a virtual domain from the list in the main menu.

To make it easier to add policies, create groups of services and then add one policy to allow or block access for all the services in the group. A service group can contain predefined services and custom services in any combination. A service group cannot be added to another service group.

To view the service group list, go to Firewall > Service > Group.

The service group list has the following icons and features:

- **Create New** Select to add a service group.
- **Group Name** The name to identify the service group.
- **Members** The services added to the service group.
- **Delete icon** Select to remove the entry from the list. The Delete icon is only available if the service group has not been used in a firewall policy.
- **Edit icon** Select to edit the following information: Group Name and Members.
Configuring service groups

Service groups can be created during firewall policy configuration by selecting Create New from the dropdown list.

To organize services into a service group, go to **Firewall > Service > Group**.

**Figure 186: Service group options**

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Enter a name to identify the service group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Services</td>
<td>The list of configured and predefined services. Use the arrows to move services between the lists.</td>
</tr>
<tr>
<td>Members</td>
<td>The list of services in the group. Use the arrows to move services between the lists.</td>
</tr>
</tbody>
</table>
Firewall Schedule

This section describes how to use schedules to control when policies are active or inactive. You can create one-time schedules or recurring schedules. One-time schedules are effective once for the period of time specified in the schedule. Recurring schedules repeat weekly. Recurring schedules are effective only at specified times of the day or on specified days of the week.

This section describes:
- Viewing the one-time schedule list
- Configuring one-time schedules
- Viewing the recurring schedule list
- Configuring recurring schedules

Viewing the one-time schedule list

If virtual domains are enabled on the FortiGate unit, one-time schedules are configured separately for each virtual domain. To access one-time schedules, select a virtual domain from the list on the main menu.

Create a one-time schedule that activates or deactivates a policy for a specified period of time. For example, a firewall might be configured with a default policy that allows access to all services on the Internet at all times. Add a one-time schedule to block access to the Internet during a holiday period.

To view the one-time schedule list, go to Firewall > Schedule > One-time.

Figure 187: One-time schedule list

<table>
<thead>
<tr>
<th>Name</th>
<th>Start</th>
<th>Stop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Christmas</td>
<td>2005/12/24 12:00</td>
<td>2005/12/27 00:00</td>
</tr>
</tbody>
</table>

The one-time schedule list has the following icons and features:

Create New: Select to add a one-time schedule.
Name: The name of the one-time schedule.
Start: The start date and time for the schedule.
Stop: The stop date and time for the schedule.
Delete icon: Select to remove the schedule from the list. The Delete icon only appears if the schedule is not being used in a firewall policy.
Edit icon: Select to edit the schedule.
**Configuring one-time schedules**

One-time schedules can be created during firewall policy configuration by selecting Create New from the Schedule dropdown list.

To add a one-time schedule, go to **Firewall > Schedule > One-time**.

![New One-time Schedule](image)

**Viewing the recurring schedule list**

If virtual domains are enabled on the FortiGate unit, recurring schedules are created separately for each virtual domain. To access recurring schedules, select a virtual domain from the list on the main menu.

Create a recurring schedule that activates or deactivates policies at specified times of the day or on specified days of the week. For example, prevent game play during working hours by creating a recurring schedule.

**Note:** A recurring schedule with a stop time that occurs before the start time starts at the start time and finishes at the stop time on the next day. Use this technique to create recurring schedules that run from one day to the next. Create a recurring schedule that runs for 24 hours by setting the start and stop times to the same time.

To view the recurring schedule list, go to **Firewall > Schedule > Recurring**.

![Recurring schedule list](image)

The recurring schedule list has the following icons and features:

- **Create New**: Select to add a recurring schedule.
- **Name**: The name of the recurring schedule.
- **Day**: The initials of the days of the week on which the schedule is active.
- **Start**: The start time of the recurring schedule.
Configuring recurring schedules

Recurring schedules can be created during firewall policy configuration by selecting Create New from the Schedule dropdown list.

To add a recurring schedule, go to Firewall > Schedule > Recurring.

Figure 190: New Recurring Schedule

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name to identify the recurring schedule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>Select the days of the week for the schedule to be active.</td>
</tr>
<tr>
<td>Start</td>
<td>Select the start time for the recurring schedule.</td>
</tr>
<tr>
<td>Stop</td>
<td>Select the stop time for the recurring schedule.</td>
</tr>
</tbody>
</table>

Recurring schedules use a 24-hour clock.
Firewall Virtual IP

This section describes FortiGate Virtual IPs and IP Pools and how to configure and use them in firewall policies.

This section describes:

- Virtual IPs
- Viewing the virtual IP list
- Configuring virtual IPs
- Virtual IP Groups
- Viewing the VIP group list
- Configuring VIP groups
- IP pools
- Viewing the IP pool list
- Configuring IP Pools
- Double NAT: combining IP pool with virtual IP

Virtual IPs

Virtual IPs can be used to allow connections through a FortiGate unit using network address translation (NAT) firewall policies. Virtual IPs use Proxy ARP so that the FortiGate unit can respond to ARP requests on a network for a server that is actually installed on another network. Proxy ARP is defined in RFC 1027.

For example, you can add a virtual IP to an external FortiGate unit interface so that the external interface can respond to connection requests for users who are actually connecting to a server on the DMZ or internal network.

How virtual IPs map connections through the FortiGate unit

An example use of static NAT virtual IP is to allow easy public access to a web server on a private network protected by a FortiGate unit. Reduced to its basics, this example involves only three parts, as shown in Figure 191: the web server on a private network, the browsing computer on the Internet, and the FortiGate unit connecting the two networks.

A client computer attempts to contact the server. The client computer sends data packets and the FortiGate unit receives them. The addresses in the packets are remapped, and they’re forwarded to the server on the private network.

Figure 191: A simple static NAT virtual IP example.
The packets sent from the client computer have a source IP of 192.168.37.55 and a destination IP of 192.168.37.4. The FortiGate unit receives these packets at its external interface. The virtual IP settings indicate a mapping from 192.168.37.4 to 10.10.10.42 so the packets' addresses are changed. The source address is changed to 10.10.10.2 and the destination is changed to 10.10.10.42. The FortiGate unit makes a note of this translation in the firewall session table it maintains internally. The packets are then sent on their way and arrive at the server computer.

Figure 192: Example of packet address remapping during NAT from client to server.

Note that the client computer's address does not appear in the packets the server receives. After the FortiGate unit translates the network addresses, there is no reference to the client computer's network. The server has no indication another network exists. As far as the server can tell, all the communication is coming directly from the FortiGate unit.

When the server answers the client computer, the procedure works the same way but in the other direction. The server sends its response packets having a source IP address of 10.10.10.42 and a destination IP address of 10.10.10.2. The FortiGate unit receives these packets at its internal interface. This time however, the firewall session table entry is used to determine what the destination address will be translated to.

In this example, the source address is changed to 192.168.37.4 and the destination is changed to 192.168.37.55. The packets are then sent on their way and arrive at the client computer.

The server computer's address does not appear in the packets the client receives. After the FortiGate unit translates the network addresses, there is no reference to the server computer's network. The client has no indication the server's private network exists. As far as the client is concerned, the FortiGate unit is the web server.

Figure 193: Example of packet address remapping during NAT from server to client.

Note: Virtual IPs are not available or required in transparent mode.

A Virtual IP can be a single IP address or an IP address range bound to a FortiGate unit interface. When you bind an IP address or IP address range to a FortiGate unit interface using a virtual IP, the interface responds to ARP requests for the bound IP address or IP address range.
If the NAT check box is not selected when building the firewall policy, the resulting policy will perform destination network address translation (DNAT). DNAT accepts packets from an external network that are intended for a specific destination IP address, translates the destination address of the packets to a mapped IP address on another hidden network, and then forwards the packets through the FortiGate unit to the hidden destination network. Unlike in the previous examples, the source address is not translated. Once on the hidden destination network, the packets can arrive at their final destination.

Virtual IPs also translate the source IP address or addresses of return packets from the source address on the hidden network to be the same as the destination address of the originating packets.

Virtual IP ranges can be of almost any size and can translate addresses to different subnets. Virtual IP ranges have the following restrictions:

- The mapped IP cannot include 0.0.0.0 or 255.255.255.255.
- The external IP cannot be 0.0.0.0 if the virtual IP type is static NAT and is mapped to a range of IP addresses. Only load balance virtual IPs, and static NAT virtual IPs mapped to a single IP address, support an external IP of 0.0.0.0.
- Port mapping maps a range of external port numbers to a range of internal port numbers. The number of ports in these two ranges must be equal. Therefore, the external port must not be set so that its range exceeds 65535. For example, an internal range of 20 ports mapped from external port 65530 is invalid as the last port in the range would be 65550.
- When port forwarding, the external IP range cannot include any interface IP addresses.
- The mapped IP range must not include any interface IP addresses.
- Virtual IP name cannot be the same as any address name or address group name.
- No duplicate entries or overlapping ranges are permitted.

In addition to binding the IP address or IP address range to the interface, the virtual IP also contains all of the information required to map the IP address or IP address range from the interface that receives the packets to the interface connected to the same network as the actual IP address or IP address range.

You can create different kinds of virtual IPs, each of which can be used for a different DNAT variation.
Viewing the virtual IP list

To view the virtual IP list, go to Firewall > Virtual IP > Virtual IP.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP</th>
<th>Service Port</th>
<th>Map to IP/Range</th>
<th>Map to Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development</td>
<td>192.168.1.254/24</td>
<td>tel/225</td>
<td>192.168.25.2-1</td>
<td>tel/2580</td>
</tr>
<tr>
<td>Marketing</td>
<td>192.168.25.10</td>
<td></td>
<td>172.31.1.25-3-1</td>
<td></td>
</tr>
</tbody>
</table>
The virtual IP list has the following icons and features:

- **Create New**: Select to add a virtual IP.
- **Name**: The name of the virtual IP.
- **IP**: The external IP address or IP address range.
- **Service Port**: The external port number or port number range. The service port is included in port forwarding virtual IPs.
- **Map to IP/IP Range**: The mapped to IP address or address range on the destination network.
- **Map to Port**: The mapped to port number or port number range. The map to port is included in port forwarding virtual IPs.
- **Delete icon**: Remove the virtual IP from the list. The Delete icon only appears if the virtual IP is not being used in a firewall policy.
- **Edit icon**: Edit the virtual IP to change any virtual IP option including the virtual IP name.

### Configuring virtual IPs

To add a virtual IP, go to **Firewall > Virtual IP > Virtual IP** and select Create new. To edit a virtual IP, go to **Firewall > Virtual IP > Virtual IP** and select the Edit icon for the virtual IP to edit.

- **Name**: Enter or change the name to identify the virtual IP. To avoid confusion, firewall policies, addresses, address groups, and virtual IPs cannot share names.
- **External Interface**: Select the virtual IP external interface from the list. The external interface is connected to the source network and receives the packets to be forwarded to the destination network. You can select any FortiGate interface, VLAN subinterface, or VPN interface.
- **Type**: Select Static NAT or Server Load Balance. For details about VIP types, see “How virtual IPs map connections through the FortiGate unit” on page 305.
- **External IP Address/Range**: Enter the external IP address that you want to map to an address on the destination network. To configure a dynamic virtual IP that accepts connections for any IP address, set the external IP address to 0.0.0.0. For a static NAT dynamic virtual IP you can only add one mapped IP address. For a load balance dynamic virtual IP you can specify a single mapped address or a mapped address range.
- **Mapped IP Address/Range**: Enter the real IP address on the destination network to which the external IP address is mapped. You can also enter an address range to forward packets to multiple IP addresses on the destination network. For a static NAT virtual IP, if you add a mapped IP address range the FortiGate unit calculates the external IP address range and adds the IP address range to the External IP Address/Range field.
Configuring virtual IPs

Firewall Virtual IP

Method
If you select Server Load Balance, you can select one of the following load balancing methods.

- **Static**: The traffic load is spread evenly across all servers, no additional server is required.
- **Round Robin**: Directs requests to the next server, and treats all servers as equals regardless of response time or number of connections. Dead servers or non-responsive servers are avoided. A separate server is required.
- **Weighted**: Servers with a higher weight value will receive a larger percentage of connections. Set the server weight when adding a server.

Port forwarding
Select to add a port forwarding virtual IP.

Protocol
Select the protocol (TCP or UDP) that you want the forwarded packets to use.

External Service Port
Enter the external service port number for which you want to configure port forwarding.

Map to Port
Enter the port number on the destination network to which the external port number is mapped.
You can also enter a port number range to forward packets to multiple ports on the destination network.
For a static NAT virtual IP, if you add a map to port range the FortiGate unit calculates the external port number range and adds the port number range to the External Service port field.

Real Servers
If you select Server Load Balancing for the VIP type, enter the real server IP addresses. At least one IP address is required and you can enter up to eight addresses.
To enter a server IP address, select Add under Real Servers and enter the following information:

- **IP**: Enter the IP address of the server.
- **Port**: If you enable port forwarding, enter the port number on the destination network to which the external port number is mapped.
- **Dead interval**: The interval of time that a connection can remain idle before it is dropped. A range of 10-255 seconds can be used.
- **Wake interval**: The interval of time the connection will try to detect a server before giving up. A range of 10-255 seconds can be used.
- **Weight**: Determines the weight value of a specific server. The higher the weight value, the higher the percentage of connections the server will handle. A range of 1-255 can be used.
- **Health Check**: Enable this option to use ping detection to check the status of the server before forwarding the session.

Adding a static NAT virtual IP for a single IP address

The IP address 192.168.37.4 on the Internet is mapped to 10.10.10.42 on a private network. Attempts to communicate with 192.168.37.4 from the Internet are translated and sent to 10.10.10.42 by the FortiGate unit. The computers on the Internet are unaware of this translation and see a single computer at 192.168.37.4 rather than a FortiGate unit with a private network behind it.
To add a static NAT virtual IP for a single IP address

1. Go to Firewall > Virtual IP > Virtual IP.
2. Select Create New.
3. Use the following procedure to add a virtual IP that allows users on the Internet to connect to a web server on the DMZ network. In our example the external interface of the FortiGate unit is connected to the Internet and the dmz1 interface is connected to the DMZ network.

   **Name**: simple_static_NAT
   **External Interface**: external
   **Type**: Static NAT
   **External IP Address/Range**: The Internet IP address of the web server. The external IP address must be a static IP address obtained from your ISP for your web server. This address must be a unique IP address that is not used by another host and cannot be the same as the IP address of the external interface the virtual IP will be using. However, the external IP address must be routed to the selected interface. The virtual IP address and the external IP address can be on different subnets. When you add the virtual IP, the external interface responds to ARP requests for the external IP address.

   **Map to IP/IP Range**: The IP address of the server on the internal network. Since there is only one IP address, leave the second field blank.

4. Select OK.
To add a static NAT virtual IP for a single IP address to a firewall policy

Add a external to dmz1 firewall policy that uses the virtual IP so that when users on the Internet attempt to connect to the web server IP address packets pass through the FortiGate unit from the external interface to the dmz1 interface. The virtual IP translates the destination address of these packets from the external IP to the DMZ network IP address of the web server.

1. Go to Firewall > Policy and select Create New.
2. Configure the firewall policy:
   - **Source Interface/Zone**: external
   - **Source Address**: All (or a more specific address)
   - **Destination Interface/Zone**: dmz1
   - **Destination Address**: simple_static_nat
   - **Schedule**: always
   - **Service**: HTTP
   - **Action**: ACCEPT

3. Select NAT.
4. Select OK.

Adding a static NAT virtual IP for an IP address range

The IP address range 192.168.37.4-192.168.37.6 on the Internet is mapped to 10.10.10.42-10.10.123.44 on a private network. Packets from Internet computers communicating with 192.168.37.4 are translated and sent to 10.10.10.42 by the FortiGate unit. Similarly, packets destined for 192.168.37.5 are translated and sent to 10.10.10.43, and packets destined for 192.168.37.6 are translated and sent to 10.10.10.44. The computers on the Internet are unaware of this translation and see three computers with individual IP addresses rather than a FortiGate unit with a private network behind it.

To add a static NAT virtual IP for an IP address range

1. Go to Firewall > Virtual IP > Virtual IP.
2. Select Create New.
3 Use the following procedure to add a virtual IP that allows users on the Internet to connect to three individual web servers on the DMZ network. In our example the external interface of the FortiGate unit is connected to the Internet and the dmz1 interface is connected to the DMZ network.

Use the following procedure to add a virtual IP that allows users on the Internet to connect to three individual web servers on the DMZ network. In our example the external interface of the FortiGate unit is connected to the Internet and the dmz1 interface is connected to the DMZ network.

<table>
<thead>
<tr>
<th>Name</th>
<th>static_NAT_range</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Interface</td>
<td>external</td>
</tr>
<tr>
<td>Type</td>
<td>Static NAT</td>
</tr>
<tr>
<td>External IP Address/Range</td>
<td>The Internet IP address range of the web servers. The external IP addresses must be static IP addresses obtained from your ISP for your web server. These addresses must be unique IP addresses that are not used by another host and cannot be the same as the IP addresses of the external interface the virtual IP will be using. However, the external IP addresses must be routed to the selected interface. The virtual IP addresses and the external IP address can be on different subnets. When you add the virtual IP, the external interface responds to ARP requests for the external IP addresses.</td>
</tr>
<tr>
<td>Map to IP/IP Range</td>
<td>The IP address range of the servers on the internal network. Define the range by entering the first address of the range in the first field and the last address of the range in the second field.</td>
</tr>
</tbody>
</table>

4 Select OK.

To add a static NAT virtual IP with an IP address range to a firewall policy

Add a external to dmz1 firewall policy that uses the virtual IP so that when users on the Internet attempt to connect to the server IP addresses, packets pass through the FortiGate unit from the external interface to the dmz1 interface. The virtual IP translates the destination addresses of these packets from the external IP to the DMZ network IP addresses of the servers.

1 Go to Firewall > Policy and select Create New.
2 Configure the firewall policy:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>external</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>All (or a more specific address)</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>dmz1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>static_NAT_range</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>HTTP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

3 Select NAT.
4 Select OK.
Adding static NAT port forwarding for a single IP address and a single port

The IP address 192.168.37.4, port 80 on the Internet is mapped to 10.10.10.42, port 8000 on a private network. Attempts to communicate with 192.168.37.4, port 80 from the Internet are translated and sent to 10.10.10.42, port 8000 by the FortiGate unit. The computers on the Internet are unaware of this translation and see a single computer at 192.168.37.4, port 80 rather than a FortiGate unit with a private network behind it.

Figure 199: Static NAT virtual IP port forwarding for a single IP address and a single port example

To add static NAT virtual IP port forwarding for a single IP address and a single port

1. Go to Firewall > Virtual IP > Virtual IP.
2. Select Create New.
3. Use the following procedure to add a virtual IP that allows users on the Internet to connect to a web server on the DMZ network. In our example the external interface of the FortiGate unit is connected to the Internet and the dmz1 interface is connected to the DMZ network.

<table>
<thead>
<tr>
<th>Name</th>
<th>Port_fwd_NAT_VIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Interface</td>
<td>external</td>
</tr>
<tr>
<td>Type</td>
<td>Static NAT</td>
</tr>
<tr>
<td>External IP Address/Range</td>
<td>The Internet IP address of the web server. The external IP address must be a static IP address obtained from your ISP for your web server. This address must be a unique IP address that is not used by another host and cannot be the same as the IP address of the external interface the virtual IP will be using. However, the external IP address must be routed to the selected interface. The virtual IP address and the external IP address can be on different subnets. When you add the virtual IP, the external interface responds to ARP requests for the external IP address.</td>
</tr>
<tr>
<td>Map to IP/IP Range</td>
<td>The IP address of the server on the internal network. Since there is only one IP address, leave the second field blank.</td>
</tr>
<tr>
<td>Port Forwarding</td>
<td>Selected</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
</tbody>
</table>
Firewall Virtual IP

Configuring virtual IPs

Firewall Virtual IP

Figure 200: Virtual IP options; Static NAT port forwarding virtual IP for a single IP address and a single port

To add static NAT virtual IP port forwarding for a single IP address and a single port to a firewall policy

Add a external to dmz1 firewall policy that uses the virtual IP so that when users on the Internet attempt to connect to the web server IP addresses, packets pass through the FortiGate unit from the external interface to the dmz1 interface. The virtual IP translates the destination addresses and ports of these packets from the external IP to the dmz network IP addresses of the web servers.

1. Go to Firewall > Policy and select Create New.
2. Configure the firewall policy:

   - Source Interface/Zone: external
   - Source Address: All (or a more specific address)
   - Destination Interface/Zone: dmz1
   - Destination Address: Port_fwd_NAT_VIP
   - Schedule: always
   - Service: HTTP
   - Action: ACCEPT

3. Select NAT.
4. Select OK.

Adding static NAT port forwarding for an IP address range and a port range

Ports 80 to 83 of addresses 192.168.37.4 to 192.168.37.7 on the Internet are mapped to ports 8000 to 8003 of addresses 10.10.10.42 to 10.10.10.44 on a private network. Attempts to communicate with 192.168.37.5, port 82 from the Internet, for example, are translated and sent to 10.10.10.43, port 8002 by the FortiGate unit. The computers on the Internet are unaware of this translation and see a single computer at 192.168.37.5 rather than a FortiGate unit with a private network behind it.
To add static NAT virtual IP port forwarding for an IP address range and a port range

1. Go to Firewall > Virtual IP > Virtual IP.
2. Select Create New.
3. Use the following procedure to add a virtual IP that allows users on the Internet to connect to a web server on the DMZ network. In our example the external interface of the FortiGate unit is connected to the Internet and the dmz1 interface is connected to the DMZ network.

   - **Name**: Port_fwd_NAT_VIP_port_range
   - **External Interface**: external
   - **Type**: Static NAT
   - **External IP Address/Range**: The external IP addresses must be static IP addresses obtained from your ISP. This addresses must be unique, not used by another host, and cannot be the same as the IP address of the external interface the virtual IP will be using. However, the external IP addresses must be routed to the selected interface. The virtual IP addresses and the external IP address can be on different subnets. When you add the virtual IP, the external interface responds to ARP requests for the external IP addresses.
   - **Map to IP/IP Range**: The IP addresses of the server on the internal network. Define the range by entering the first address of the range in the first field and the last address of the range in the second field.
   - **Port Forwarding**: Selected
   - **Protocol**: TCP
   - **External Service Port**: The ports that traffic from the Internet will use. For a web server, this will typically be port 80.
   - **Map Port**: The ports on which the server expects traffic. Define the range by entering the first port of the range in the first field and the last port of the range in the second field. If there is only one port, leave the second field blank.

4. Select OK.
To add static NAT virtual IP port forwarding for an IP address range and a port range to a firewall policy

Add a external to dmz1 firewall policy that uses the virtual IP so that when users on the Internet attempt to connect to the web server IP addresses, packets pass through the FortiGate unit from the external interface to the dmz1 interface. The virtual IP translates the destination addresses and ports of these packets from the external IP to the dmz network IP addresses of the web servers.

1. Go to Firewall > Policy and select Create New.
2. Configure the firewall policy:
   - Source Interface/Zone: external
   - Source Address: All (or a more specific address)
   - Destination Interface/Zone: dmz1
   - Destination Address: Port_fwd_NAT_VIP_port_range
   - Schedule: always
   - Service: HTTP
   - Action: ACCEPT

3. Select NAT.
4. Select OK.

Adding a server load balance virtual IP

In this example the IP address 192.168.37.4 on the Internet, is mapped to the following servers behind the fortiGate unit, 10.10.123.42, 10.10.123.43, and 10.10.123.44. The IP address mapping is determined by the FortiGate unit’s load balancing algorithm. Attempts to communicate with 192.168.37.4 from the Internet are translated and sent to 10.10.10.42, 10.10.10.43, or 10.10.10.44 by the FortiGate unit. The computers on the Internet are unaware of this translation and see a single computer at 192.168.37.4 rather than a FortiGate unit with a private network behind it.

**Note:** Server load balancing maps a single IP on one network to up to eight real server IPs on another network. At least one real address must be added to use this feature.

**Figure 202: Server Load balance virtual IP**
To add a server load balance virtual IP

1. Go to **Firewall > Virtual IP > Virtual IP**.
2. Select **Create New**.
3. Use the following procedure to add a virtual IP that allows users on the Internet to connect to a web server on the DMZ network. In our example the external interface of the FortiGate unit is connected to the Internet and the dmz1 interface is connected to the DMZ network.

   **Name**
   - **Load_Bal_VIP**

   **External Interface**
   - **external**

   **Type**
   - **Server Load Balance**

   **External IP address/Range**
   - The public IP addresses of the web servers.
   The external IP address must be a static IP address obtained from your ISP for your web server. This address must be a unique IP address that is not used by another host and cannot be the same as the IP address of the external interface the virtual IP will be using. However, the external IP address must be routed to the selected interface. The virtual IP address and the external IP address can be on different subnets. When you add the virtual IP, the external interface responds to ARP requests for the external IP address.

   **Method**
   - Select one of the load balance methods. For details, see "Configuring virtual IPs" on page 309.

   **Real Servers**
   - If you select Server Load Balancing for the VIP type, enter the real server IP addresses. For details about real server settings, see "Configuring virtual IPs" on page 309.

   **Figure 203: Virtual IP options; server load balancing virtual IP**

4. Select **OK**.
To add a server load balance virtual IP to a firewall policy

Add a external to dmz1 firewall policy that uses the virtual IP so that when users on the Internet attempt to connect to the web server IP address packets pass through the FortiGate unit from the external interface to the dmz1 interface. The virtual IP translates the destination address of these packets from the external IP to the dmz network IP addresses of the web servers.

1. Go to Firewall > Policy and select Create New.
2. Configure the firewall policy:
   - Source Interface/Zone: external
   - Source Address: All (or a more specific address)
   - Destination Interface/Zone: dmz1
   - Destination Address: Server_Load_Bal_VIP
   - Schedule: always
   - Service: HTTP
   - Action: ACCEPT

Adding a server load balance port forwarding virtual IP

In this example, connections to 192.168.37.4 on the Internet are mapped to 10.10.10.42, 10.10.10.43, and 10.10.10.44 on a private network. The IP address mapping is determined by the FortiGate unit’s load balancing algorithm. The external service port on 192.168.37.4 is mapped to specified ports in conjunction with the specified IP addresses. The computers on the Internet are unaware of this translation and see a single computer at 192.168.37.4 rather than a FortiGate unit with a private network behind it.

Figure 204: Server load balance virtual IP port forwarding

To add a server load balance port forwarding virtual IP

1. Go to Firewall > Virtual IP > Virtual IP.
2. Select Create New.
3. Use the following procedure to add a virtual IP that allows users on the Internet to connect to a web server on the DMZ network. In our example the external interface of the FortiGate unit is connected to the Internet and the dmz1 interface is connected to the DMZ network.
Configuring virtual IPs

Name: Load_Bal_VIP_port_forward
External Interface: external
Type: Server Load Balance

**External IP Address/Range:**
The public IP addresses of the web servers. The external IP address must be a static IP address obtained from your ISP for your web server. This address must be a unique IP address that is not used by another host and cannot be the same as the IP address of the external interface the virtual IP will be using. However, the external IP address must be routed to the selected interface. The virtual IP address and the external IP address can be on different subnets. When you add the virtual IP, the external interface responds to ARP requests for the external IP address.

**Method:** Select one of the load balance methods. For details, see “Configuring virtual IPs” on page 309.

**Real Servers:** If you select Server Load Balancing for the VIP type, enter the real server IP addresses. For details about real server settings, see “Configuring virtual IPs” on page 309.

**Port Forwarding:** Selected

**Protocol:** TCP

**External Service Port:** The ports that traffic from the Internet will use. For a web server, this will typically be port 80.

Figure 205: Server load balanced port forwarding

4. Select OK.
To add a server load balance virtual IP to a firewall policy

Add a external to dmz1 firewall policy that uses the virtual IP so that when users on the Internet attempt to connect to the web server IP address packets pass through the FortiGate unit from the external interface to the dmz1 interface. The virtual IP translates the destination address of these packets from the external IP to the dmz network IP addresses of the web servers.

1. Go to Firewall > Policy and select Create New.
2. Configure the firewall policy:
   - **Source Interface/Zone**: external
   - **Source Address**: All (or a more specific address)
   - **Destination Interface/Zone**: dmz1
   - **Destination Address**: Load_Bal_VIP_port_forward
   - **Schedule**: always
   - **Service**: HTTP
   - **Action**: ACCEPT
3. Select NAT.
4. Select OK.

Adding dynamic virtual IPs

Adding a dynamic virtual IP is similar to adding a virtual IP. The difference is that the External IP address must be set to 0.0.0.0 so the External IP address matches any IP address.

To add a dynamic virtual IP

1. Go to Firewall > Virtual IP > Virtual IP.
2. Select Create New.
3. Enter a name for the dynamic virtual IP.
4. Select the virtual IP External Interface from the list.
   - The external interface is connected to the source network and receives the packets to be forwarded to the destination network.
   - Select any firewall interface or a VLAN subinterface.
5. Set the External IP Address to 0.0.0.0.
   - The 0.0.0.0 External IP Address matches any IP address.
6. Enter the Map to IP address to which to map the external IP address. For example, the IP address of a PPTP server on an internal network.
7. Select Port Forwarding.
8. For Protocol, select TCP.
9. Enter the External Service Port number for which to configure dynamic port forwarding.
   - The external service port number must match the destination port of the packets to be forwarded. For example, if the virtual IP provides PPTP passthrough access from the Internet to a PPTP server, the external service port number should be 1723 (the PPTP port).
10 Enter the Map to Port number to be added to packets when they are forwarded.
Enter the same number as the External Service Port if the port is not to be translated.

11 Select OK.

Adding a virtual IP with port translation only

When adding a virtual IP, if you enter the virtual IP address as same as the mapped IP address and use port forwarding, the destination IP address will not be changed, but the port number will be changed as you specify.

To add a virtual IP with port translation only

1 Go to Firewall > Virtual IP > Virtual IP.
2 Select Create New.
3 Enter a name for the dynamic virtual IP.
4 Select the virtual IP External Interface from the list.
The external interface is connected to the source network and receives the packets to be forwarded to the destination network.
Select any firewall interface or a VLAN subinterface.
5 Set the External IP Address as the mapped IP address.
6 Enter the Map to IP address to which to map the external IP address. For example, the IP address of a PPTP server on an internal network.
7 Select Port Forwarding.
8 For Protocol, select TCP.
9 Enter the External Service Port number for which to configure dynamic port forwarding.
The external service port number must match the destination port of the packets to be forwarded. For example, if the virtual IP provides PPTP passthrough access from the Internet to a PPTP server, the external service port number should be 1723 (the PPTP port).
10 Enter the Map to Port number to be added to packets when they are forwarded.
11 Select OK.

Virtual IP Groups

You can create virtual IP groups to facilitate firewall policy traffic control. For example, on the DMZ interface, if you have two email servers that use Virtual IP mapping, you can put these two VIPs into one VIP group and create one external-to-DMZ policy, instead of two policies, to control the traffic.

Viewing the VIP group list

To view the virtual IP group list, go to Firewall > Virtual IP > VIP Group.
Configuring VIP groups

To add a VIP group, go to **Firewall > Virtual IP > VIP Group** and select Create new. To edit a VIP group, go to **Firewall > Virtual IP > VIP Group** and select the Edit icon for the VIP group to edit.

Configure the following settings and select OK:
IP pools

Use IP pools to add NAT policies that translate source addresses to addresses randomly selected from the IP pool rather than being limited to the IP address of the destination interface.

An IP pool defines an address or a range of IP addresses, all of which respond to ARP requests on the interface to which the IP pool is added.

Select Enable Dynamic IP Pool in a firewall policy to translate the source address of outgoing packets to an address randomly selected from the IP pool. An IP pool list appears when the policy destination interface is the same as the IP pool interface.

With an IP pool added to the internal interface, you can select Dynamic IP pool for policies with the internal interface as the destination.

Add multiple IP pools to any interface and select the IP pool to use when configuring a firewall policy.

A single IP address is entered normally. For example, 192.168.110.100 is a valid IP pool address. If an IP address range is required, use either of the following formats.

- x.x.x.x-x.x.x.x, for example 192.168.110.100-192.168.110.120
- x.x.x.[x-x], for example 192.168.110.[100-120]

IP pools and dynamic NAT

Use IP pools for dynamic NAT. For example, an organization might have purchased a range of Internet addresses but has only one Internet connection on the external interface of the FortiGate unit.

Assign one of the organization’s Internet IP addresses to the external interface of the FortiGate unit. If the FortiGate unit is operating in NAT/Route mode, all connections from the network to the Internet appear to come from this IP address.

For connections to originate from all the Internet IP addresses, add this address range to an IP pool for the external interface. Then select Dynamic IP Pool for all policies with the external interface as the destination. For each connection, the firewall dynamically selects an IP address from the IP pool to be the source address for the connection. As a result, connections to the Internet appear to be originating from any of the IP addresses in the IP pool.
**IP Pools for firewall policies that use fixed ports**

Some network configurations do not operate correctly if a NAT policy translates the source port of packets used by the connection. NAT translates source ports to keep track of connections for a particular service. Select fixed port for NAT policies to prevent source port translation. However, selecting fixed port means that only one connection can be supported through the firewall for this service. To be able to support multiple connections, add an IP pool to the destination interface, and then select dynamic IP pool in the policy. The firewall randomly selects an IP address from the IP pool and assigns it to each connection. In this case the number of connections that the firewall can support is limited by the number of IP addresses in the IP pool.

**Source IP address and IP pool address matching**

When the source addresses are translated to the IP pool addresses, one of the following three cases may occur:

**Scenario 1: The number of source addresses equals that of IP pool addresses**

In this case, the FortiGate unit will always match the IP addressed one to one. If you use fixed port in such a case, the FortiGate unit will preserve the original source port. However, this may cause conflicts if more than one firewall policy uses the same IP pool, or the same IP addresses are used in more than one IP pool.

<table>
<thead>
<tr>
<th>Original address</th>
<th>Change to</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>172.16.30.1</td>
</tr>
<tr>
<td>192.168.1.2</td>
<td>172.16.30.2</td>
</tr>
<tr>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>192.168.1.254</td>
<td>172.16.30.254</td>
</tr>
</tbody>
</table>

**Scenario 2: The number of source addresses is more than that of IP pool addresses**

In this case, the FortiGate unit translates IP addresses using a wrap-around mechanism. If you use fixed port in such a case, the FortiGate unit preserves the original source port. But conflicts may occur since users may have different sessions using the same TCP 5 tuples.

<table>
<thead>
<tr>
<th>Original address</th>
<th>Change to</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>172.16.30.10</td>
</tr>
<tr>
<td>192.168.1.2</td>
<td>172.16.30.11</td>
</tr>
<tr>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>192.168.1.10</td>
<td>172.16.30.19</td>
</tr>
<tr>
<td>192.168.1.11</td>
<td>172.16.30.10</td>
</tr>
<tr>
<td>192.168.1.12</td>
<td>172.16.30.11</td>
</tr>
<tr>
<td>192.168.1.13</td>
<td>172.16.30.12</td>
</tr>
<tr>
<td>......</td>
<td>......</td>
</tr>
</tbody>
</table>
Scenario 3: The number of source addresses is fewer than that of IP pool addresses

In this case, some of the IP pool addresses will be used and the rest of them will not be used.

<table>
<thead>
<tr>
<th>Original address</th>
<th>Change to</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>172.16.30.10</td>
<td></td>
</tr>
<tr>
<td>192.168.1.2</td>
<td>172.16.30.11</td>
<td></td>
</tr>
<tr>
<td>192.168.1.3</td>
<td>172.16.30.12</td>
<td></td>
</tr>
<tr>
<td>No more source addresses</td>
<td>172.16.30.13 and other addresses will not be used</td>
<td></td>
</tr>
</tbody>
</table>

Viewing the IP pool list

If virtual domains are enabled on the FortiGate unit, IP pools are created separately for each virtual domain. To access IP pools, select a virtual domain from the list on the main menu. IP pools are not available in Transparent mode.

To view the IP pool list go to Firewall > Virtual IP > IP Pool.

Figure 208: IP pool list

<table>
<thead>
<tr>
<th>Name</th>
<th>Start IP</th>
<th>End IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin_Dev</td>
<td>192.168.100</td>
<td>192.168.109.100</td>
</tr>
<tr>
<td>Finance_Dev</td>
<td>192.168.108.25</td>
<td>192.168.109.59</td>
</tr>
<tr>
<td>wan1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment</td>
<td>192.168.110.1</td>
<td>192.168.119.100</td>
</tr>
</tbody>
</table>

The IP pool list has the following icons and features:

- **Create New**: Select to add an IP pool.
- **Name**: The name of the IP pool.
- **Start IP**: The start IP defines the start of an address range.
- **End IP**: The end IP defines the end of an address range.
- **Delete icon**: Select to remove the entry from the list. The Delete icon only appears if the IP pool is not being used in a firewall policy.
- **Edit icon**: Select to edit the following information: Name, Interface, IP Range/Subnet.
Configuring IP Pools

To add an IP pool, go to **Firewall > Virtual IP > IP Pool**.

**Figure 209: New Dynamic IP Pool**

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter or change the name for the IP pool.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Select the interface to which to add an IP pool.</td>
</tr>
<tr>
<td>IP Range/Subnet</td>
<td>Enter the IP address range for the IP pool. The IP range defines the start and end of an address range. The start of the range must be lower than the end of the range. The IP range does not have to be on the same subnet as the IP address of the interface to which the IP pool is being added.</td>
</tr>
</tbody>
</table>

**Double NAT: combining IP pool with virtual IP**

When creating a firewall policy, you can use both IP pool and virtual IP for double IP and/or port translation.

For example, in the following network topology:

- Users in the 10.1.1.0/24 subnet use port 8080 to access server 172.16.1.1.
- The server’s listening port is 80.
- Fixed ports must be used.

**Figure 210: Double NAT**
To allow the local users to access the server, you can use fixed port and IP pool to allow more than one user connection while using virtual IP to translate the destination port from 8080 to 80.

**To create an IP pool**
1. Go to **Firewall > Virtual IP > IP Pool**.
2. Select Create New.
3. Enter the following information and select OK.
   - **Name**: pool-1
   - **Interface**: DMZ
   - **IP Range/Subnet**: 10.1.3.1-10.1.3.254

**To create a Virtual IP with port translation only**
1. Go to **Firewall > Virtual IP > Virtual IP**.
2. Select Create New.
3. Enter the following information and select OK.
   - **Name**: server-1
   - **External Interface**: Internal
   - **Type**: Static NAT
   - **External IP**: 172.16.1.1
   - **Address/Range**: Note this address is the same as the server address.
   - **Mapped IP**: 172.16.1.1
   - **Address/Range**: 
   - **Port Forwarding**: Enable
   - **Protocol**: TCP
   - **External Service Port**: 8080
   - **Map to Port**: 80

**To create a firewall policy**
Add an internal to dmz firewall policy that uses the virtual IP to translate the destination port number and the IP pool to translate the source addresses.
1. Go to **Firewall > Policy** and select Create New.
2. Configure the firewall policy:
   - **Source Interface/Zone**: internal
   - **Source Address**: 10.1.1.0/24
   - **Destination Interface/Zone**: dmz
   - **Destination Address**: server-1
   - **Schedule**: always
   - **Service**: HTTP
   - **Action**: ACCEPT
3. Select NAT.
4. Select OK.
Firewall Protection Profile

This section describes how to add protection profiles to NAT/Route mode and Transparent mode policies.

This section describes:

• What is a protection profile?
• Default protection profiles
• Viewing the protection profile list
• Configuring a protection profile
• Adding a protection profile to a policy
• Protection profile CLI configuration

What is a protection profile?

A protection profile is a group of settings you can adjust to suit a particular purpose. Since protection profiles apply different protection settings to traffic controlled by firewall policies, you can tailor the settings to the type of traffic each policy handles. Use protection profiles to:

• Configure antivirus protection for HTTP, FTP, IMAP, POP3, SMTP, and IM policies.
• Configure web filtering for HTTP and HTTPS policies.
• Configure web category filtering for HTTP and HTTPS policies.
• Configure spam filtering for IMAP, POP3, and SMTP policies.
• Enable IPS for all services.
• Configure content archiving for HTTP, HTTPS, FTP, IMAP, POP3, SMTP, and IM policies.
• Configure IM filtering and access control for AIM, ICQ, MSN, Yahoo, and SIMPLE instant messaging.
• Configure P2P access and bandwidth control for Bit Torrent, eDonkey, Gnutella, Kazaa, Skype, and WinNY peer to peer clients.
• Configure which protection profile actions will be logged.
• Configure rate limiting for VoIP protocols (SIP and SCCP).

Using protection profiles, you can customize types and levels of protection for different firewall policies.

For example, while traffic between internal and external addresses might need strict protection, traffic between trusted internal addresses might need moderate protection. Configure policies for different traffic services to use the same or different protection profiles.

If virtual domains are enabled on the FortiGate unit, protection profiles are configured globally and are available to all virtual domains. To access protection profiles, go to Global Configuration > Firewall > Protection Profile.
Default protection profiles

The FortiGate unit is preconfigured with four default protection profiles. In many cases you can use these default protection profiles as is instead of adding new protection profiles.

**Strict**
- Apply maximum protection to HTTP, FTP, IMAP, POP3, and SMTP traffic. The strict protection profile may not be useful under normal circumstances but it is available when maximum protection is required.

**Scan**
- Apply virus scanning to HTTP, FTP, IMAP, POP3, and SMTP traffic. Quarantine is also selected for all content services. On FortiGate models with a hard drive, if antivirus scanning finds a virus in a file, the file is quarantined on the FortiGate hard disk. If required, system administrators can recover quarantined files.

**Web**
- Apply virus scanning and web content blocking to HTTP traffic. Add this protection profile to firewall policies that control HTTP traffic.

**Unfiltered**
- Apply no scanning, blocking or IPS. Use the unfiltered content profile if no content protection for content traffic is required. Add this protection profile to firewall policies for connections between highly trusted or highly secure networks where content does not need to be protected.

Viewing the protection profile list

To view the protection profile list, go to **Firewall > Protection Profile**.

**Figure 211: Default protection profiles**

<table>
<thead>
<tr>
<th>Name</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan</td>
<td><img src="icon1.png" alt="Icon" /></td>
</tr>
<tr>
<td>Strict</td>
<td><img src="icon2.png" alt="Icon" /></td>
</tr>
<tr>
<td>Unfiltered</td>
<td><img src="icon3.png" alt="Icon" /></td>
</tr>
<tr>
<td>Web</td>
<td><img src="icon4.png" alt="Icon" /></td>
</tr>
</tbody>
</table>

The Protection Profile list has the following icons and features:

- **Create New**: Select to add a protection profile.
- **Name**: The name of the protection profile
- **Delete**: Select to remove a protection profile from the list. The Delete icon is only available if the profile is not being used in a firewall policy.
- **Edit**: Select to modify a protection profile.

**Note**: A protection profile cannot be deleted (the Delete icon is not visible) if it is selected in a firewall policy or included in a user group.
Configuring a protection profile

If the default protection profiles do not provide the settings required, create custom protection profiles.

To add a protection profile, go to Firewall > Protection Profile and select Create New.

Figure 212: New Protection Profile

Profile Name
Enter a name for the protection profile.

Comments
If required, enter a description of the profile. The comment text must be less than 63 characters long. Otherwise, it will be truncated.

AntiVirus
See “Antivirus options” on page 332.

Web Filtering
See “Web filtering options” on page 333.

FortiGuard Web Filtering
See “FortiGuard Web Filtering options” on page 334.

Spam Filtering
See “Spam filtering options” on page 336.

IPS
See “IPS options” on page 338.

Content Archive
See “Content archive options” on page 338.

IM & P2P
See “IM and P2P options” on page 339.

VoIP
See “VoIP options” on page 340.

Logging
See “Logging options” on page 341.

Note: If both Virus Scan and File Block are enabled, the FortiGate unit blocks files matching enabled file patterns before they are scanned for viruses.
Antivirus options

Figure 213: Protection profile antivirus options

<table>
<thead>
<tr>
<th>Option</th>
<th>HTTP</th>
<th>FTP</th>
<th>IMAP</th>
<th>POP3</th>
<th>SMTP</th>
<th>IM</th>
<th>NNTP</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus Scan</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Pattern</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quarantine</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pass Fragmented Emails</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comfort Clients</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interval (1 - 999 seconds)</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amount (1 - 19249 bytes)</td>
<td>10</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Over-sized File/Email</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Book</td>
<td>Pass</td>
</tr>
<tr>
<td>Threshold (1 - 547 MB)</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add signature to outgoing emails</td>
<td>Enable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(SMTP only)</td>
</tr>
</tbody>
</table>

Note: NNTP options cannot be selected. Support will be added in the future.

The following options are available for antivirus through the protection profile.

**Virus Scan**: Enable or disable virus scanning for each protocol (HTTP, FTP, IMAP, POP3, SMTP, IM). Grayware, if enabled in AntiVirus > Config > Grayware, is included with the Virus Scan. Heuristic, if enabled with the CLI, is also included with the Virus Scan. Note that streaming mode is enabled automatically when you enable virus scanning.

**File Pattern**: Enable or disable file pattern processing for each protocol. Files can be blocked or allowed by name, extension, or any other pattern. File pattern processing provides the flexibility to block files that may contain harmful content.

**Quarantine (log disk required)**: Enable or disable quarantine for each protocol. Quarantine suspect files to view them or submit files to Fortinet for analysis. The quarantine option is not displayed in the protection profile if the FortiGate does not have a hard drive or a configured FortiAnalyzer unit.

**Pass fragmented emails**: Enable or disable passing fragmented email for mail protocols (IMAP, POP3, SMTP). Fragmented email cannot be scanned for viruses.

**Comfort Clients**: Enable or disable client comforting for HTTP and FTP traffic. Client comforting provides a visual status for files that are being buffered for downloads using HTTP and FTP. Users can observe web pages being drawn or file downloads progressing. If disabled, users have no indication the FortiGate unit is buffering the download and they may cancel the transfer thinking it has failed.

**Interval**: The time in seconds before client comforting starts after the download has begun. It is also the time between subsequent intervals.

**Amount**: The number of bytes sent at each interval.
Oversized File/Email

Select block or pass for files and email messages exceeding configured thresholds for each protocol.

Threshold

If the file is larger than the threshold value in megabytes, the file is passed or blocked, as set in the Oversized File/Email drop down. The maximum threshold for scanning in memory is 10% of the FortiGate unit RAM.

Note: For email scanning, the oversize threshold refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes smaller than the configured oversize threshold.

Add signature to outgoing emails

Create and enable a signature to append to outgoing email (SMTP only).

See “AntiVirus” on page 397 for more antivirus configuration options.

Web filtering options

Figure 214: Protection profile web filtering options

<table>
<thead>
<tr>
<th>Web Filtering</th>
<th>HTTP</th>
<th>HTTPS</th>
<th>URL Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Content Block</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Content Exempt</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web URL Filter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ActiveX Filter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cookie Filter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Java Applet Filter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Processing Decorated Block</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Unread Emails</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following options are available for web filtering through the protection profile.

Web Content Block

Enable or disable web page blocking for HTTP traffic based on the content block patterns in the content block list.

Web content block drop-down list: Select which content block list will be used with this protection profile.

Threshold: If the combined scores of the content block patterns appearing on a web page exceed the threshold value, the page will be blocked. See “Viewing the web content block list” on page 427 for details.

Web Content Exempt

Enable or disable the override of web content block based on the content exempt patterns in the content exempt list.

Web content exempt drop-down list: Select which content exempt list will be used with this protection profile.

Web URL Filter

Enable or disable web page filtering for HTTP and HTTPS traffic based on the URL list.

Web URL filter drop-down list: Select which web URL filter list will be used with this protection profile.

ActiveX Filter

Enable blocking of ActiveX controls.

Cookie Filter

Enable blocking of cookies.

Java Applet Filter

Enable blocking of Java applets.
Configuring a protection profile

Web resume download block

Enable to block downloading parts of a file that have already been partially downloaded. Enabling this option will prevent the unintentional download of virus files hidden in fragmented files. Note that some types of files, such as PDFs, are fragmented to increase download speed. Enabling this option can cause download interruptions with these types of file.

Block Invalid URLs

The FortiGate unit can perform validation on the CN to ensure that it is a valid hostname before applying web-filtering. If the CN is not a valid hostname, the traffic will be blocked if you enable this option.

See "Web Filter" on page 423 for more web filter configuration options.

FortiGuard Web Filtering options

Figure 215: Protection profile FortiGuard Web Filtering options

<table>
<thead>
<tr>
<th>Category</th>
<th>Allow</th>
<th>Block</th>
<th>Log</th>
<th>Allow Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potentially Usable</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Controversial</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Potentially Non-productive</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Potentially Bandwidths Consuming</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Potential Security Violating</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>General Interest</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Business-Oriented</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Others</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Unrated</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Local Categories</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

The following options are available for web category filtering through the protection profile.

Enable FortiGuard Web Filtering

Enable FortiGuard Web Filtering category blocking.

Enable FortiGuard Web Filtering Overrides

Enable category overrides. When selected, a list of groups is displayed. If no groups are available, the option is grayed out. For more information about overrides, see "Viewing the override list" on page 436 and "Configuring override rules" on page 437. For more information about groups, see "User groups" on page 386.

Provide details for blocked HTTP 4xx and 5xx errors (HTTP only)

Display a replacement message for 400 and 500-series HTTP errors. If the error is allowed through, malicious or objectionable sites can use these common error pages to circumvent web category blocking.
Rate images by URL (blocked images will be replaced with blanks) (HTTP only)

Block images that have been rated by FortiGuard. Blocked images are replaced on the originating web pages with blanks. Image types that are rated are GIF, JPEG, PNG, BMP, and TIFF.

Allow websites when a rating error occurs

Allow web pages that return a rating error from the web filtering service.

Strict Blocking

Strict blocking only has an effect when either a URL fits into a category and classification or IP rating is enabled. With IP rating enabled, all URLs have two categories and up to two classifications (one set for the domain and one set for the IP address). All URLs belong to at least one category (Unrated is a category) and may belong to one classification too.

If strict blocking is enabled, a site is blocked if it is in at least one blocked category or classification and only allowed if all categories or classifications it falls under are allowed.

With strict blocking disabled, a site is allowed if it belongs to at least one allowed category or classification and only blocked if all categories or classifications it falls under are allowed.

For example, if a protection profile blocks “Search Engines” but allows “Image Search” and the URL “images.google.ca” falls into the Search Engines category and the Image Search classification.

With strict blocking enabled, this URL is blocked because it belongs to the Search Engines category, which is blocked.

With strict blocking disabled, the URL is allowed because it is classified as Image Search, which is allowed. It would only be blocked if both the Search Engines category and Image Search classification were blocked.

This option is enabled by default.

Rate URLs by domain and IP address

When enabled, this option sends both the URL and the IP address of the requested site for checking, providing additional security against attempts to bypass the FortiGuard system. However, because IP rating is not updated as quickly as URL rating, some false ratings may occur.

This option is disabled by default.

Category

The FortiGuard Web Filtering content filtering service provides many categories by which to filter web traffic. Set the action to take on web pages for each category. Choose from allow, block, log, or allow override.

Classification

Classifications block whole classes of web sites. Web sites that provide cached content, Google for example, can be blocked. Web sites that allow image, audio, or video searches can also be blocked. Web sites that are classified are also rated in one of the categories or are unrated. Choose from allow, block, monitor, or allow override.

See “FortiGuard - Web Filter” on page 435 for more category blocking configuration options.
Spam filtering options

Figure 216: Protection profile spam filtering options

<table>
<thead>
<tr>
<th>Spam Filtering</th>
<th>IP</th>
<th>FOPS</th>
<th>SMTP</th>
<th>NNTP</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGuard Anti-spam IP address check</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL check</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail checksum check</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam submission</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address DMY check</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HELO DNS lookup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email address DMY check</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Return email DNS check</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blocked word check</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Spam Action: tagged - tagged - tagged

Appeared to: subject - MIME - subject - MIME

Appeared with: Spam - Spam - Spam - Spam

Note: NNTP options cannot be selected. Support will be added in the future.

The following options are available for spam filtering through the protection profile.

**FortiGuard Antispam IP address check**
Enable or disable the FortiGuard Antispam filtering IP address blacklist. FortiGuard Antispam extracts the SMTP mail server source address and sends the IP address to a FortiGuard Antispam server to see if this IP address matches the list of known spammers. If the IP address is found, FortiGuard Antispam terminates the session. If FortiGuard Antispam does not find a match, the mail server sends the email to the recipient.

See "FortiGuard Antispam Service" on page 187 for more information about this service.

**URL check**
Enable or disable the FortiGuard Antispam spam filtering URL blacklist. FortiGuard Antispam checks the body of email messages to extract any URL links. These URL links are sent to a FortiGuard Antispam server to see if any are listed. Spam messages often contain URL links to advertisements (also called spamvertising). If a URL match is found, FortiGuard Antispam terminates the session. If FortiGuard Antispam does not find a match, the mail server sends the email to the recipient.

See "FortiGuard Antispam Service" on page 187 for more information about this service.

**E-mail checksum check**
Enable or disable the FortiGuard Antispam email message checksum blacklist. If enabled, this filter calculates the checksum of an email message and sends this checksum to the FortiGuard servers to determine if the checksum is in the blacklist. The FortiGate unit then passes or marks/blocks the email message according to the server response.

**Spam submission**
When enabled, all e-mail messages marked as spam have a link added to the message body. If an email message is not spam, simply click the link in the message to inform FortiGuard of the false positive.
See "Antispam" on page 443 for more spam filter configuration options. To configure the FortiGuard Anti-spam service, see "Configuring the FortiGate unit for FDN and FortiGuard services" on page 188.
IPS options

Figure 217: Protection profile IPS options

<table>
<thead>
<tr>
<th>IPS</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Signature</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPS Anomaly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following options are available for IPS through the protection profile.

**IPS Signature**
Select one or more IPS signature severity levels for this profile. Options are Critical, High, Medium, Low, and Information. Signatures with severity levels that have not been selected are not triggered.

**IPS Anomaly**
Select one or more IPS anomaly severity levels for this profile. Options are Critical, High, Medium, Low, and Information. Anomalies with severity levels that have not been selected are not triggered.

See "Intrusion Protection" on page 411 for more IPS configuration options.

Content archive options

You can choose to display the content meta-information of the HTTP, HTTPS, FTP, IMAP, POP3, SMTP, and IM traffic on the system dashboard, or archive the full content to a FortiAnalyzer device.

You must enable at least one of the content protection functions, such as AV scanning, web filtering, and spam filtering, for the relevant protocol, before you can use the full content archiving features for that protocol. In other words, if no content protection function is enabled for a protocol, the full content of that protocol will not be archived to the FortiAnalyzer even if you enable Full Content Archive.

Taking FTP for example, the following lists the three content archiving scenarios:

- If you do not enable AV scanning for FTP, but you select Full Content Archive, the FTP files will not be archived to the FortiAnalyzer device. Only the meta-information is recorded.
- If you enable AV scanning for FTP, but you select Pass for files larger than 10MB, files larger than 10MB will not be archived to the FortiAnalyzer device. Only the meta-information is recorded.
- If you enable AV scanning for FTP, but you select Block for files larger than 10MB, files larger than 10MB will not be archived to the FortiAnalyzer device, and the meta-information will not be recorded either.

To be able to access all content archiving options, a FortiAnalyzer unit must be configured and logging to the FortiAnalyzer must be enabled. For more information, see "Logging to a FortiAnalyzer unit" on page 472.

Figure 218: Protection profile content archive options
Note: NNTP and file archiving options cannot be selected. Support will be added in the future.

The following options are available for content archive through the protection profile.

**Display content meta-information on the system dashboard**
Enable to have meta-information for each type of traffic display in the Statistics section of the FortiGate status page. View statistics for HTTP traffic, HTTPS traffic, FTP traffic, and email message traffic (IMAP, POP3, and SMTP combined).

**Archive to FortiAnalyzer**
Select one from the following three options:

- **None**: No archiving.
- **Summary**: Archiving content meta-information to a FortiAnalyzer unit for each protocol. Content meta-information can include date and time, source and destination information, request and response size, and scan result. Content archive is only available if FortiAnalyzer is enabled under Log&Report > Log Config > Log Setting.
- **Full**: Archiving copies of downloaded files for HTTP and FTP, or copies of all email messages for IMAP, POP3, and SMTP.

**Archive SPAMed emails to FortiAnalyzer**
Enable to save spam email messages together with normal email messages. By default, spam email messages are not archived.

**Display content meta-information on the system dashboard (AIM, ICQ, MSN, Yahoo)**
Enable to have meta-information for each type of traffic display in the Statistics section of the FortiGate status page.

**Archive IM to FortiAnalyzer (AIM, ICQ, MSN, Yahoo)**
Select one from the following three options:

- **None**: No archiving.
- **Summary**: Logging summary information for IM protocols: AIM, ICQ, MSN, and Yahoo. Summary information can include date and time, source and destination information, request and response size, and scan result.
- **Full**: Archiving full chat information for IM protocols to a FortiAnalyzer unit for each protocol. Content archive is only available if FortiAnalyzer is enabled under Log&Report > Log Config > Log Setting.

Note: You must enable IM options in the IM & P2P section of the protection profile for content archiving to function.

### IM and P2P options

**Figure 219: Protection profile IM and P2P options**

<table>
<thead>
<tr>
<th>IM / P2P</th>
<th>AIM</th>
<th>ICQ</th>
<th>MSN</th>
<th>Yahoo</th>
<th>SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block IM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block IRC chat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Audio</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block HTTP Referer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block GIF/Flash</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block JavaScript</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block User Agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following options are available for IM and P2P through the protection profile.
Changes to IM protection profile options, while IM users are logged in, will take effect only upon their next login. Enabling Block Login, for example, cannot be used to disconnect currently logged in users.

See "IM, P2P & VoIP" on page 459 for more IM configuration options.

**VoIP options**

The FortiGate unit supports rate limiting for SIP (including SIMPLE) and SCCP protocols.

**Figure 220: Protection profile VoIP options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Login</td>
<td>Enable to prevent instant message users from logging in to AIM, ICQ, MSN, Yahoo, and SIMPLE services.</td>
</tr>
<tr>
<td>Block File Transfers</td>
<td>Enable to block file transfers for AIM, ICQ, MSN, and Yahoo protocols.</td>
</tr>
<tr>
<td>Block Audio</td>
<td>Enable to block audio for AIM, ICQ, MSN, and Yahoo protocols.</td>
</tr>
<tr>
<td>Inspect Non-standard Port</td>
<td>Enable inspection of non-standard ports for IM traffic.</td>
</tr>
</tbody>
</table>
| Action                        | Pass, block, or rate limit P2P transfers for BitTorrent, eDonkey, Gnutella, Kazaa, and WinNY protocols. Skype transfers can be passed or blocked, but not rate limited.
| Limit (KBytes/s)              | Specify bandwidth limit for BitTorrent, eDonkey, Gnutella, Kazaa, and WinNY protocols if action is set to rate limit. |

The following options are available for VoIP through the protection profile:

**Limit RIGISTER Request**  Set a rate limit to SIP RIGISTER requests (per second).
**Limit INVITE Request**  Set a rate limit to SIP INVITE requests (per second).
**Limit Call Setup**  Set a rate limit to SCCP call setup (calls per minute) between call clients and the call manager.
Logging options

Figure 221: Protection profile logging options

<table>
<thead>
<tr>
<th>Logging</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td></td>
</tr>
<tr>
<td>Viruses</td>
<td></td>
</tr>
<tr>
<td>Blocked Files</td>
<td></td>
</tr>
<tr>
<td>Oversized Files / E-mails</td>
<td></td>
</tr>
<tr>
<td>Web Filtering</td>
<td></td>
</tr>
<tr>
<td>Content Block</td>
<td></td>
</tr>
<tr>
<td>URL Filter</td>
<td></td>
</tr>
<tr>
<td>ActiveX Filter</td>
<td></td>
</tr>
<tr>
<td>Cookie Filter</td>
<td></td>
</tr>
<tr>
<td>Java Applet Filter</td>
<td></td>
</tr>
<tr>
<td>FortiGuard Web Filtering</td>
<td></td>
</tr>
<tr>
<td>Rating Errors (HTTP only)</td>
<td>✔</td>
</tr>
<tr>
<td>Spam Filtering</td>
<td></td>
</tr>
<tr>
<td>Log Spam</td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td></td>
</tr>
<tr>
<td>Log Intrusions</td>
<td></td>
</tr>
<tr>
<td>IM / P2P</td>
<td></td>
</tr>
<tr>
<td>Log IM Activity</td>
<td></td>
</tr>
<tr>
<td>Log P2P Activity</td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td></td>
</tr>
<tr>
<td>Log VoIP Activity</td>
<td></td>
</tr>
</tbody>
</table>

The following options are available for logging through the protection profile:

**Antivirus**
- Viruses: Enable logging of scanned viruses.
- Blocked Files: Enable logging of blocked files.
- Oversized Files/Emails: Enable logging of oversized files and email messages.

**Web Filtering**
- Content Block: Enable logging of content blocking.
- URL Block: Enable logging of blocked and exempted URLs.
- ActiveX Filter: Enable logging of blocked Active X.
- Cookie Filter: Enable logging of blocked cookies.
- Java Applet Filter: Enable logging of blocked Java Applets.

**FortiGuard Web Filtering**
- Log rating errors (HTTP only): Enable logging of rating errors.

**Spam Filtering**
- Log Spam: Enable logging of spam detected.

**IPS**
- Log Intrusions: Enable logging of signature and anomaly intrusions.

**IM and P2P**
- Log IM Activity: Enable logging of IM activity.

**VoIP**
- Log VoIP Activity: Enable logging of VoIP activity.

For more information about logging, see “Log & Report” on page 469.
Adding a protection profile to a policy

Enable protection profiles for firewall policies with action set to allow or IPSec and with service set to ANY, HTTP, FTP, IMAP, POP3, SMTP, or a service group that includes these services.

If virtual domains are enabled on the FortiGate unit, protection profiles must be added to policies in each virtual domain. To access the policy, select a virtual domain from the main menu.

1. Go to Firewall > Policy.
2. Select a policy list to which to add a protection profile.
   For example, to enable network protection for files downloaded from the web by internal network users, select an internal to external policy list.
3. Select Create New to add a policy, or select Edit for the policy to modify.
4. Select protection profile.
5. Select a protection profile from the list.
6. Configure the remaining policy settings, if required.
7. Select OK.
8. Repeat this procedure for any policies for which to enable network protection.

Protection profile CLI configuration

Use the `config firewall profile` CLI command to add, edit or delete protection profiles. Use protection profiles to apply different protection settings for traffic controlled by firewall policies.

**Note:** For complete descriptions and examples of how to use CLI commands, see the *FortiGate CLI Reference*. 
VPN IPSEC

This section provides information about policy-based (tunnel-mode) and route-based (interface mode) Internet Protocol Security (IPSec) VPN options available through the web-based manager. FortiGate units implement the Encapsulated Security Payload (ESP) protocol. The encrypted packets look like ordinary packets that can be routed through any IP network. Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates. As an option, you can specify manual keys. Interface mode is supported in NAT/Route mode only. It creates a virtual interface for the local end of a VPN tunnel.

Note: For information about how to configure an IPSec VPN, see the FortiGate IPSec VPN User Guide.

This section describes:

• Overview of IPSec interface mode
• Auto Key
• Manual Key
• Concentrator
• Monitor

Overview of IPSec interface mode

When you define a route-based (interface mode) IPSec tunnel, a virtual IPSec interface is created automatically. This is a subinterface of the FortiGate local interface you selected in the IPSec phase 1 parameters. The local interface can be a physical, aggregate, VLAN, inter-VDOM link or wireless interface.

An IPSec virtual interface is considered to be up when it can establish a phase 1 connection with a VPN peer or client. However, the virtual IPSec interface cannot be used to send traffic through a tunnel until it is bound to a phase 2 definition.

Virtual IPSec interface bindings are shown on the System > Network > Interface page. The names of all tunnels bound to physical interfaces are displayed under their associated physical interface names in the Name column. For more information about the Interface page, see "Interface" on page 79.

Note: You can bind a virtual IPSec interface to a zone.

After an IPSec virtual interface has been bound to a tunnel, traffic can be routed to the interface using specific metrics for both static routes and policy routes. In addition, you can create a firewall policy having the virtual IPSec interface as the source or destination interface.
You can create the equivalent of a tunnel-mode concentrator in any of the following ways:

- Define a firewall policy between each pair of IPSec interfaces that you want to concentrate. For dialup, the same interface can be both source and destination. This can become tedious if you have many site-to-site connections.
- Put all the IPSec interfaces into a zone and then define a single zone-to-zone policy.
- Put all the IPSec interfaces in a zone and enable intra-zone traffic. There must be more than one IPSec interface.

For more information and an example, see the FortiGate IPSec VPN User Guide.

When IP traffic that originates from behind a local FortiGate unit reaches an outbound FortiGate interface that acts as the local end of an IPSec tunnel (that is, IPSec interface mode is enabled on the interface), the tunnel encapsulates the traffic and forwards it through the physical interface to which the IPSec virtual interface is bound. When encapsulated traffic from a remote VPN peer or client reaches a local FortiGate physical interface, the FortiGate unit determines if an IPSec virtual interface is associated with the physical interface through selectors in the traffic. If the traffic matches predefined selectors, it is decapsulated and forwarded to the IPSec virtual interface.

In the outbound direction, the FortiGate unit performs a route lookup to find the interface through which it must forward traffic to reach the next hop router. If the FortiGate unit finds a route through a virtual interface that is bound to a specific VPN tunnel, the traffic is encrypted and sent through the VPN tunnel. In the inbound direction, the FortiGate unit identifies a VPN tunnel using the destination IP address and the Security Parameter Index (SPI) in the ESP datagram to match a phase 2 Security Association (SA). If a matching SA is found, the datagram is decrypted and the associated IP traffic is redirected through the IPSec virtual interface.

The firewall policy associated with a specific path is responsible for controlling all IP traffic passing between the source and destination addresses. If required, you can configure more than one firewall policy to regulate the flow of traffic going into and/or emerging from a route-based VPN tunnel. Two firewall policies are needed to support bidirectional traffic through a route-based IPSec tunnel: one to control traffic in the outbound direction, and the other to control traffic in the inbound direction.

Route-based VPNs help to simplify the implementation of VPN tunnel redundancy. You can configure a route for the same IP traffic using different route metrics. You can also configure the exchange of dynamic (RIP, OSPF, or BGP) routing information through VPN tunnels. If the primary VPN connection fails or the priority of a route changes through dynamic routing, an alternative route will be selected to forward traffic using the redundant connection.

A simple way to provide failover redundancy is to create a backup IPSec interface. You can do this in the CLI. Refer to the FortiGate CLI Reference. See the monitor-phase1 keyword of the ipsec vpn phase1-interface command. An example configuration is provided.
Auto Key

Two VPN peers (or a FortiGate dialup server and a VPN client) can be configured to generate unique Internet Key Exchange (IKE) keys automatically during the IPSec phase 1 and phase 2 exchanges.

To configure the FortiGate unit to generate unique keys automatically in phase 1 and phase 2, go to VPN > IPSEC > Auto Key (IKE).

When you define phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection for the tunnel and authenticate the remote peer.

Auto Key configuration applies to both tunnel-mode and interface-mode VPNs.

Figure 222: Auto Key list

<table>
<thead>
<tr>
<th>Create Phase 1</th>
<th>Create Phase 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>Phase 2</td>
</tr>
<tr>
<td>Dialup_group</td>
<td>Tunnel Mode</td>
</tr>
<tr>
<td></td>
<td>Port1</td>
</tr>
<tr>
<td>Static2</td>
<td>Interface Mode</td>
</tr>
<tr>
<td></td>
<td>Port1</td>
</tr>
</tbody>
</table>

Create Phase 1: Create a new phase 1 tunnel configuration. See “Creating a new phase 1 configuration” on page 345.

Create Phase 2: Create a new phase 2 configuration. See “Creating a new phase 2 configuration” on page 350.

Phase 1: The names of existing phase 1 tunnel configurations.

Phase 2: The names of existing phase 2 configurations.

Interface Binding: The names of the local interfaces to which IPSec tunnels are bound. These can be physical, aggregate, VLAN, inter-VDOM link or wireless interfaces.

Delete and Edit icons: Delete or edit a phase 1 configuration.

Creating a new phase 1 configuration

In phase 1, two VPN peers (or a FortiGate dialup server and a VPN client) authenticate each other and exchange keys to establish a secure communication channel between them. The basic phase 1 settings associate IPSec phase 1 parameters with a remote gateway and determine:

- whether the various phase 1 parameters will be exchanged in multiple rounds with encrypted authentication information (main mode) or in a single message with authentication information that is not encrypted (aggressive mode)
- whether a pre-shared key or digital certificates will be used to authenticate the identities of the two VPN peers (or a VPN server and its client)
- whether a special identifier, certificate distinguished name, or group name will be used to identify the remote VPN peer or client when a connection attempt is made
To define basic IPSec phase 1 parameters, go to **VPN > IPSEC > Auto Key (IKE)** and select Create Phase 1. For information about how to choose the correct phase 1 settings for your particular situation, see the FortiGate IPSec VPN User Guide.

**Figure 223: New Phase 1**

| Name | Type a name to represent the phase 1 definition. The maximum name length is 15 characters for an interface mode VPN, 35 characters for a policy-based VPN. If Remote Gateway is Dialup User, the maximum name length is further reduced depending on the number of dialup tunnels that can be established: by 2 for up to 9 tunnels, by 3 for up to 99 tunnels, 4 for up to 999 tunnels, and so on. For a tunnel mode VPN, the name should reflect the origination of the remote connection. For a route-based tunnel, the FortiGate unit also uses the name for the virtual IPSec interface that it creates automatically. |
| Remote Gateway | Select the nature of the remote connection:  
  - If the remote peer has a static IP address, select Static IP Address.  
  - If one or more FortiClient™ or FortiGate dialup clients with dynamic IP addresses will connect to the FortiGate unit, select Dialup User.  
  - If a remote peer that has a domain name and subscribes to a dynamic DNS service will be connecting to the FortiGate unit, select Dynamic DNS. |
| IP Address | If Static IP Address is selected, type the IP address of the remote peer. |
| Dynamic DNS | If Dynamic DNS is selected, type the domain name of the remote peer. |
| Local Interface | This option is available in NAT/Route mode only. Select the name of the interface through which remote peers or dialup clients connect to the FortiGate unit. The FortiGate unit obtains the IP address of the interface from **System > Network > Interface** settings (see "Interface" on page 79) unless you are configuring an IPSec interface, in which case you can specify a different IP address in the Local Gateway IP field under Advanced settings (see "Local Gateway IP" on page 349). |
Mode

Select Main or Aggressive:

- In Main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.

- In Aggressive mode, the phase 1 parameters are exchanged in single message with authentication information that is not encrypted.

When the remote VPN peer has a dynamic IP address and is authenticated by a pre-shared key, you must select aggressive mode if there is more than one dialup phase1 configuration for the interface IP address.

When the remote VPN peer has a dynamic IP address and is authenticated by a certificate, you must select aggressive mode if there is more than one phase 1 configuration for the interface IP address and these phase 1 configurations use different proposals. Peer Options settings may require a particular mode. See Peer Options, below.

Authentication Method

Select Preshared Key or RSA Signature.

Pre-shared Key

If Pre-shared Key is selected, type the pre-shared key that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. You must define the same value at the remote peer or client. The key must contain at least 6 printable characters and should only be known by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

Certificate Name

If RSA Signature is selected, select the name of the server certificate that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. To obtain and load the required server certificate, see the FortiGate Certificate Management User Guide.

Peer Options

One or more of the following options are available to authenticate VPN peers or clients, depending on the Remote Gateway and Authentication Method settings.

Accept any peer ID

Accept the local ID of any remote VPN peer or client. The FortiGate unit does not check identifiers (local IDs). Mode can be set to Aggressive or Main.

You can use this option with RSA Signature authentication. But, for highest security, you should configure a PKI user/group for the peer and set Peer Options to Accept this peer certificate only.

Accept this peer ID

Authenticate remote peers based on a particular identifier. Enter the identifier in the field. The remote peer must be configured with the same identifier. This option is available only if the remote peer has a dynamic IP address.

If the remote peer is a FortiGate unit, the identifier must be specified in the Local ID field of the phase 1 configuration. For FortiClient dialup clients, select Config in the Policy section of the Advanced Settings for the connection and specify the identifier in the Local ID field.

Accept peer ID in dialup group

Authenticate multiple FortiGate or FortiClient dialup clients that use unique identifiers and unique pre-shared keys (or unique pre-shared keys only) through the same VPN tunnel.

You must create a dialup user group for authentication purposes. See “User groups” on page 386. Select the group from the list adjacent to the Accept peer ID in dialup group option.

To configure FortiGate dialup clients, refer to the FortiGate IPSec VPN User Guide. To configure FortiClient dialup clients, refer to the Authenticating FortiClient Dialup Clients Technical Note.

Mode must be set to Aggressive when the dialup clients use unique identifiers and unique pre-shared keys. If the dialup clients use unique pre-shared keys only, you can set Mode to Main if there is only one dialup phase 1 configuration for this interface IP address.
Auto Key

Defining phase 1 advanced settings

The advanced P1 Proposal parameters select the encryption and authentication algorithms that the FortiGate unit uses to generate keys for the IKE exchange. Additional advanced phase 1 settings can be selected to ensure the smooth operation of phase 1 negotiations.

To modify IPSec phase 1 advanced parameters, go to VPN > IPSEC > Auto Key (IKE), select Create Phase 1, and then select Advanced. For information about how to choose the correct advanced phase 1 settings for your particular situation, see the FortiGate IPSec VPN User Guide.

Figure 224: Phase 1 advanced settings

<table>
<thead>
<tr>
<th>Advanced...</th>
<th>(XAUTH, Nat Traversal, DPD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IPSec Interface Mode</td>
<td></td>
</tr>
<tr>
<td>Local Gateway IP</td>
<td>□ Main Interface IP □ Specify 0.0.0.0</td>
</tr>
<tr>
<td>P1 Proposal</td>
<td>1 - Encryption □ 3DES □ Authentication □ SHA1 □ 2 - Encryption □ 3DES □ Authentication □ MD5 □</td>
</tr>
<tr>
<td>DH Group</td>
<td>□ 1 □ 2 □ 3</td>
</tr>
<tr>
<td>Keylife</td>
<td>28800 (120-172800 seconds)</td>
</tr>
<tr>
<td>Local ID</td>
<td>(optional)</td>
</tr>
<tr>
<td>XAuth</td>
<td>□ Enable as Client □ Enable as Server</td>
</tr>
<tr>
<td>Nat traversal</td>
<td>□ Enable</td>
</tr>
<tr>
<td>Keepalive Frequency</td>
<td>□ 0-900 seconds</td>
</tr>
<tr>
<td>Dead Peer Detection</td>
<td>□ Enable</td>
</tr>
</tbody>
</table>
**Enable IPSec Interface Mode**
Create a virtual interface for the local end of the VPN tunnel. This is not available in Transparent mode.

**Local Gateway IP**
If you selected Enable IPSec Interface Mode, you need to specify an IP address for the local end of the VPN tunnel. Select one of the following:

- **Main Interface IP** - the FortiGate unit obtains the IP address of the interface from System > Network > Interface settings (see "Interface" on page 79)
- **Specify** - specify an IP address. The IP address is assigned to the interface selected in the phase 1 Local Interface field (see "Local Interface" on page 346).

You cannot configure Interface mode in a Transparent mode VDOM.

**P1 Proposal**
Select the encryption and authentication algorithms used to generate keys for protecting negotiations. Add or delete encryption and authentication algorithms as required. Select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define.

You can select any of the following symmetric-key algorithms:

- DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES-Triple-DES, in which plain text is encrypted three times by three keys.
- AES128-A 128-bit block algorithm that uses a 128-bit key.
- AES192-A 128-bit block algorithm that uses a 192-bit key.
- AES256-A 128-bit block algorithm that uses a 256-bit key.

You can select either of the following message digests to check the authenticity of messages during phase 1 negotiations:

- MD5-Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.

To specify a third combination, use the Add button beside the fields for the second combination.

**DH Group**
Select one or more Diffie-Hellman groups from DH group 1, 2, and 5. When using aggressive mode, DH groups cannot be negotiated.

- If both VPN peers (or a VPN server and its client) have static IP addresses and use aggressive mode, select a single DH group. The setting on the FortiGate unit must be identical to the setting on the remote peer or dialup client.
- When the remote VPN peer or client has a dynamic IP address and uses aggressive mode, select up to three DH groups on the FortiGate unit and one DH group on the remote peer or dialup client. The setting on the remote peer or client must be identical to one of the selections on the FortiGate unit.
- If the VPN peer or client employs main mode, you can select multiple DH groups. At least one of the settings on the remote peer or client must be identical to the selections on the FortiGate unit.

**Keylife**
Type the length of time (in seconds) until the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172800 seconds.
Auto Key VPN IPSEC

Creating a new phase 2 configuration

After IPSec phase 1 negotiations complete successfully, phase 2 begins. The phase 2 parameters define the algorithms that the FortiGate unit may use to encrypt and transfer data for the remainder of the session. During phase 2, the specific IPSec security associations needed to implement security services are selected and a tunnel is established.

The basic phase 2 settings associate IPSec phase 2 parameters with the phase 1 configuration that specifies the remote end point of the VPN tunnel. In most cases, you need to configure only basic phase 2 settings.

To configure phase 2 settings, go to VPN > IPSEC > Auto Key (IKE) and select Create Phase 2. For information about how to choose the correct phase 2 settings for your particular situation, see the FortiGate IPSec VPN User Guide.
In phase 2, the FortiGate unit and the VPN peer or client exchange keys again to establish a secure communication channel between them. The P2 Proposal parameters select the encryption and authentication algorithms needed to generate keys for protecting the implementation details of Security Associations (SAs). The keys are generated automatically using a Diffie-Hellman algorithm.

A number of additional advanced phase 2 settings are available to enhance the operation of the tunnel. To modify IPSec phase 2 advanced parameters, go to **VPN > IPSEC Auto Key (IKE)**, select Create Phase 2, and then select Advanced. For information about how to choose the correct advanced phase 2 settings for your particular situation, see the *FortiGate IPSec VPN User Guide*.

---

**Figure 225: New Phase 2**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type a name to identify the phase 2 configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>Select the phase 1 tunnel configuration. See &quot;Creating a new phase 1 configuration&quot; on page 345. The phase 1 configuration describes how remote VPN peers or clients will be authenticated on this tunnel, and how the connection to the remote peer or client will be secured.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Define advanced phase 2 parameters. See &quot;Defining phase 2 advanced settings&quot; on page 351.</td>
</tr>
</tbody>
</table>

**Defining phase 2 advanced settings**

In phase 2, the FortiGate unit and the VPN peer or client exchange keys again to establish a secure communication channel between them. The P2 Proposal parameters select the encryption and authentication algorithms needed to generate keys for protecting the implementation details of Security Associations (SAs). The keys are generated automatically using a Diffie-Hellman algorithm.

A number of additional advanced phase 2 settings are available to enhance the operation of the tunnel. To modify IPSec phase 2 advanced parameters, go to **VPN > IPSEC Auto Key (IKE)**, select Create Phase 2, and then select Advanced. For information about how to choose the correct advanced phase 2 settings for your particular situation, see the *FortiGate IPSec VPN User Guide*.

**Figure 226: Phase 2 advanced settings**

<table>
<thead>
<tr>
<th>P2 Proposal</th>
<th>Encryption: 3DES</th>
<th>Authentication: SHA1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keylife:</td>
<td>Seconds 1600</td>
<td>(Seconds) 600000</td>
</tr>
<tr>
<td>Autokey Keep Alive</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>Quick Mode Selector</td>
<td>Source address</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>
P2 Proposal

Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to three proposals. To establish a VPN connection, the remote peer must be configured to use at least one of the proposals that you specify. Initially there are two proposals. To specify only one proposal, use the minus button to remove the second proposal. To specify a third proposal, use the plus button beside the second proposal.

It is invalid to set both Encryption and Authentication to NULL.

Encryption

You can select any of the following symmetric-key algorithms:

- NULL-Do not use an encryption algorithm.
- DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES-Triple-DES, in which plain text is encrypted three times by three keys.
- AES128-A 128-bit block algorithm that uses a 128-bit key.
- AES192-A 128-bit block algorithm that uses a 192-bit key.
- AES256-A 128-bit block algorithm that uses a 256-bit key.

Authentication

You can select either of the following message digests to check the authenticity of messages during an encrypted session:

- NULL-Do not use a message digest.
- MD5-Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.

Enable replay detection

Optionally enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPSec packets and replays them back into the tunnel.

Enable perfect forward secrecy (PFS)

Enable or disable PFS. Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.

DH Group

Select one Diffie-Hellman group (1, 2, or 5). The remote peer or dialup client must be configured to use the same group.

Keylife

Select the method for determining when the phase 2 key expires: Seconds, KBytes, or Both. If you select both, the key expires when either the time has passed or the number of KB have been processed. The range is from 120 to 172800 seconds, or from 5120 to 2147483648 KB.

Autokey Keep Alive

Enable the option if you want the tunnel to remain active when no data is being processed.

DHCP-IPSec

Select Enable if the FortiGate unit acts as a dialup server and FortiGate DHCP relay will be used to assign VIP addresses to FortiClient dialup clients. The DHCP relay parameters must be configured separately. For more information, see “System DHCP” on page 129.

If the FortiGate unit acts as a dialup server and you manually assigned FortiClient dialup clients VIP addresses that match the network behind the dialup server, select Enable to cause the FortiGate unit to act as a proxy for the dialup clients.

This is available only for tunnel mode phase 2 configurations associated with a dialup phase 1 configuration.

Note: You can enable VPN users to browse the Internet through the FortiGate unit. See “Internet browsing configuration” on page 353.
You can enable VPN users to browse the Internet through the FortiGate unit. You do this with firewall policies. The required policies are different for policy-based and route-based VPNs. For more information about firewall policies, see “Configuring firewall policies” on page 271.

**Policy-based VPN Internet browsing configuration**

Configure an additional firewall policy as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Interface/Zone</td>
<td>Select the FortiGate unit public interface.</td>
</tr>
<tr>
<td>Source Address Name</td>
<td>Select All</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Select the FortiGate unit public interface.</td>
</tr>
<tr>
<td>Destination Address Name</td>
<td>Select the remote network address name.</td>
</tr>
<tr>
<td>Action</td>
<td>Select IPSEC.</td>
</tr>
</tbody>
</table>
Manual Key

If required, you can manually define cryptographic keys for establishing an IPSec VPN tunnel. You would define manual keys in situations where:

- Prior knowledge of the encryption and/or authentication key is required (that is, one of the VPN peers requires a specific IPSec encryption and/or authentication key).
- Encryption and authentication needs to be disabled.

In both cases, you do not specify IPSec phase 1 and phase 2 parameters; you define manual keys on the VPN > IPSEC > Manual Key page instead.

Note: It may not be safe or practical to define manual keys because network administrators must be trusted to keep the keys confidential, and propagating changes to remote VPN peers in a secure manner may be difficult.

For general information about how to configure an IPSec VPN, see the FortiGate IPSec VPN User Guide.

Figure 227: Manual Key list

Create New

Create a new manual key configuration. See “Creating a new manual key configuration” on page 355.

Tunnel Name

The names of existing manual key configurations.

Remote Gateway

The IP addresses of remote peers or dialup clients.
Creating a new manual key configuration

If one of the VPN devices uses specific authentication and/or encryption keys to establish a tunnel, both VPN devices must be configured to use identical authentication and/or encryption keys. In addition, it is essential that both VPN devices be configured with complementary Security Parameter Index (SPI) settings.

Each SPI identifies a Security Association (SA). The value is placed in ESP datagrams to link the datagrams to the SA. When an ESP datagram is received, the recipient refers to the SPI to determine which SA applies to the datagram. An SPI must be specified manually for each SA. Because an SA applies to communication in one direction only, you must specify two SPIs per configuration (a local SPI and a remote SPI) to cover bidirectional communications between two VPN devices.

Caution: If you are not familiar with the security policies, SAs, selectors, and SA databases for your particular installation, do not attempt the following procedure without qualified assistance.

To specify manual keys for creating a tunnel, go to VPN > IPSEC > Manual Key and select Create New.

Figure 228: New Manual Key

<table>
<thead>
<tr>
<th>Name</th>
<th>Ska3_to_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local SPI</td>
<td>1234++ (Hex)</td>
</tr>
<tr>
<td>Remote SPI</td>
<td>953bba (Hex)</td>
</tr>
<tr>
<td>Remote Gateway</td>
<td>10.30.40.1</td>
</tr>
<tr>
<td>Local Interface</td>
<td>port1</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>3DES</td>
</tr>
<tr>
<td>Encryption Key (Hex)</td>
<td>3232323232323232</td>
</tr>
<tr>
<td>Authentication Algorithm</td>
<td>SHA1</td>
</tr>
<tr>
<td>Authentication Key (Hex)</td>
<td>SHA1SHA1SHA1SHA1SHA1SHA1</td>
</tr>
<tr>
<td>IPSEC Interface Mode</td>
<td></td>
</tr>
</tbody>
</table>

Name
Type a name for the VPN tunnel. The maximum name length is 15 characters for an interface mode VPN, 35 characters for a policy-based VPN.

Local SPI
Type a hexadecimal number (up to 8 characters, 0-9, a-f) that represents the SA that handles outbound traffic on the local FortiGate unit. The valid range is from 0x100 to 0x0fffffff. This value must match the Remote SPI value in the manual key configuration at the remote peer.
### Remote SPI
Type a hexadecimal number (up to 8 characters, 0-9, a-f) that represents the SA that handles inbound traffic on the local FortiGate unit. The valid range is from `0x100` to `0xffffffff`. This value must match the Local SPI value in the manual key configuration at the remote peer.

### Remote Gateway
Type the IP address of the public interface to the remote peer. The address identifies the recipient of ESP datagrams.

### Local Interface
This option is available in NAT/Route mode only. Select the name of the interface to which the IPSec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from `System > Network > Interface` settings (see "Interface" on page 79).

### Encryption Algorithm
Select one of the following symmetric-key encryption algorithms:
- **DES**-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- **3DES**-Triple-DES, in which plain text is encrypted three times by three keys.
- **AES128**-A 128-bit block algorithm that uses a 128-bit key.
- **AES192**-A 128-bit block algorithm that uses a 192-bit key.
- **AES256**-A 128-bit block algorithm that uses a 256-bit key.

**Note:** The algorithms for encryption and authentication cannot both be NULL.

#### Encryption Key
If you selected:
- **DES**, type a 16-character hexadecimal number (0-9, a-f).
- **3DES**, type a 48-character hexadecimal number (0-9, a-f) separated into three segments of 16 characters.
- **AES128**, type a 32-character hexadecimal number (0-9, a-f) separated into two segments of 16 characters.
- **AES192**, type a 48-character hexadecimal number (0-9, a-f) separated into three segments of 16 characters.
- **AES256**, type a 64-character hexadecimal number (0-9, a-f) separated into four segments of 16 characters.

### Authentication Algorithm
Select one of the following message digests:
- **MD5**-Message Digest 5 algorithm, which produces a 128-bit message digest.
- **SHA1**-Secure Hash Algorithm 1, which produces a 160-bit message digest.

**Note:** The Algorithms for encryption and authentication cannot both be NULL.

#### Authentication Key
If you selected:
- **MD5**, type a 32-character hexadecimal number (0-9, a-f) separated into two segments of 16 characters.
- **SHA1**, type 40-character hexadecimal number (0-9, a-f) separated into one segment of 16 characters and a second segment of 24 characters.

### IPSec Interface Mode
Create a virtual interface for the local end of the VPN tunnel. This command is available only in NAT/Route mode.
Concentrator

In a hub-and-spoke configuration, policy-based VPN connections to a number of remote peers radiate from a single, central FortiGate unit. Site-to-site connections between the remote peers do not exist; however, VPN tunnels between any two of the remote peers can be established through the FortiGate unit “hub”.

In a hub-and-spoke network, all VPN tunnels terminate at the hub. The peers that connect to the hub are known as “spokes”. The hub functions as a concentrator on the network, managing all VPN connections between the spokes. VPN traffic passes from one tunnel to the other through the hub.

You define a concentrator to include spokes in the hub-and-spoke configuration.

To define a concentrator, go to **VPN > IPSEC > Concentrator**. For detailed information and step-by-step procedures about how to set up a hub-and-spoke configuration, see the *FortiGate IPSec VPN User Guide*.

Figure 229: Concentrator list

<table>
<thead>
<tr>
<th>Concentrator Name</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concentrator_1</td>
<td>Start_to_Site2_Tunnel, Dualhop_group</td>
</tr>
<tr>
<td>Concentrator_2</td>
<td>Fo_Site2, TechDoc_users</td>
</tr>
</tbody>
</table>

Create New       Define a new concentrator for an IPSec hub-and-spoke configuration. See “Defining concentrator options” on page 357.

Concentrator Name The names of existing IPSec VPN concentrators.

Members          The tunnels that are associated with the concentrators.

Delete and Edit icons Delete or edit a concentrator.

Defining concentrator options

A concentrator configuration specifies which spokes to include in an IPSec hub-and-spoke configuration.

To specify the spokes of an IPSec hub-and-spoke configuration, go to **VPN > IPSEC > Concentrator** and select Create New.

Figure 230: New VPN Concentrator
Monitor

You can use the monitor to view activity on IPSec VPN tunnels and start or stop those tunnels. The display provides a list of addresses, proxy IDs, and timeout information for all active tunnels, including tunnel mode and route-based (interface mode) tunnels.

You can use filters control the information displayed in the list. See "Adding filters to web-based manager lists" on page 43.

To view active tunnels, go to **VPN > IPSEC > Monitor**.

![Monitor list](image)

- **Type**: Select the types of VPN to display: All, Dialup, or Static IP and Dynamic DNS.
- **Clear All Filters**: Select to clear any column display filters you might have applied.
- **Page controls**: Display the first, previous, next or last page of monitored VPNs.
- **Name**: The name of the phase 1 configuration for the VPN.
- **Remote Gateway**: The public IP address of the remote host device, or if a NAT device exists in front of the remote host, the public IP address of the NAT device.
- **Remote Port**: The UDP port of the remote host device, or if a NAT device exists in front of the remote host, the UDP port of the NAT device. Zero (0) indicates that any port can be used.
- **Proxy ID Source**: The IP addresses of the hosts, servers, or private networks behind the FortiGate unit. A network range may be displayed if the source address in the firewall encryption policy was expressed as a range of IP addresses.
For Dialup VPNs, the list provides status information about the VPN tunnels established by dialup clients, including the IP addresses of the dialup clients. The number of tunnels shown in the list can change as dialup clients connect and disconnect.

For Static IP and dynamic DNS VPNs, the list provides status and IP addressing information about VPN tunnels, active or not, to remote peers that have static IP addresses or domain names. You can also start and stop individual tunnels from the list.

**Proxy ID Destination**

When a FortiClient dialup client establishes a tunnel:

- If VIP addresses are not used, the Proxy ID Destination field displays the public IP address of the remote host Network Interface Card (NIC).

- If VIP addresses were configured (manually or through FortiGate DHCP relay), the Proxy ID Destination field displays either the VIP address belonging to the FortiClient dialup client, or the subnet address from which VIP addresses were assigned.

When a FortiGate dialup client establishes a tunnel, the Proxy ID Destination field displays the IP address of the remote private network.

**Tunnel up or tunnel down icon**

A green arrow pointing up means the tunnel is currently processing traffic. Select to bring down tunnel.

A red arrow pointing down means the tunnel is not processing traffic. Select to bring up tunnel.
VPN PPTP

FortiGate units support PPTP to tunnel PPP traffic between two VPN peers. Windows or Linux PPTP clients can establish a PPTP tunnel with a FortiGate unit that has been configured to act as a PPTP server. As an alternative, you can configure the FortiGate unit to forward PPTP packets to a PPTP server on the network behind the FortiGate unit.

PPTP VPN is available only in NAT/Route mode. The current maximum number of PPTP and L2TP sessions is 254. The start and end IPs must be in the same 24-bit subnet, e.g. x.x.x.1 - x.x.x.254.

This section explains how to use the web-based manager to specify a range of IP addresses for PPTP clients. For information about how to perform other related PPTP VPN setup tasks, see the FortiGate PPTP VPN User Guide.

This section describes:
- PPTP Range

PPTP Range

You can specify a PPTP address range on the PPTP Range page. The PPTP address range is the range of addresses reserved for remote PPTP clients. When the remote PPTP client connects, the FortiGate unit assigns an IP address from a reserved range of IP addresses to the client PPTP interface. The PPTP client uses the assigned IP address as its source address for the duration of the connection.

To enable PPTP and specify the PPTP address range, go to VPN > PPTP > PPTP Range, select the required options, and then select Apply.

Figure 232: Edit PPTP range

| Enable PPTP | Select the option. You must add a user group before you can select the option. See “User groups” on page 386.
| Starting IP | Type the starting address in the range of reserved IP addresses.
| Ending IP | Type the ending address in the range of reserved IP addresses.
| User Group | Select the name of the PPTP user group that you defined.
| Disable PPTP | Select the option to disable PPTP support.
VPN SSL

This section provides information about the features of the **VPN > SSL** page in the web-based manager. The SSL VPN feature is supported on FortiGate units that run in NAT/Route mode only.

![Note:](image)

For detailed instructions about how to configure web-only mode or tunnel mode operation, see the *FortiGate SSL VPN User Guide*.

This section describes:

- Configuring SSL VPN
- Monitoring SSL VPN sessions
- SSL VPN bookmarks
- Viewing the SSL VPN bookmark list
- Configuring SSL VPN bookmarks
- Viewing the SSL VPN Bookmark Groups list
- Configuring SSL VPN bookmark groups

### Configuring SSL VPN

The Config page contains basic SSL VPN settings including timeout values and SSL encryption preferences. If required, you can also enable the use of digital certificates for authenticating remote clients.

![Note:](image)

If required, you can enable SSL version 2 encryption (for compatibility with older browsers) through a FortiGate CLI command. For more information, see “ssl settings” in the “vpn” chapter of the *FortiGate CLI Reference*.

Go to **VPN > SSL > Config** to enable SSL VPN and make configuration selections.
Figure 233: SSL-VPN Settings

<table>
<thead>
<tr>
<th>SSL-VPN Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable SSL-VPN</strong></td>
</tr>
<tr>
<td><strong>Login Port</strong></td>
</tr>
<tr>
<td><strong>Tunnel IP Range</strong></td>
</tr>
<tr>
<td><strong>Server Certificate</strong></td>
</tr>
<tr>
<td><strong>Require Client Certificate</strong></td>
</tr>
<tr>
<td><strong>Encryption Key Algorithm</strong></td>
</tr>
<tr>
<td><strong>Idle Timeout</strong></td>
</tr>
</tbody>
</table>

### Advanced (DNS and WINS Servers)
- DNS Server #1
- DNS Server #2
- WINS Server #1
- WINS Server #2

---

**Enable SSL VPN**
- Select to enable SSL VPN connections.

**Login Port**
- Optionally enter a different HTTPS port number for remote client web browsers to connect to the FortiGate unit. The default port number is 10443.

**Tunnel IP Range**
- Specify the range of IP addresses reserved for tunnel-mode SSL VPN clients. Type the starting and ending address that defines the range of reserved IP addresses.

**Server Certificate**
- Select the signed server certificate to use for authentication purposes. If you leave the default setting (Self-Signed), the FortiGate unit offers its factory installed (self-signed) certificate from Fortinet to remote clients when they connect.

**Require Client Certificate**
- If you want to enable the use of group certificates for authenticating remote clients, select the option. Afterward, when the remote client initiates a connection, the FortiGate unit prompts the client for its client-side certificate as part of the authentication process.

**Encryption Key Algorithm**
- Select the algorithm for creating a secure SSL connection between the remote client web browser and the FortiGate unit.
  - **Default - RC4(128 bits) and higher**
    - If the web browser on the remote client is capable of matching a 128-bit or greater cipher suite, select this option.
  - **High - AES(128/256 bits) and 3DES**
    - If the web browser on the remote client is capable of matching a high level of SSL encryption, select this option to enable cipher suites that use more than 128 bits to encrypt data.
  - **Low - RC4(64 bits), DES and higher**
    - If you are not sure which level of SSL encryption the remote client web browser supports, select this option to enable a 64-bit or greater cipher suite.
Monitoring SSL VPN sessions

You can display a list of all active SSL VPN sessions. The list displays the user name of the remote user, the IP address of the remote client, and the time that the connection was made. The list also identifies which services are being provided, and allows you to delete an active web session from the FortiGate unit.

Go to VPN > SSL > Monitor to view the list of active SSL VPN sessions.

<table>
<thead>
<tr>
<th>No.</th>
<th>User</th>
<th>Source IP</th>
<th>Begin Time</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SSL</td>
<td>172.20.10.41</td>
<td>Tue Feb 4 06:10:10 2007</td>
<td>Tunnel IP 10.200.200.0</td>
<td>Delete</td>
</tr>
</tbody>
</table>

**SSL VPN bookmarks**

If you create a user account that permits web-only mode access, you can create hyperlinks to frequently accessed server applications that the user can use to start any session from the home page through the hyperlinks. The FortiGate unit forwards client requests to servers on the Internet or internal network. To use the web-portal applications, you add the URL, IP address, or name of the server application to the Bookmarks list. The bookmarks are available when the user starts an active SSL VPN session.
Viewing the SSL VPN bookmark list

You can display a list of all existing SSL VPN bookmarks created using the FortiGate unit. The list details the name of the bookmark, type of bookmark, and the link details.

To view the list of predefined SSL VPN bookmarks, go to **VPN > SSL > Bookmark**.

**Figure 235: Bookmark list**

<table>
<thead>
<tr>
<th>Bookmark Name</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td><a href="http://www.fortinet.com">http://www.fortinet.com</a></td>
</tr>
<tr>
<td>Telnet</td>
<td>telnet://198.168.5.238</td>
</tr>
</tbody>
</table>

**Bookmark Name**  The type/names of links to remote server applications and network services.

**Link**  The URL, host, or folder of the bookmark link.

Delete and Edit icons  Delete or edit an entry in the list.

Configuring SSL VPN bookmarks

Go to **VPN > SSL > Bookmark** and select Create New to create hyperlinks to frequently accessed server applications.

**Figure 236: Create New Bookmark**

![Create New Bookmark](image)

**Bookmark Name**  Type the text to display in the hyperlink. The name is displayed in the Bookmarks list.
Viewing the SSL VPN Bookmark Groups list

You can create a group of specific bookmarks that can be included in the configuration of an SSL VPN user group.

To view a list of bookmark groups, go to VPN > SSL > Bookmark Group.

Figure 237: Bookmark Group list

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Bookmarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Group1</td>
<td>Telnet, bookmark, WebHome</td>
</tr>
<tr>
<td>WebOnly</td>
<td>WebHome</td>
</tr>
</tbody>
</table>

**Group Name**  
Name of bookmark group

**Bookmarks**  
List of bookmarks that are available to the group of users defined in Group Name.

**Delete and Edit Icons**  
Delete or edit an entry in the list.
Configuring SSL VPN bookmark groups

Go to VPN > SSL > Bookmark Group and select Create New to create a group of selected bookmarks.

**Figure 238: Create New Bookmark Group**

<table>
<thead>
<tr>
<th>New Bookmark Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
</tbody>
</table>

**Available Bookmarks**
- FTP
- RDP
- SMB
- Telnet
- Telnet Bookmark (193.160.5.230)
- VNC
- Web
- WebHome (www.fortinet.com)

**Used Bookmarks**
- FTP
- RDP
- SMB
- Telnet
- VNC
- Web

<table>
<thead>
<tr>
<th><img src="image1" alt="Available Bookmarks" /></th>
<th><img src="image2" alt="Used Bookmarks" /></th>
</tr>
</thead>
</table>

**Right arrow button**
Add a bookmark to the Used Bookmarks list. Select a user or server name in the Available Bookmarks list and select the right arrow button to move it to the Used Bookmarks list.

**Left arrow button**
Remove a bookmark from the Used Bookmarks list. Select a bookmark in the Used Bookmarks list and select the left arrow button to move it to the Available Bookmarks list.

**Create New...**
Select to create a new bookmark for inclusion in the Available Bookmarks list.
VPN Certificates

This section explains how to manage X.509 security certificates using the FortiGate web-based manager. Refer to this module to generate certificate requests, install signed certificates, import CA root certificates and certificate revocation lists, and back up and restore installed certificates and private keys. For additional background information, see the FortiGate Certificate Management User Guide.

This section describes:
- Local Certificates
- Remote Certificates
- CA Certificates
- CRL

Local Certificates

Certificate requests and installed server certificates are displayed in the Local Certificates list. After you submit the request to a CA, the CA will verify the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA will then sign and send the signed certificate to you to install on the FortiGate unit.

To view certificate requests and/or import signed server certificates, go to VPN > Certificates > Local Certificates. To view certificate details, select the View Certificate Detail icon in the row that corresponds to the certificate.

The first entry in the list is the FortiGate unit’s self-signed certificate, which you cannot delete.

Figure 239: Local Certificates list

<table>
<thead>
<tr>
<th>Name</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate_Local</td>
<td>C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = <a href="mailto:support@fortinet.com">support@fortinet.com</a></td>
</tr>
<tr>
<td>FortiGate_Local2</td>
<td></td>
</tr>
</tbody>
</table>

**Generate**  Generate a local certificate request. See “Generating a certificate request” on page 370.

**Import**  Import a signed local certificate. See “Importing a signed server certificate” on page 373.

**Name**  The names of existing local certificates and pending certificate requests.

**Subject**  The Distinguished Names (DNs) of local signed certificates.
Generating a certificate request

The FortiGate unit generates a certificate request based on the information you enter to identify the FortiGate unit. Generated requests are displayed in the Local Certificates list with a status of PENDING. After you generate a certificate request, you can download the request to a computer that has management access to the FortiGate unit and then forward the request to a CA.

To fill out a certificate request, go to VPN > Certificates > Local Certificates and select Generate. To download and send the certificate request to a CA, see “Downloading and submitting a certificate request” on page 372.
### Figure 241: Generate Certificate Signing Request

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>NewLocalCert</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject Information</strong></td>
<td>host IP: 0.0.0.0</td>
</tr>
<tr>
<td>ID Type</td>
<td>Host IP</td>
</tr>
<tr>
<td>IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td><strong>Optional Information</strong></td>
<td>Marketing</td>
</tr>
<tr>
<td></td>
<td>Sales</td>
</tr>
<tr>
<td></td>
<td>New Business</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Marketing</td>
</tr>
<tr>
<td></td>
<td>Sales</td>
</tr>
<tr>
<td></td>
<td>New Business</td>
</tr>
<tr>
<td>Organization</td>
<td></td>
</tr>
<tr>
<td>Locality (City)</td>
<td></td>
</tr>
<tr>
<td>State/Province</td>
<td></td>
</tr>
<tr>
<td>Country/Region</td>
<td></td>
</tr>
<tr>
<td>e-mail</td>
<td></td>
</tr>
<tr>
<td><strong>Key Type</strong></td>
<td>RSA</td>
</tr>
<tr>
<td><strong>Key Size</strong></td>
<td>1024 bit</td>
</tr>
<tr>
<td><strong>Enrollment Method</strong></td>
<td>File Based</td>
</tr>
<tr>
<td></td>
<td>Online SCEP</td>
</tr>
<tr>
<td><strong>Challenge Password</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Certification Name</strong></td>
<td>Type a certificate name. Typically, this would be the name of the FortiGate unit. To enable the export of a signed certificate as a PKCS12 file later on if required, do not include spaces in the name.</td>
</tr>
<tr>
<td><strong>Subject Information</strong></td>
<td>Enter the information needed to identify the FortiGate unit:</td>
</tr>
<tr>
<td><strong>Host IP</strong></td>
<td>If the FortiGate unit has a static IP address, select Host IP and enter the public IP address of the FortiGate unit. If the FortiGate unit does not have a public IP address, use an email address (or domain name if available) instead.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>If the FortiGate unit has a static IP address and subscribes to a dynamic DNS service, use a domain name if available to identify the FortiGate unit. If you select Domain Name, enter the fully qualified domain name of the FortiGate unit. Do not include the protocol specification (http://) or any port number or path names. If a domain name is not available and the FortiGate unit subscribes to a dynamic DNS service, an &quot;unable to verify certificate&quot; type message may be displayed in the user’s browser whenever the public IP address of the FortiGate unit changes.</td>
</tr>
<tr>
<td><strong>E-Mail</strong></td>
<td>If you select E-mail, enter the email address of the owner of the FortiGate unit.</td>
</tr>
<tr>
<td><strong>Optional Information</strong></td>
<td>All fields under Optional Information are not required.</td>
</tr>
<tr>
<td><strong>Organization Unit</strong></td>
<td>Type the name of your department(s). You can enter a maximum of 5 Organization Units. To add or remove a unit, use the plus (+) or minus (-) icon.</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Type the legal name of your company or organization.</td>
</tr>
</tbody>
</table>
Downloading and submitting a certificate request

You have to fill out a certificate request and generate the request before you can submit the results to a CA. For more information, see “Generating a certificate request” on page 370.

To download and submit a certificate request

1. Go to VPN > Certificates > Local Certificates.
2. In the Local Certificates list, select the Download icon in the row that corresponds to the generated certificate request.
3. In the File Download dialog box, select Save to Disk.
4. Name the file and save it to the local file system.
5. Submit the request to your CA as follows:
   a. Using the web browser on the management computer, browse to the CA website.
   b. Follow the CA instructions to place a base-64 encoded PKCS#12 certificate request and upload your certificate request.
   c. Follow the CA instructions to download their root certificate and Certificate Revocation List (CRL), and then install the root certificate and CRL on each remote client (refer to the browser documentation).
6. When you receive the signed certificate from the CA, install the certificate on the FortiGate unit. See “Importing a signed server certificate” on page 373.

Local Certificates

VPN Certificates
Importing a signed server certificate

Your CA will provide you with a signed server certificate to install on the FortiGate unit. When you receive the signed certificate from the CA, save the certificate on a computer that has management access to the FortiGate unit.

To install the signed server certificate, go to VPN > Certificates > Local Certificates and select Import. Install the signed certificate through the Upload Local Certificate dialog box at the top of the page. The certificate file can be in either PEM or DER format. The other dialog boxes are for importing previously exported certificates and private keys.

**Figure 242: Upload Local Certificate**

<table>
<thead>
<tr>
<th>Certificate File</th>
<th>Enter the full path to and file name of the signed server certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse</td>
<td>Alternatively, browse to the location on the management computer where the certificate has been saved, select the certificate, and then select OK.</td>
</tr>
</tbody>
</table>

Importing an exported server certificate and private key

The server certificate and private key to import must have been exported previously as a single PKCS12 file through the `execute vpn certificate key export` CLI command. The file is associated with a password, which you will need to know in order to import the file. Before you begin, save a copy of the file on a computer that has management access to the FortiGate unit. For more information, see the FortiGate Certificate Management User Guide.

To import the PKCS12 file, go to VPN > Certificates > Local Certificates and select Import.

**Figure 243: Upload PKCS12 Certificate**

<table>
<thead>
<tr>
<th>Certificate with key file</th>
<th>Enter the full path to and file name of the previously exported PKCS12 file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse</td>
<td>Alternatively, browse to the location on the management computer where the PKCS12 file has been saved, select the file, and then select OK.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password needed to upload the PKCS12 file.</td>
</tr>
</tbody>
</table>
Importing separate server certificate and private key files

Use the Upload Certificate dialog box to import a server certificate and the associated private key file when the server certificate request and private key were not generated by the FortiGate unit. The two files to import must be available on the management computer.

Figure 244: Upload Certificate

| Certificate file | Enter the full path to and file name of the previously exported certificate file. |
| Key file | Enter the full path to and file name of the previously exported key file. |
| Browse | Browse to the location of the previously exported certificate file/key file, select the file, and then select OK. |
| Password | If a password is required to upload and open the files, type the password. |

Remote Certificates

Note: The certificate file must not use 40-bit RC2-CBC encryption.

For dynamic certificate revocation, an OCSP (Online Certificate Status Protocol) server is used. Remote certificates are public certificates without a private key. The OCSP is configured in the CLI only. For more information, see the FortiGate CLI Reference.

Note: There is one OCSP per vdom.

Figure 245: Remote certificate list

<table>
<thead>
<tr>
<th>Name</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>REMOTE_Cert_1</td>
<td>C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = <a href="mailto:support@fortiguard.com">support@fortiguard.com</a></td>
</tr>
</tbody>
</table>

Installed Remote (OCSP) certificates are displayed in the Remote Certificates list. To view installed Remote (OCSP) certificates or import a Remote (OCSP) certificate, go to VPN > Certificates > Remote. To view certificate details, select the View Certificate Detail icon in the row that corresponds to the certificate.
Importing Remote (OCSP) certificates

To import a Remote (OCSP) certificate, go to VPN > Certificates > Remote and select Import.

Figure 246: Upload Remote Certificate

| Import | Import a public OCSP certificate. See “Importing CA certificates” on page 376. |
| Name | The names of existing Remote (OCSP) certificates. The FortiGate unit assigns unique names (REMOTE_Cert_1, REMOTE_Cert_2, REMOTE_Cert_3, and so on) to the Remote (OCSP) certificates when they are imported. |
| Subject | Information about the Remote (OCSP) certificate. |
| Delete icon | Delete a Remote (OCSP) certificate. |
| View Certificate Detail icon | Display certificate details. |
| Download icon | Save a copy of the Remote (OCSP) certificate to a local computer. |

Importing Remote (OCSP) certificates

To import a Remote (OCSP) certificate, go to VPN > Certificates > Remote and select Import.

| Local PC | Use a local administrator’s PC to upload a public certificate. Enter the location, or select Browse to navigate to the location of the certificate. |
| Browse | Browse to the location on the management computer where the certificate has been saved, select the certificate, and then select OK. |

The system assigns a unique name to each Remote (OCSP) certificate. The names are numbered consecutively (REMOTE_Cert_1, REMOTE_Cert_2, REMOTE_Cert_3, and so on).

CA Certificates

When you apply for a signed personal (administrative) or group certificate to install on remote clients, you must obtain the corresponding root certificate and CRL from the issuing CA.

When you receive the signed personal or group certificate, install the signed certificate on the remote client(s) according to the browser documentation. Install the corresponding root certificate and CRL from the issuing CA on the FortiGate unit.

Installed CA certificates are displayed in the CA Certificates list. You cannot delete the Fortinet_CA certificate. To view installed CA root certificates or import a CA root certificate, go to VPN > Certificates > CA Certificates. To view root certificate details, select the View Certificate Detail icon in the row that corresponds to the certificate.
For detailed information and step-by-step procedures related to obtaining and installing digital certificates, see the *FortiGate Certificate Management User Guide*.

### Importing CA certificates

After you download the root certificate of the CA, save the certificate on a PC that has management access to the FortiGate unit.

To import a CA root certificate, go to **VPN > Certificates > CA Certificates** and select Import.

**Figure 248: Import CA Certificate**

- **SCEP**: Select to use an SCEP server to access CA certificate for user authentication. Enter the URL of the SCEP server from which to retrieve the CA certificate. Optionally, enter identifying information of the CA, such as the file name. Select OK.

- **Local PC**: Select to use a local administrator’s PC to upload a public certificate. Enter the location, or browse to the location on the management computer where the certificate has been saved, select the certificate, and then select OK.

When you select OK and you have elected to import a certificate via the SCEP server, the system starts the retrieval process immediately.

The system assigns a unique name to each CA certificate. The names are numbered consecutively (CA_Cert_1, CA_Cert_2, CA_Cert_3, and so on).
CRL

A Certificate Revocation List (CRL) is a list of CA certificate subscribers paired with certificate status information. Installed CRLs are displayed in the CRL list. The FortiGate unit uses CRLs to ensure that the certificates belonging to CAs and remote clients are valid.

To view installed CRLs, go to **VPN > Certificates > CRL**.

**Figure 249: Certificate revocation list**

<table>
<thead>
<tr>
<th>Name</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRL_1</td>
<td>C = US, ST = California, O=AT&amp;T/OU=AT&amp;T WorldNet(R) Certificate Services - Class 1 Individual CA</td>
</tr>
</tbody>
</table>

*View Certificate Detail*  
*Download*

**Import**  
Import a CRL. See “Importing a certificate revocation list” on page 377.

**Name**  
The names of existing certificate revocation lists. The FortiGate unit assigns unique names (CRL_1, CRL_2, CRL_3, and so on) to certificate revocation lists when they are imported.

**Subject**  
Information about the certificate revocation lists.

**Delete icon**  
Delete the selected CRL from the Fortigate configuration.

**View Certificate Detail icon**  
Display CRL details such as the issuer name and CRL update dates. See example **Figure 250**.

**Download icon**  
Save a copy of the CRL to a local computer.

**Figure 250: CRL Certificate Detail**

<table>
<thead>
<tr>
<th>Certificate Detail Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Name: CRL_2</td>
</tr>
<tr>
<td>Issuer: (O=AT&amp;T/OU=AT&amp;T WorldNet(R) Certificate Services - Class 1 Individual CA</td>
</tr>
<tr>
<td>Last Update: Mar 24 11 00:00:00 2005 GMT</td>
</tr>
<tr>
<td>Next Update: Apr 21 11 00:00:00 2005 GMT</td>
</tr>
</tbody>
</table>

**Importing a certificate revocation list**

Certificate revocation lists from CA web sites must be kept updated on a regular basis to ensure that clients having revoked certificates cannot establish a connection with the FortiGate unit. After you download a CRL from the CA web site, save the CRL on a computer that has management access to the FortiGate unit.

**Note:** When the CRL is configured with an LDAP, HTTP, and/or SCEP server, the latest version of the CRL is retrieved automatically from the server when the FortiGate unit does not have a copy of it or when the current copy expires.

To import a certificate revocation list, go to **VPN > Certificates > CRL** and select Import.
CRL

VPN Certificates

Figure 251: Import CRL

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Select to use an HTTP server to retrieve the CRL. Enter the URL of the HTTP server.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Select to use an LDAP server to retrieve the CRL. Select the LDAP server from the drop-down list.</td>
</tr>
<tr>
<td>SCEP</td>
<td>Select to use an SCEP server to retrieve the CRL. Select the Local Certificate from the drop-down list. Enter the URL of the SCEP server from which the CRL can be retrieved.</td>
</tr>
<tr>
<td>Local PC</td>
<td>Select to use a local administrator’s PC to upload a public certificate. Enter the location, or browse to the location on the management computer where the certificate has been saved, select the certificate, and then select OK.</td>
</tr>
</tbody>
</table>

The system assigns a unique name to each CRL. The names are numbered consecutively (CRL_1, CRL_2, CRL_3, and so on).
User

This section explains how to set up user accounts, user groups and external authentication servers. These are components of user authentication that you can use to control access to network resources.

This section describes:
- Configuring user authentication
- Local user accounts
- RADIUS servers
- LDAP servers
- PKI authentication
- Windows AD servers
- User groups
- Configuring peers and peer groups
- Authentication settings

Configuring user authentication

FortiGate authentication controls access by user group, but creating user groups is not the first step in configuring authentication. You must configure user authentication in the following order:

1. If external authentication using RADIUS or LDAP servers is needed, configure access to those servers. See "RADIUS servers" on page 381 and "LDAP servers" on page 382.

2. Configure local user accounts in User > Local. For each user, you can choose whether the password is verified by the FortiGate unit, by a RADIUS server or by an LDAP server. See "Local user accounts" on page 380.

3. If you use a Microsoft Windows Active Directory server for authentication, configure access to it. See "Configuring a Windows AD server" on page 386. Users authenticated by Active Directory server do not need local user accounts on the FortiGate unit. You must install the Fortinet Server Authentication Extensions (FSAE) on your Windows network.

4. To use certificate-based authentication for administrative access (HTTPS GUI), IPSec, SSL-VPN, and web-based authentication, configure using User > PKI. See "Configuring PKI users" on page 385.

5. Create user groups in User > User Group and add members. There are three types of user groups: Firewall, Active Directory and SSL VPN. See "Configuring a user group" on page 389.

For PKI authentication, only Firewall and SSL VPN user groups are applicable.

6. To change the authentication timeout value or select protocol support options, go to User > Authentication > Authentication. See "Authentication settings" on page 394.
Local user accounts

Go to User > Local to add local user accounts and configure authentication.

Figure 252: Local user list

| Create New | Add a new local user account. |
| User Name | The local user name. |
| Type | The authentication type to use for this user. |
| Delete icon | Delete the user. **Note:** The delete icon is not available if the user belongs to a user group. |
| Edit icon | Edit the user account. |

**Note:** Deleting the user name deletes the authentication configured for the user.

Configuring a user account

Go to User > Local and select Create New or the Edit icon of an existing user account.

Figure 253: Local user options

| User Name | Type or edit the user name. |
| Disable | Select Disable to prevent this user from authenticating. |
| Password | Select Password to authenticate this user using a password stored on the FortiGate unit. Type or edit the password. The password should be at least six characters long. |
| LDAP | Select LDAP to authenticate this user using a password stored on an LDAP server. Select the LDAP server from the drop-down list. **Note:** You can only select an LDAP server that has been added to the FortiGate LDAP configuration. See “LDAP servers” on page 382. |
| RADIUS | Select RADIUS to authenticate this user using a password stored on a RADIUS server. Select the RADIUS server from the drop-down list. **Note:** You can only select a RADIUS server that has been added to the FortiGate RADIUS configuration. See “RADIUS servers” on page 381. |
RADIUS servers

If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the FortiGate unit sends the user’s credentials to the RADIUS server for authentication. If the RADIUS server can authenticate the user, the user is successfully authenticated with the FortiGate unit. If the RADIUS server cannot authenticate the user, the connection is refused by the FortiGate unit.

Note: The default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645, use the CLI to change the default RADIUS port. For more information see the `config system global` command in the FortiGate CLI Reference.

To configure a RADIUS server, go to User > RADIUS.

Figure 254: RADIUS server list

Create New Add a new RADIUS server.
Name The name of the RADIUS server on the FortiGate unit.
Server Name/IP The domain name or IP address of the RADIUS server.
Delete icon Delete a RADIUS server configuration.
Note: You cannot delete a RADIUS server that has been added to a user group.
Edit icon Edit a RADIUS server configuration.

Configuring a RADIUS server

Go to User > RADIUS and select Create New or the Edit icon of an existing RADIUS server.

Figure 255: RADIUS configuration

Name Type or edit the name used to identify the RADIUS server.
Primary Server Name/IP Type or edit the domain name or IP address of the primary RADIUS server.
LDAP servers

If you have configured LDAP support and a user is required to authenticate using an LDAP server, the FortiGate unit contacts the LDAP server for authentication. To authenticate with the FortiGate unit, the user enters a user name and password. The FortiGate unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiGate unit. If the LDAP server cannot authenticate the user, the connection is refused by the FortiGate unit.

The FortiGate unit supports LDAP protocol functionality defined in RFC2251 for looking up and validating user names and passwords. FortiGate LDAP supports all LDAP servers compliant with LDAP v3. In addition, FortiGate LDAP supports LDAP over SSL/TLS. To configure SSL/TLS authentication, refer to the FortiGate CLI Reference.

FortiGate LDAP support does not extend to proprietary functionality, such as notification of password expiration, that is available from some LDAP servers. FortiGate LDAP support does not supply information to the user about why authentication failed.

Go to User > LDAP to configure an LDAP server.

Figure 256: LDAP server list

| Create New | Add a new LDAP server. |
| Name | The name that identifies the LDAP server on the FortiGate unit. |
| Server Name/IP | The domain name or IP address of the LDAP server. |
| Port | The port used to communicate with the LDAP server. |
| Common Name Identifier | The common name identifier for the LDAP server. The common name identifier for most LDAP servers is cn. However, some servers use other common name identifiers such as uid. |
| Distinguished Name | The distinguished name used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. |
| Delete icon | Delete the LDAP server configuration. |
| Edit icon | Edit the LDAP server configuration. |

LDAP servers

If you have configured LDAP support and a user is required to authenticate using an LDAP server, the FortiGate unit contacts the LDAP server for authentication. To authenticate with the FortiGate unit, the user enters a user name and password. The FortiGate unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiGate unit. If the LDAP server cannot authenticate the user, the connection is refused by the FortiGate unit.

The FortiGate unit supports LDAP protocol functionality defined in RFC2251 for looking up and validating user names and passwords. FortiGate LDAP supports all LDAP servers compliant with LDAP v3. In addition, FortiGate LDAP supports LDAP over SSL/TLS. To configure SSL/TLS authentication, refer to the FortiGate CLI Reference.

FortiGate LDAP support does not extend to proprietary functionality, such as notification of password expiration, that is available from some LDAP servers. FortiGate LDAP support does not supply information to the user about why authentication failed.

Go to User > LDAP to configure an LDAP server.

Figure 256: LDAP server list

<table>
<thead>
<tr>
<th>Name</th>
<th>Server Name/IP</th>
<th>Port</th>
<th>Common Name Identifier</th>
<th>Distinguished Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP1</td>
<td>2.2.2.2</td>
<td>389</td>
<td>on</td>
<td>su=accounts,ou=marketing,dc=fortinet,dc=com</td>
</tr>
<tr>
<td>LDAP_2</td>
<td>1.32.4.5</td>
<td>389</td>
<td>on</td>
<td>su=shipping,dc=fortinet,dc=com</td>
</tr>
</tbody>
</table>

Create New | Add a new LDAP server. |
Name | The name that identifies the LDAP server on the FortiGate unit. |
Server Name/IP | The domain name or IP address of the LDAP server. |
Port | The port used to communicate with the LDAP server. |
Common Name Identifier | The common name identifier for the LDAP server. The common name identifier for most LDAP servers is cn. However, some servers use other common name identifiers such as uid. |
Distinguished Name | The distinguished name used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. |
Delete icon | Delete the LDAP server configuration. |
Edit icon | Edit the LDAP server configuration. |
Configuring an LDAP server

Go to User > LDAP and select Create New or the Edit icon of an existing LDAP server.

Figure 257: LDAP server configuration

<table>
<thead>
<tr>
<th>New LDAP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Server Name/IP</td>
</tr>
<tr>
<td>Server Port</td>
</tr>
<tr>
<td>Common Name Identifier</td>
</tr>
<tr>
<td>Distinguished Name</td>
</tr>
<tr>
<td>Secure Connection</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>Certificate</td>
</tr>
</tbody>
</table>

Name
Type or edit the name used to identify the LDAP server.

Server Name/IP
Type or edit the domain name or IP address of the LDAP server.

Server Port
Type or edit the port used to communicate with the LDAP server. By default, LDAP uses port 389.

Note: If you use a secure LDAP server, the default port will reflect your selection in Protocol.

Common Name Identifier
Type or edit the common name identifier for the LDAP server. 20 characters maximum.
The common name identifier for most LDAP servers is cn. However some servers use other common name identifiers such as uid.

Distinguished Name
Type or edit the distinguished name used to look up entries on the LDAP server.
Enter the base distinguished name for the server using the correct X.500 or LDAP format. The FortiGate unit passes this distinguished name unchanged to the server.
For example, you could use the following base distinguished name: ou=marketing,dc=fortinet,dc=com
where ou is organization unit and dc is domain component.
You can also specify multiple instances of the same field in the distinguished name, for example, to specify multiple organization units: ou=accounts,ou=marketing,dc=fortinet,dc=com

Query icon
View the LDAP server Distinguished Name Query tree for the base Distinguished Name.
The LDAP Distinguished Name Query list displays the LDAP Server IP address, and all the distinguished names associated with the Common Name Identifier for the LDAP server. The tree helps you to determine the appropriate entry for the DN field. Expand the Common Name Identifier to see the associated DNs. Select the DN from the list. The DN you select is displayed in the Distinguished Name field. Select OK and the Distinguished Name you selected will be saved in the Distinguished Name field of the LDAP Server configuration. To see the users within the LDAP Server user group for the selected Distinguished Name, expand the Distinguished Name in the LDAP Distinguished Name Query tree.

Secure Connection
Select to use a secure LDAP server connection for authentication.
PKI authentication

Public Key Infrastructure (PKI) authentication utilizes a certificate authentication library that takes a list of ‘peers’, ‘peer’ groups, and/or user groups and returns authentication ‘successful’ or ‘denied’ notifications. Users only need a valid certificate for successful authentication - no username or password are necessary.

For more information about certificate authentication, see the FortiGate Certificate Management User Guide. For information about the detailed PKI configuration settings only available through the CLI, see the FortiGate CLI Reference.

Go to User > PKI to configure PKI users.

Figure 259: User > PKI user list

<table>
<thead>
<tr>
<th>User Name</th>
<th>Subject</th>
<th>Issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td>pki_user1</td>
<td>C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = <a href="mailto:support@fortinet.com">support@fortinet.com</a></td>
<td></td>
</tr>
</tbody>
</table>

Create New    Add a new PKI user.
User Name      The name of the PKI user.
Subject        The text string that appears in the subject field of the certificate of the authenticating user.
Issuer         The CA certificate that is used to authenticate this user.
Delete icon    Delete this PKI user.
Edit icon      Edit this PKI user.

Note: The following fields in the PKI User List correspond to the noted fields in the PKI User dialog:
User Name: Name
Subject: Subject
CA: Issuer (CA certificate)
Configuring PKI users

Go to User > PKI and select Create New or the Edit icon of an existing PKI user.

Figure 260: PKI user configuration

![New PKI User](image)

Name            Enter the name of the PKI user. This field is mandatory. The PKI user can also be defined in the CLI using `config user peer`. For more information, see the FortiGate CLI Reference.

Subject         Enter the text string that appears in the subject field of the certificate of the authenticating user. This field is optional.

CA              Enter the CA certificate that must be used to authenticate this user. This field is optional.

Note: Even though Subject and CA are optional fields, one of them must be set. The following fields in the PKI User dialog correspond to the noted fields in the PKI User List:

Name: User Name

Subject: Subject

Issuer: CA (CA certificate)

Windows AD servers

On networks that use Windows Active Directory (AD) servers for authentication, FortiGate units can transparently authenticate users without asking them for their user name and password. You must install the Fortinet Server Authentication Extensions (FSAE) on the network and configure the FortiGate unit to retrieve information from the Windows AD server. For more information about FSAE, see the FSAE Technical Note.

Go to User > Windows AD to configure Windows AD servers.

Figure 261: Windows AD server list

<table>
<thead>
<tr>
<th>Name</th>
<th>FSAE Collector IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>WindowsAD_HQ</td>
<td>192.168.1.5:8000</td>
</tr>
</tbody>
</table>

Create New        Add a new Windows AD server.

Name               The name of the Windows AD server with FSAE.
You can expand the server name to display Windows AD domain group information.

FSAE Collector IP  The IP addresses and TCP ports of up to five collector agents that send Windows AD server logon information to the FortiGate unit.

Delete icon        Delete this Windows AD server.

Edit icon          Edit this Windows AD server.

Refresh icon       Get current domain and group information from the Windows AD server.
Configuring a Windows AD server

Go to **User > Windows AD** and select Create New or the Edit icon of an existing Windows AD server.

**Figure 262: Windows AD server configuration**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type or edit the name of the Windows AD server. This name appears in the list of Windows AD servers when you create user groups. Enter the following information for up to five collector agents.</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSAE Collector IP</td>
<td>Type or edit the IP address of the Windows AD server where this collector agent is installed.</td>
</tr>
<tr>
<td>Port</td>
<td>Type or edit the TCP port used for Windows AD. This must be the same as the FortiGate listening port specified in the FSAE collector agent configuration.</td>
</tr>
<tr>
<td>Password</td>
<td>Type or edit the password for the collector agent. This is required only if you configured your FSAE collector agent to require authenticated access.</td>
</tr>
</tbody>
</table>

**User groups**

A user group is a list of user identities. An identity can be:

- a local user account (user name and password) stored on the FortiGate unit
- a local user account with a password stored on a RADIUS or LDAP server
- a RADIUS or LDAP server (all identities on the server can authenticate)
- a user group defined on a Microsoft Active Directory server

In most cases, the FortiGate unit authenticates users by requesting their user name and password. The FortiGate unit checks local user accounts first. If a match is not found, the FortiGate unit checks the RADIUS or LDAP servers that belong to the user group. Authentication succeeds when a matching user name and password are found.

For an Active Directory user group, the Active Directory server authenticates users when they log on to the network. The FortiGate unit receives the user’s name and IP address from the FSAE collector agent. For more information about FSAE, see the *FSAE Technical Note*. 
You can configure user groups to provide authenticated access to:

- Firewall policies that require authentication
  See “Adding authentication to firewall policies” on page 276.
- SSL VPNs on the FortiGate unit
  See “SSL-VPN firewall policy options” on page 281.
- IPSec VPN Phase 1 configurations for dialup users
  See “Creating a new phase 1 configuration” on page 345.
- XAuth for IPSec VPN Phase 1 configurations
  See XAUTH in “Defining phase 1 advanced settings” on page 348.
- FortiGate PPTP configuration
  See “PPTP Range” on page 361.
- FortiGate L2TP configuration
  This is configurable only using the `config vpn l2tp` CLI command. See the FortiGate CLI Reference.
- Administrator login with RADIUS authentication
  See “Configuring RADIUS authentication for administrators” on page 163.
- FortiGuard Web Filtering override groups
  See “FortiGuard - Web Filter” on page 435.

For each resource that requires authentication, you specify which user groups are permitted access. You need to determine the number and membership of user groups appropriate to your authentication needs.

**User group types**

There are three types of user group:

- Firewall
- Active Directory
- SSL VPN

**Firewall**

A firewall user group provides access to a firewall policy that requires firewall type authentication and lists the user group as one of the allowed groups. The FortiGate unit requests the group member’s user name and password when the user attempts to access the resource that the policy protects. A user may also be authenticated by certificate if this method is selected in the firewall policy. For more information, see “Adding authentication to firewall policies” on page 276.

A firewall user group can also provide access to an IPSec VPN for dialup users. In this case, the IPSec VPN phase 1 configuration uses the Accept peer ID in dialup group peer option. The user’s VPN client is configured with the user name as peer ID and the password as pre-shared key. The user can connect successfully to the IPSec VPN only if the user name is a member of the allowed user group and the password matches the one stored on the FortiGate unit. A user group cannot be a dialup group if any member is authenticated using a RADIUS or LDAP server. For more information, see “Creating a new phase 1 configuration” on page 345.
A firewall user group can be used to provide override privileges for FortiGuard web filtering. See “Configuring FortiGuard override options for a user group” on page 391. For detailed information about FortiGuard Web Filter, including the override feature, see “FortiGuard - Web Filter” on page 435.

**Active Directory**

On a Microsoft Windows network, the FortiGate unit can allow access to members of Active Directory server user groups who have been authenticated on the Windows network. The Fortinet Server Authentication Extensions (FSAE) must be installed on the network domain controllers.

An Active Directory user group provides access to a firewall policy that requires Active Directory type authentication and lists the user group as one of the allowed groups. The members of the user group are Active Directory groups that you select from a list that the FortiGate unit receives from the Windows AD servers that you have configured. See “Windows AD servers” on page 385.

*Note:* An Active Directory user group cannot have FortiGuard Web Filter override privileges or SSL VPN access.

**SSL VPN**

An SSL VPN user group provides access to a firewall policy that requires SSL VPN type authentication and lists the user group as one of the allowed groups. Local user accounts, LDAP, and RADIUS servers can be members of an SSL VPN user group. The FortiGate unit requests the user’s user name and password when the user accesses the SSL VPN web portal. The user group settings include options for SSL VPN features. See “Configuring SSL VPN user group options” on page 392.

An SSL VPN user group can also provide access to an IPSec VPN for dialup users. In this case, the IPSec VPN phase 1 configuration uses the Accept peer ID in dialup group peer option. The user’s VPN client is configured with the user name as peer ID and the password as pre-shared key. The user can connect successfully to the IPSec VPN only if the user name is a member of the allowed user group and the password matches the one stored on the FortiGate unit.

*Note:* A user group cannot be an IPSec dialup group if any member is authenticated using a RADIUS or LDAP server.

For more information, see “Creating a new phase 1 configuration” on page 345.
User group list

Go to User > User Group to configure user groups.

Figure 263: User group list

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Members</th>
<th>Protection Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>User10, User11, User12, User13, User14, User15, LDAP1</td>
<td>strict</td>
</tr>
<tr>
<td>Active Directory</td>
<td>DOCTEST/Developers, DOCTEST/Engineering</td>
<td>scan</td>
</tr>
<tr>
<td>SSL VPN</td>
<td>Users1, Users2, Users3, Users4, Users5</td>
<td></td>
</tr>
</tbody>
</table>

Create New Add a new user group.

Group Name The name of the user group. User group names are listed by type of user group: Firewall, Active Directory and SSL VPN.

Members The users, RADIUS servers, or LDAP servers in the user group.

Protection Profile The protection profile associated with this user group.

Delete icon Delete the user group.

Note: You cannot delete a user group that is included in a firewall policy, a dialup user phase 1 configuration, or a PPTP or L2TP configuration.

Edit icon Edit the membership and options of the group.

Configuring a user group

Go to User > Group and select Create New or the Edit icon of an existing user group.

Figure 264: User group configuration

Name Type or enter the name of the user group.
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Select this group in any firewall policy that requires Firewall authentication. See “Adding authentication to firewall policies” on page 276.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Select this group in any firewall policy that requires Active Directory authentication. See “Adding authentication to firewall policies” on page 276.</td>
</tr>
<tr>
<td>SSL VPN</td>
<td>Select this group in any firewall policy with Action set to SSL VPN. See “SSL-VPN firewall policy options” on page 281.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protection Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Users</td>
<td>The list of users, RADIUS servers, LDAP servers, or PKI users that can be added to the user group.</td>
</tr>
<tr>
<td>Members</td>
<td>The list of users, RADIUS servers, LDAP servers, or PKI users that belong to the user group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Right arrow button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Add a user or server to the Members list. Select a user or server name in the Available Users list and select the right arrow button to move it to the Members list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Left arrow button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Remove a user or server from the Members list. Select a user name or server name in the Members list and select the left arrow button to move it to the Available Users list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FortiGuard Web Filtering Override</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure Web Filtering override capabilities for this group. See &quot;Configuring FortiGuard override options for a user group&quot; on page 391.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSL-VPN User Group Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For detailed instructions about how to configure web-only mode or tunnel mode operation, see the FortiGate SSL VPN User Guide.</td>
</tr>
</tbody>
</table>

**Note:** If you try to add LDAP servers or local users to a group configured for administrator authentication, an “Entry not found” error occurs.
Configuring FortiGuard override options for a user group

Go to User > Group and select the Edit icon for a firewall user group. Expand the FortiGuard Web Filtering Override section.

Figure 265: FortiGuard Web Filtering Override configuration

Allowed to perform FortiGuard Web Filtering overrides

Select to allow members of this group to request an override on the FortiGuard Web Filtering Block page. The firewall protection profile governing the connection must have FortiGuard overrides enabled. The protection profile may have more than one user group as an override group. Members of an override group can authenticate on the FortiGuard Web Filter Block Override page to access the blocked site.

For detailed information see “FortiGuard - Web Filter” on page 435.

Override Scope

The override can apply to just the user who requested the override, or include others. Make a selection from the drop-down list to include:

- **User**: Only the user
- **User Group**: The user group to which the user belongs
- **IP**: Any user at the user’s IP address
- **Profile**: Any user with the specified protection profile of the user group
- **Ask**: Authenticating user, who chooses the override scope

Override Type

Select from the drop-down list to allow access to:

- **Directory**: Only the lowest level directory in the URL
- **Domain**: The entire website domain
- **Categories**: The FortiGuard category
- **Ask**: Authenticating user, who chooses the override type

Off-site URLs

Select from the drop-down list whether the user can follow links to sites off of the blocked site:

- **Allow**: User can follow links to other sites.
- **Deny**: User can follow links only to destinations as defined by Override Type.
- **Ask**: Authenticating user chooses whether to allow use of off-site links.
Configuring SSL VPN user group options

Go to User > Group and select the Edit icon for an SSL VPN user group. Expand the SSL-VPN User Group Options section.

For detailed instructions about how to configure web-only mode or tunnel mode operation, see the FortiGate SSL VPN User Guide.

Override Time
Select to set the duration of the override:

- **Constant**: Select to set the duration of override in days, hours, minutes.
- **Ask**: Select to allow the authenticating user to determine the duration of override. The duration set is the maximum.

Protection Profiles Available
List of defined protection profiles configured (available for Firewall or Active Directory user groups only).

One protection profile can have several user groups with override permissions. Verification of the user group occurs once the username and password are entered. The overrides can still be enabled/disabled on a profile-wide basis regardless of the user groups that have permissions to override the profile.

Permission Granted For
Select the protection profiles that will have override privileges within the user group.

Enable SSL-VPN Tunnel Service
Select to allow users in this group to connect to the network behind the FortiGate unit using the SSL VPN tunnel. Not available in Transparent mode.

Allow Split Tunneling
Select to allow split tunneling for this group. Split tunneling ensures that only the traffic for the private network is sent to the SSL VPN gateway. Internet traffic is sent through the usual unencrypted route.

Restrict tunnel IP range for this group
Type the starting and ending IP address range for this group if you want to override the Tunnel IP range defined in VPN > SSL > Config.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Web Application</strong></td>
<td>Select to enable the web portal to provide access to web applications. This is not available in Transparent mode. If you enabled Web Application, select to enable each of the applications that users in this group are permitted to access.</td>
</tr>
<tr>
<td><strong>HTTP/HTTPS Proxy</strong></td>
<td>Select to enable the web portal to provide access to web applications. This is not available in Transparent mode. If you enabled Web Application, select to enable each of the applications that users in this group are permitted to access.</td>
</tr>
<tr>
<td><strong>FTP</strong></td>
<td>HTTP/HTTPS Proxy</td>
</tr>
<tr>
<td><strong>Telnet (applet)</strong></td>
<td>HTTP/HTTPS Proxy</td>
</tr>
<tr>
<td><strong>SMB/CIFS</strong></td>
<td>HTTP/HTTPS Proxy</td>
</tr>
<tr>
<td><strong>VNC</strong></td>
<td>HTTP/HTTPS Proxy</td>
</tr>
<tr>
<td><strong>RDP</strong></td>
<td>HTTP/HTTPS Proxy</td>
</tr>
<tr>
<td><strong>Check FortiClient AV Installed and Running</strong></td>
<td>Select to allow the client to connect only if it is running FortiClient Host Security AV software. For information about this software, see the Fortinet Technical Documentation web site.</td>
</tr>
<tr>
<td><strong>Check FortiClient FW Installed and Running</strong></td>
<td>Select to allow the client to connect only if it is running FortiClient Host Security FW software. For information about this software, see the Fortinet Technical Documentation web site.</td>
</tr>
<tr>
<td><strong>Check for Third Party AV Software</strong></td>
<td>Select to allow the client to connect only if it has supported antivirus software installed. The software must be installed and enabled (running). See “AV/Firewall supported product detection” for supported products for Windows XP SP2. For all other systems, Norton (Symantec) AntiVirus or McAfee VirusScan software is supported. <strong>Note</strong>: This option is not available if you select Check FortiClient Installed and Running.</td>
</tr>
<tr>
<td><strong>Check for Third Party Firewall Software</strong></td>
<td>Select to allow the client to connect only if it has supported firewall software installed. The software must be installed and enabled (running). See “AV/Firewall supported product detection” for supported products for Windows XP SP2. For all other systems, Norton (Symantec) AntiVirus or McAfee VirusScan software is supported. <strong>Note</strong>: This option is not available if you select Check FortiClient Installed and Running.</td>
</tr>
<tr>
<td><strong>Enable Cache Clean</strong></td>
<td>Select to remove all temporary Internet files created on the client computer between user login and logout. This is executed with a downloaded ActiveX control for IE, and a plugin for Firefox. Works on Internet Explorer and Firefox with Windows 2000/ Windows XP. <strong>Note</strong>: If the client’s browser cannot install and run the cache cleaner, the user is not allowed to access the SSL VPN portal.</td>
</tr>
<tr>
<td><strong>Bookmarks</strong></td>
<td>Enable to allow the SSL VPN user group to use the pre-configured bookmark group that you select from the drop-down menu.</td>
</tr>
<tr>
<td><strong>Redirect URL</strong></td>
<td>Select to open a second browser window at this URL when the SSL VPN web portal page opens. The web server for this URL must reside on the private network behind the FortiGate unit. <strong>Note</strong>: You can modify the SSL VPN web portal login page. For more information, see “Changing the SSL-VPN login message” on page 157.</td>
</tr>
<tr>
<td><strong>Customize portal message for this group</strong></td>
<td>Type or edit a custom web portal home page caption for this group.</td>
</tr>
</tbody>
</table>
Configuring peers and peer groups

You can define peers and peer groups used for authentication in some VPN configurations and for PKI certificate authentication. Use the CLI `config user peer` and `config user peergrp` commands to do this. For more information, see the “User” chapter of the FortiGate CLI Reference.

Authentication settings

You can define global settings for user authentication, including authentication timeout, supported protocols, and authentication certificates.

Authentication timeout controls how long an authenticated firewall connection can be idle before the user must authenticate again.

When user authentication is enabled on a firewall policy, the authentication challenge is normally issued for any of the four protocols (dependent on the connection protocol):

- HTTP (can also be set to redirect to HTTPS)
- HTTPS
- FTP
- Telnet

The selections made in the Protocol Support list of the Authentication Settings screen control which protocols support the authentication challenge. The user must connect with a supported protocol first so they can subsequently connect with other protocols. If HTTPS is selected as a method of protocol support, it allows the user to authenticate with a customized Local certificate.

### Table 33: AV/Firewall supported product detection

<table>
<thead>
<tr>
<th>Product</th>
<th>AV</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Norton Internet Security 2006</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Trend Micro PC-cillin</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>McAfee</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Sophos Anti-Virus</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Panda Platinum 2006 Internet Security</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>F-Secure</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Secure Resolutions</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Cat Computer Services</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>AhnLab</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Kaspersky</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>ZoneAlarm</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
When you enable user authentication on a firewall policy, the end users using the firewall policy will be challenged to authenticate themselves. In the case of user ID and password authentication, end users must provide their user name and password. In case of certificate authentication (HTTPS or HTTP redirected to HTTPS only), you can install customized certificates on the FortiGate unit and the end users can also have customized certificates installed on their browsers. Otherwise, the end users will see a warning message and have to accept the default FortiGate certificate, which the end users’ browsers may deem as invalid.

**Note:** When you use certificate authentication, if you do not specify any certificate when you create the firewall policy, the global settings will be used. If you specify a certificate, the per-policy setting will overwrite the global setting. For information about how to use certificate authentication, see *FortiGate Certificate Management User Guide*.

Go to **User > Authentication > Authentication** to configure user authentication global settings.

**Figure 267:** Authentication Settings

<table>
<thead>
<tr>
<th>Authentication Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Timeout</strong></td>
</tr>
<tr>
<td><strong>Protocol Support</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Certificate</strong></td>
</tr>
<tr>
<td><strong>Apply</strong></td>
</tr>
</tbody>
</table>
AntiVirus

This section describes how to configure the antivirus options associated with firewall protection profiles.

This section describes:

- Order of operations
- Antivirus elements
- Antivirus settings and controls
- File pattern
- Quarantine
- Config
- Antivirus CLI configuration

Order of operations

Antivirus processing includes various modules and engines that perform separate tasks. The FortiGate unit performs antivirus processing in the order the elements appear in the web-based manager menu:

- File pattern
- Virus scan
- Grayware
- Heuristics

If a file fails any of the elements of the antivirus scan, no further scans are performed. For example, if the file “fakefile.EXE”, is recognized as a blocked pattern, the FortiGate unit will send the end user a replacement message and the file will be deleted or quarantined. The virus scan, grayware and heuristic scans will not be performed as the file is already found to be a threat and has been dealt with; there is no need to use further system resources on the file at this time.

Antivirus elements

The antivirus elements work in sequence to give you an efficient method of scanning incoming files. The first three elements have specific functions, the fourth, the heuristics, is to cover any new, previously unknown, virus threats. The four elements work together to offer your network unparalleled antivirus protection. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The elements will be discussed in the order that they are applied followed by FortiGuard antivirus.
File pattern

Once a file is accepted, the FortiGate unit applies the file pattern recognition filter. The FortiGate will check the file against the file pattern setting you have configured. If the file is a blocked pattern, "*.EXE" for example, then it is stopped and a replacement message is sent to the end user. No other levels of protection are applied. If the file is not a blocked pattern the next level of protection is applied.

Virus scan

If the file is passed by the file pattern it will have a virus scan applied to it. The virus definitions are kept up to date through the FortiNet Distribution Network. The list is updated on a regular basis so you do not have to wait for a firmware upgrade. For more information on updating virus definitions see "FortiGuard antivirus" on page 398.

Grayware

Once past the file pattern and the virus scan, the incoming file will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information on configuring grayware please see “Viewing the grayware list” on page 407.

Heuristics

After an incoming file has passed the first three antivirus elements, it is subjected to the heuristics element. The FortiGate heuristic antivirus engine performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results.

Note: Heuristics is configurable only through the CLI. See the FortiGate CLI Reference.

FortiGuard antivirus

FortiGuard antivirus services are an excellent resource and include automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNSBL, through the FortiGuard Distribution Network (FDN). The FortiGuard Center also provides the FortiGuard antivirus virus and attack encyclopedia and the FortiGuard Bulletin. Visit the Fortinet Knowledge Center for details and a link to the FortiGuard Center.

The connection between the FortiGate unit and FortiGuard Center is configured in System > Maintenance > FortiGuard Center. See “Configuring the FortiGate unit for FDN and FortiGuard services” on page 188 for more information.

Note: If virtual domains are enabled on the FortiGate unit, antivirus features are configured globally. To access these features, select Global Configuration on the main menu.
Antivirus settings and controls

While antivirus settings are configured for system-wide use, specific settings can be implemented on a per profile basis. Table 34 compares antivirus options in protection profiles and the antivirus menu.

Table 34: Antivirus and Protection Profile antivirus configuration

<table>
<thead>
<tr>
<th>Protection Profile antivirus options</th>
<th>Antivirus setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus Scan</td>
<td>AntiVirus &gt; Config &gt; Virus List</td>
</tr>
<tr>
<td>Enable or disable virus scanning for each protocol (HTTP, FTP, IMAP, POP3, SMTP, IM).</td>
<td>View a read-only list of current viruses.</td>
</tr>
<tr>
<td>File Pattern</td>
<td>AntiVirus &gt; File Pattern</td>
</tr>
<tr>
<td>Enable or disable file pattern handling for each protocol.</td>
<td>Configure file patterns to block or allow files. Patterns can also be individually enabled or disabled.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>AntiVirus &gt; Quarantine</td>
</tr>
<tr>
<td>Enable or disable quarantining for each protocol. Quarantine is only available on units with a local disk, or with a configured FortiAnalyzer unit.</td>
<td>View and sort the list of quarantined files, configure file patterns to upload automatically to Fortinet for analysis, and configure quarantining options in AntiVirus.</td>
</tr>
<tr>
<td>Pass fragmented email messages</td>
<td></td>
</tr>
<tr>
<td>Enable or disable passing fragmented email messages. Fragmented email messages cannot be scanned for viruses.</td>
<td></td>
</tr>
<tr>
<td>Comfort Clients</td>
<td></td>
</tr>
<tr>
<td>Enable or disable for HTTP and FTP traffic. Set the interval and byte amount to trigger client comforting.</td>
<td></td>
</tr>
<tr>
<td>Oversized file/email</td>
<td></td>
</tr>
<tr>
<td>Configure the FortiGate unit to block or pass oversized files and email messages for each protocol. Set the size thresholds for files and email messages for each protocol in AntiVirus.</td>
<td>AntiVirus &gt; Config &gt; Grayware</td>
</tr>
<tr>
<td>Add signature to outgoing email messages</td>
<td></td>
</tr>
<tr>
<td>Create and enable a signature to append to outgoing email messages (SMTP only).</td>
<td></td>
</tr>
</tbody>
</table>
File pattern

Configure file patterns to block all files that are a potential threat and to prevent active computer virus attacks. Files can be blocked by name, extension, or any other pattern. File pattern blocking provides the flexibility to block potentially harmful content.

**Note:** File pattern entries are not case sensitive. For example, adding `*.exe` to the file pattern list also blocks any files ending in `.exe`.

For standard operation, you can choose to disable File Pattern in the Protection Profile, and enable it temporarily to block specific threats as they occur.

The FortiGate unit blocks files that match a configured file pattern and displays a replacement message instead. The FortiGate unit also writes a message to the virus log and sends an alert email message if configured to do so.

If both File Pattern and Virus Scan are enabled, the FortiGate unit blocks files that match enabled file patterns and does not scan these files for viruses.

**Note:** If virtual domains are enabled on the FortiGate unit, antivirus features are configured globally. To access these features, select **Global Configuration** on the main menu.

Viewing the file pattern list catalog

You can add multiple file pattern lists FortiGate and then select the best file pattern list for each protection profile. To view the file pattern list catalog, go to **AntiVirus** > **File Pattern**. To view any individual file pattern list, select the edit icon for the list you want to see.

**Figure 268:** Sample file pattern list catalog

<table>
<thead>
<tr>
<th>Name</th>
<th># Entries</th>
<th>Profiles</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>built-in-patterns</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>web</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td>2</td>
<td></td>
<td>For remote off</td>
</tr>
</tbody>
</table>

**Note:** The default file pattern list catalog is called built-in-patterns.

**Create New**

Select Create New to add a new file pattern list to the catalog.

**Name**

The available file pattern lists.

**# Entries**

The number of file patterns in each file pattern list.

**Profiles**

The protection profiles each file pattern list has been applied to.

**Comment**

Optional description of each file pattern list.

**Delete icon**

Select to remove the file pattern list from the catalog. The delete icon is only available if the file pattern list is not selected in any protection profiles.

**Edit icon**

Select to edit the file pattern list, list name, or list comment.

Select file pattern lists in protection profiles. For more information, see "Antivirus options" on page 332.
Creating a new file pattern list

To add a file pattern list to the file pattern list catalog, go to AntiVirus > File Pattern and select Create New.

Figure 269: New File Pattern List dialog box

Viewing the file pattern list

To view the file pattern list FortiGate, go to AntiVirus > File Pattern and select the edit icon of the file pattern list you want to view.

Figure 270: Sample file pattern list

The file pattern list has the following icons and features:

- **Name**: Enter the name of the new list.
- **Comment**: Enter a comment to describe the list, if required.

**Pattern**

The current list of file patterns.

**Action**

Files matching the file patterns can be set to block or allow.

**Enable**

Clear the checkbox to disable the file pattern.

**Delete icon**

Select to remove the file pattern from the list.

**Edit icon**

Select to edit the file pattern and action.

**Move To icon**

Select to move the file pattern to any position in the list.

Files are compared to the enabled file patterns from top to bottom. If a file does not match any specified patterns, it is passed along to antivirus scanning (if enabled). In effect, files are passed if not explicitly blocked.
Using the allow action, this behavior can be reversed with all files being blocked unless explicitly passed. Simply enter all the file patterns to be passed with the allow attribute. At the end of the list, add an all-inclusive wildcard (*.*) with a block action. Allowed files continue to antivirus scanning (if enabled) while files not matching any allowed patterns are blocked by the wildcard at the end.

The file pattern list is preconfigured with a default list of file patterns:

- executable files (*.bat, *.com, and *.exe)
- compressed or archive files (*.gz, *.rar, *.tar, *.tgz, and *.zip)
- dynamic link libraries (*.dll)
- HTML application (*.hta)
- Microsoft Office files (*.doc, *.ppt, *.xl?)
- Microsoft Works files (*.wps)
- Visual Basic files (*.vb?)
- screen saver files (*.scr)
- program information files (*.pif)

File pattern is enabled in protection profiles. For more information, see “Antivirus options” on page 332.

### Configuring the file pattern list

File patterns can be up to 80 characters long. The maximum number of file patterns in a list is 5000.

To add a new file pattern while viewing a file pattern list, select Create New. To edit an existing file pattern, select the edit icon associated with the pattern.

![Figure 271: New file pattern](image)

**Pattern**

Enter the file pattern. The file pattern can be an exact file name or can include wildcards.

**Action**

Select an action from the drop down list: Block or Allow.

**Enable**

Select to enable the pattern.

---

**Quarantine**

FortiGate units with a local disk can quarantine blocked and infected files. View the file name and status information about the file in the quarantined file list. Submit specific files and add file patterns to the AutoSubmit list so they will automatically be uploaded to Fortinet for analysis.

FortiGate units without a local disk can quarantine blocked and infected files to a FortiAnalyzer unit. Files stored on the FortiAnalyzer can be retrieved for viewing. To configure the FortiAnalyzer unit, go to Log & Report > Log Config > Log Setting.
Viewing the Quarantined Files list

The Quarantined Files list displays information about each file quarantined because of virus infection or file blocking. Sort the files by file name, date, service, status, duplicate count (DC), or time to live (TTL). Filter the list to view only quarantined files with a specific status or from a specific service.

To view the Quarantined Files list, go to **AntiVirus > Quarantine > Quarantined Files**.

Figure 272: Quarantined files list

<table>
<thead>
<tr>
<th>File Name</th>
<th>Date</th>
<th>Service</th>
<th>Status</th>
<th>Status Description</th>
<th>DC</th>
<th>TTL</th>
<th>Heuristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>19990101.doc</td>
<td>2005-11-22 15:20</td>
<td>POP3</td>
<td>Blocked</td>
<td>File was stopped by file block pattern</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>exac.exe</td>
<td>2005-11-23 00:04</td>
<td>HTTP</td>
<td>Infected</td>
<td>File is infected with &quot;RICOH.TEST_FILE&quot;</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>import-details.zip</td>
<td>2005-11-23 23:59</td>
<td>HTTP</td>
<td>Heuristics</td>
<td>File is suspicious, caught by heuristics</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Source_file.exe</td>
<td>2004-11-23 00:11</td>
<td>FTP</td>
<td>Heuristics</td>
<td>File is suspicious, caught by heuristics</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

The quarantined files list has the following features and displays the following information about each quarantined file:

**Apply**: Select to apply the sorting and filtering selections to the quarantined files list.

**Sort by**: Sort the list. Choose from: status, service, file name, date, TTL, or duplicate count. Select Apply to complete the sort.

**Filter**: Filter the list. Choose from status (infected, blocked, or heuristics) or service (HTTP, FTP, SMTP, POP3, IMAP). Select Apply to complete the filtering. Heuristics mode is configurable through the CLI only. See "Antivirus CLI configuration" on page 409.

**File Name**: The processed file name of the quarantined file. When a file is quarantined, all spaces are removed from the file name, and a 32-bit checksum is performed on the file. The checksum appears in the replacement message but not in the quarantined file. The file is stored on the FortiGate hard disk with the following naming convention: `<32bit_CRC>.<processed_filename>`. For example, a file named Over Size.exe is stored as 3fc155d2.oversize.exe.

**Date**: The date and time the file was quarantined, in the format dd/mm/yyyy hh:mm. This value indicates the time that the first file was quarantined if the duplicate count increases.

**Service**: The service from which the file was quarantined (HTTP, FTP, IMAP, POP3, SMTP, IM).

**Status**: The reason the file was quarantined: infected, heuristics, or blocked.

**Status Description**: Specific information related to the status, for example, “File is infected with "W32/Klez.h"” or “File was stopped by file block pattern.”

**DC**: Duplicate count. A count of how many duplicates of the same file were quarantined. A rapidly increasing number can indicate a virus outbreak.

**TTL**: Time to live in the format hh:mm. When the TTL elapses, the FortiGate unit labels the file as EXP under the TTL heading. In the case of duplicate files, each duplicate found refreshes the TTL. The TTL information is not available if the files are quarantined on a FortiAnalyzer unit.
Configure the FortiGate unit to upload suspicious files automatically to Fortinet for analysis. Add file patterns to the AutoSubmit list using wildcard characters (* or ?). File patterns are applied for AutoSubmit regardless of file blocking settings.

Upload files to Fortinet based on status (blocked or heuristics), or submit individual files directly from the quarantined files list. The FortiGate unit uses encrypted email to autosubmit files to an SMTP server through port 25. This option is only available on FortiGate units with a local disk.

To view the AutoSubmit list, go to AntiVirus > Quarantine > AutoSubmit.

Figure 273: Sample AutoSubmit list

AutoSubmit list has the following icons and features:

- **Create New**: Select to add a new file pattern to the AutoSubmit list.
- **File Pattern**: The current list of file patterns that will be automatically uploaded. Create a pattern by using ? or * wildcard characters. Enable the check box to enable all file patterns in the list.
- **Delete icon**: Select to remove the entry from the list.
- **Edit icon**: Select to edit the following information: File Pattern and Enable.

**Viewing the AutoSubmit list**

Configure the FortiGate unit to upload suspicious files automatically to Fortinet for analysis. Add file patterns to the AutoSubmit list using wildcard characters (* or ?). File patterns are applied for AutoSubmit regardless of file blocking settings.

Upload files to Fortinet based on status (blocked or heuristics), or submit individual files directly from the quarantined files list. The FortiGate unit uses encrypted email to autosubmit files to an SMTP server through port 25. This option is only available on FortiGate units with a local disk.

To view the AutoSubmit list, go to AntiVirus > Quarantine > AutoSubmit.

**Figure 273: Sample AutoSubmit list**

AutoSubmit list has the following icons and features:

- **Create New**: Select to add a new file pattern to the AutoSubmit list.
- **File Pattern**: The current list of file patterns that will be automatically uploaded. Create a pattern by using ? or * wildcard characters. Enable the check box to enable all file patterns in the list.
- **Delete icon**: Select to remove the entry from the list.
- **Edit icon**: Select to edit the following information: File Pattern and Enable.

**Configuring the AutoSubmit list**

To add a file pattern to the AutoSubmit list, go to AntiVirus > Quarantine > AutoSubmit.

**Figure 274: New File Pattern dialog box**

File Pattern: Enter the file pattern or file name to be upload automatically to Fortinet.

Enable: Select to enable the file pattern.
Configuring quarantine options

Go to AntiVirus > Quarantine > Config to set quarantine configuration options, including whether to quarantine blocked or infected files and from which service. Configure the time to live and file size values, and enable AutoSubmit settings.

Figure 275: Quarantine Configuration (FortiGate with local disk)

Note: To enable automatic uploading of the configured file patterns, go to AntiVirus > Quarantine > Config, select Enable AutoSubmit, and select Use File Pattern.

Figure 276: Quarantine Configuration (FortiAnalyzer from FortiGate with local disk)
Quarantine configuration has the following options:

**Options**
- **Quarantine Infected Files**: Select the protocols from which to quarantine infected files identified by antivirus scanning.
- **Quarantine Suspicious Files**: Select the protocols from which to quarantine suspicious files identified by heuristics.
- **Quarantine Blocked Files**: Select the protocols from which to quarantine blocked files identified by antivirus file blocking. The Quarantine Blocked Files option is not available for HTTP, FTP, or IM because a file name is blocked before downloading and cannot be quarantined.

**Age limit**
The time limit in hours for which to keep files in quarantine. The age limit is used to formulate the value in the TTL column of the quarantined files list. When the limit is reached, the TTL column displays EXP. and the file is deleted (although a record is maintained in the quarantined files list). Entering an age limit of 0 (zero) means files are stored on disk indefinitely, depending on low disk space action.

**Max filesize to quarantine**
The maximum size of quarantined files in MB. Setting the maximum file size too large may affect performance.

**Low disk space**
Select the action to take when the local disk is full: overwrite the oldest file or drop the newest file.

**FortiAnalyzer**
Select to enable storage of blocked and quarantined files on a FortiAnalyzer unit. See "Log&Report" on page 469 for more information about configuring a FortiAnalyzer unit.

**Enable AutoSubmit**
Enable AutoSubmit: enables the AutoSubmit feature. Select one or both of the options below.

- **Use file pattern**: Enables the automatic upload of files matching the file patterns in the AutoSubmit list.
- **Use file status**: Enables the automatic upload of quarantined files based on their status. Select either Heuristics or Block Pattern.
  - Heuristics is configurable through the CLI only. See "Antivirus CLI configuration" on page 409.

**Apply**
Select to save the configuration.

Note: NNTP options cannot be selected. Support will be added in the future.
Config

Config displays a list of the current viruses blocked by the FortiGate unit. Also configure file and email size limits, and grayware blocking.

Note: If virtual domains are enabled on the FortiGate unit, antivirus features are configured globally. To access these features, select Global Configuration on the main menu.

Viewing the virus list

The virus list displays an alphabetical list of the current FortiGuard virus definitions (also called AV definitions) installed on the FortiGate unit. The FortiGate unit uses the virus definitions to detect and remove viruses, worms, trojans, and other threats from content as it passes through the FortiGate unit. View the entire list or parts of the list by selecting the number or alphabet ranges.

To view the virus list, go to AntiVirus > Config.

The FortiGuard virus definitions list is updated every time the FortiGate unit receives a new version of the FortiGuard AV definitions.

The FortiGuard Center Virus Encyclopedia contains detailed descriptions of the viruses, worms, trojans, and other threats that can be detected and removed by your FortiGate unit using the information in the FortiGuard virus definitions.

Figure 278: Virus list (partial)

<table>
<thead>
<tr>
<th>A - Z</th>
<th>A - F</th>
<th>G - L</th>
<th>M - R</th>
<th>S - Z</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>10MBFears.p31</td>
<td>AV7M/Mixed-D.tr</td>
<td>AVFinder.A-1424</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ambient.A.tr</td>
<td>AVAlert.A-tr</td>
<td>AntiVirus.A-tr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AntiMcAfee.1</td>
<td>AntiXTC.tr</td>
<td>AntiMcOS.A-tr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arcor.166d</td>
<td>AVRCV250</td>
<td>AntiTr.tr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Autobat.O</td>
<td>BackDo0or</td>
<td>Backdoor.B026113</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backdoor.Castor</td>
<td>BackDo0or.Ob0ub.179</td>
<td>Backdoor.Nebus.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backdoor.Sub47.tr</td>
<td>BackDo0or.Ob0ub.2</td>
<td>Backdoor.Sub47.gen</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Beagle.C.mm</td>
<td>BASHKite.A</td>
<td>BeAT.O.tr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAT/SilentZ</td>
<td>BAT/Chatroot.AB.tr</td>
<td>BAT/Chatroot.08.C.tr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAT/PermStuff.tr</td>
<td>BAT/Formater.DL.tr</td>
<td>BAT/Pep.AB.tr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAT/Pep.O.tr</td>
<td>BAT/Pep.OB.612.tr</td>
<td>BAT/Pep.OB.585.tr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAT/Pep.2.tr</td>
<td>BAT/Pep.2.Z.tr</td>
<td>BAT/Pep.64.tr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAT/Perminute.B.tr</td>
<td>BAT/KillAV.AP.tr</td>
<td>BAT/KillAV.A-tr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAT/KillerAV.A-tr</td>
<td>BAT/KillerAV.B.tr</td>
<td>BAT/KillerAV.4.tr</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usually the FortiGuard AV definitions are updated automatically from the FortiGuard Distribution Network (FDN). Go to System > Maintenance > FortiGuard Center to configure automatic AV definition updates from the FDN.

You can also update the AV definitions manually from the system dashboard (go to System > Status).

Viewing the grayware list

Grayware programs are unsolicited commercial software programs that get installed on computers, often without the user’s consent or knowledge. Grayware programs are generally considered an annoyance, but these programs can cause system performance problems or be used for malicious ends.

The FortiGate unit scans for known grayware executable programs in each enabled category. The category list and contents are added or updated whenever the FortiGate unit receives a virus update package. New categories may be added at any time and will be loaded with the virus updates. By default, all new categories are disabled. Grayware is enabled in a protection profile when Virus Scan is enabled.
Grayware categories are populated with known executable files. Each time the FortiGate unit receives a virus and attack definitions update, the grayware categories and contents are updated.

**Note:** If virtual domains are enabled on the FortiGate unit, antivirus features are configured globally. To access these features, select **Global Configuration** on the main menu.

To view the grayware list, go to **AntiVirus > Config > Grayware**.

**Figure 279: Sample grayware options**

<table>
<thead>
<tr>
<th>Category</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware</td>
<td></td>
</tr>
<tr>
<td>BHO</td>
<td></td>
</tr>
<tr>
<td>Dial</td>
<td></td>
</tr>
<tr>
<td>Download</td>
<td></td>
</tr>
<tr>
<td>Game</td>
<td></td>
</tr>
<tr>
<td>HackerTool</td>
<td></td>
</tr>
<tr>
<td>Hijacker</td>
<td></td>
</tr>
<tr>
<td>Joke</td>
<td></td>
</tr>
<tr>
<td>Keylog</td>
<td></td>
</tr>
<tr>
<td>Mix</td>
<td></td>
</tr>
<tr>
<td>NMT</td>
<td></td>
</tr>
<tr>
<td>P2P</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td></td>
</tr>
<tr>
<td>RAT</td>
<td></td>
</tr>
<tr>
<td>Spy</td>
<td></td>
</tr>
<tr>
<td>Toolbar</td>
<td></td>
</tr>
</tbody>
</table>

Enabling a grayware category blocks all files listed in the category. The categories may change or expand when the FortiGate unit receives updates. You can choose to enable the following grayware categories:

- **Adware**
  - Block adware programs. Adware is usually embedded in freeware programs and causes ads to pop up whenever the program is opened or used.

- **BHO**
  - Block browser helper objects. BHOs are DLL files that are often installed as part of a software package so the software can control the behavior of Internet Explorer 4.x and later. Not all BHOs are malicious, but the potential exists to track surfing habits and gather other information.

- **Dial**
  - Block dialer programs. Dialers allow others to use the PC modem to call premium numbers or make long distance calls.

- **Download**
  - Block download programs. Download components are usually run at Windows startup and are designed to install or download other software, especially advertising and dial software.

- **Game**
  - Block games. Games are usually joke or nuisance games that you may want to block from network users.

- **HackerTool**
  - Block hacker tools.

- **Hijacker**
  - Block browser hijacking programs. Browser hijacking occurs when a ‘spyware’ type program changes web browser settings, including favorites or bookmarks, start pages, and menu options.

- **Joke**
  - Block joke programs. Joke programs can include custom cursors and programs that appear to affect the system.

- **Keylog**
  - Block keylogger programs. Keylogger programs can record every keystroke made on a keyboard including passwords, chat, and instant messages.
The optimize feature configures CPU settings to ensure efficient operation of the FortiGate unit for either antivirus scanning or straight throughput traffic. When optimize is set to antivirus, the FortiGate unit uses symmetric multiprocessing to spread the antivirus tasks to several CPUs, making scanning faster.

This feature is available on models numbered 1000 and higher.

For more information, see the Antivirus failopen and optimization Fortinet Knowledge Center article.

The FortiGate heuristic antivirus engine performs tests on files to detect virus-like behavior or known virus indicators. Heuristic scanning is performed last, after file blocking and virus scanning have found no matches. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results.

The heuristic engine is enabled by default to pass suspected files to the recipient and send a copy to quarantine. Once configured in the CLI, heuristic scanning is enabled in a protection profile when Virus Scan is enabled.

Use the heuristic command to change the heuristic scanning mode.
config antivirus quarantine

The quarantine command also allows configuration of heuristic related settings.
This feature is available on models numbered 200 and higher.

config antivirus service <service_name>

Use this command to configure how the FortiGate unit handles antivirus scanning of large files in HTTP, FTP, IM, POP3, IMAP, or SMTP traffic, and what ports the FortiGate unit scans for the service.
Intrusion Protection

The FortiGate Intrusion Prevention System (IPS) combines signature and anomaly intrusion detection and prevention with low latency and excellent reliability. IPS provides configuration access to the IPS options enabled when creating a firewall protection profile.

This section describes how to configure the FortiGate IPS settings. For detailed information about IPS, see the FortiGate Intrusion Protection System (IPS) Guide.

This section describes:
- About intrusion protection
- Predefined signatures
- Custom signatures
- Protocol Decoders
- Anomalies
- IPS CLI configuration

About intrusion protection

The FortiGate unit can record suspicious traffic in logs, can send alert email to system administrators, and can log, pass, drop, reset, or clear suspicious packets or sessions. Adjust some IPS anomaly thresholds to work best with the normal traffic on the protected networks. Create custom signatures to customize the FortiGate IPS for diverse network environments.

The FortiGate IPS matches network traffic against patterns contained in attack signatures. Attack signatures reliably protect your network from known attacks. Fortinet’s FortiGuard infrastructure ensures the rapid identification of new threats and the development of new attack signatures.

FortiGuard services are a valuable customer resource and include automatic updates of virus and IPS (attack) engines and definitions through the FortiGuard Distribution Network (FDN). The FortiGuard Center also provides the FortiGuard virus and attack encyclopedia and the FortiGuard Bulletin. Visit the Fortinet Knowledge Center for details and a link to the FortiGuard Center.

The connection between the FortiGate unit and FortiGuard is configured in System > Maintenance > FortiGuard Center. See “Configuring the FortiGate unit for FDN and FortiGuard services” on page 188 for more information.

Configure the FortiGate unit to check automatically for and download updated attack definition files containing the latest signatures, or download the updated attack definition file manually. Alternately, configure the FortiGate unit to allow push updates of updated attack definition files as soon as they are available from the FortiGuard Distribution Network.

When the FortiGate unit installs an updated attack definition file, it checks to see if the default configuration for any existing signatures has changed. If the default configuration has changed, the changes are preserved.
Create custom attack signatures for the FortiGate unit to use in addition to an extensive list of predefined attack signatures.

Whenever the IPS detects or prevents an attack, it generates an attack message. Configure the FortiGate unit to add the message to the attack log and send an alert email to administrators. Configure how often the FortiGate unit sends alert email. Reduce the number of log messages and alerts by disabling signatures for attacks to which the system is not vulnerable, for example, web attacks when there is no web server running.

Packet logging provides administrators with the ability to analyze packets for forensics and false positive detection.

For more information about FortiGate logging and alert email, see "Log&Report" on page 469.

**IPS settings and controls**

Configure the IPS using either the web-based manager or the CLI, then enable or disable all signatures or all anomalies in individual firewall protection profiles.

**Note:** If virtual domains are enabled on the FortiGate unit, the IPS is configured globally. To access the IPS, select **Global Configuration** on the main menu.

Table 35 describes the IPS settings and where to configure and access them.

**Table 35: Protection Profile IPS and IPS configuration**

<table>
<thead>
<tr>
<th>Protection Profile IPS options</th>
<th>IPS setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Signature</td>
<td>Intrusion Protection &gt; Signature</td>
</tr>
<tr>
<td>Enable or disable IPS signatures by severity level.</td>
<td>View and configure a list of predefined signatures. Create custom signatures based on the network requirements. Configure protocol decoders.</td>
</tr>
<tr>
<td>IPS Anomaly</td>
<td>Intrusion Protection &gt; Anomaly</td>
</tr>
<tr>
<td>Enable or disable IPS anomalies by severity level.</td>
<td>View and configure a list of predefined anomalies.</td>
</tr>
<tr>
<td>Log Intrusions</td>
<td>Intrusion Protection &gt; Anomaly &gt; [individual anomaly]</td>
</tr>
<tr>
<td>Enable logging of all signature and anomaly intrusions.</td>
<td>Enable logging for each signature. Enable packet logging for each signature or anomaly.</td>
</tr>
</tbody>
</table>

To access protection profile IPS options, go to **Firewall > Protection Profile**, select Edit or Create New, and select IPS.

**When to use IPS**

IPS is best for large networks or for networks protecting highly sensitive information. Using IPS effectively requires monitoring and analysis of the attack logs to determine the nature and threat level of an attack. An administrator can adjust the threshold levels to ensure a balance between performance and intrusion prevention.
Small businesses and home offices without network administrators may be overrun with attack log messages and not have the networking background required to configure the thresholds and other IPS settings.

In addition, the other protection features in the FortiGate unit, such as antivirus (including grayware), spam filters, and web filters offer excellent protection for all networks.

Predefined signatures

By default, not all signatures are enabled. But logging of all signatures is enabled. Check the default settings to ensure they meet the requirements of the network traffic.

Disabling unneeded signatures can improve system performance and reduce the number of log messages and alert email messages the IPS generates. For example, the IPS detects a large number of web server attacks. If access to a web server behind the FortiGate unit is not provided, disable all web server attack signatures.

**Note:** By allowing your IPS signature settings to run on default, you may be slowing down the overall performance of the FortiGate unit. By fine tuning the predefined signature and logging setting, you can ensure maximum performance as well as maximum protection. See “Fine tuning IPS predefined signatures for enhanced system performance” on page 416.

Viewing the predefined signature list

Enable or disable and configure the settings for individual predefined signatures from the predefined signature list.

**Note:** If virtual domains are enabled on the FortiGate unit, the IPS is configured globally. To access the IPS, select **Global Configuration** on the main menu.

To view the predefined signature list, go to **Intrusion Protection > Signature > Predefined**. You can also use filters to display the signatures you want to view. For details, see “Using display filters” on page 415.
Predefined signatures

Table 36 describes each possible action to take for predefined signatures, custom signatures and anomalies.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>When a packet triggers a signature, the FortiGate unit generates an alert and allows the packet through the firewall without further action. If logging is disabled and action is set to Pass, the signature is effectively disabled.</td>
</tr>
<tr>
<td>Drop</td>
<td>When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The firewall session is not touched. Fortinet recommends using an action other than Drop for TCP connection based attacks.</td>
</tr>
<tr>
<td>Reset</td>
<td>When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to both the client and the server and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established, it acts as Clear Session.</td>
</tr>
</tbody>
</table>
Using display filters

By default, all the predefined signatures are displayed. You can apply filters to display only the signatures you want to view. For example, if you want to view the enabled signatures only, you can use the Enable or Disable status filter. See “Adding filters to web-based manager lists” on page 43.

To apply filters to the predefined signature list

1. Go to Intrusion Protection > Predefined.
2. Select the filter icon beside the column name in the signature table.
3. In the Edit Filters dialog box, specify the filtering criteria and enable the filter.
   If you use severity level filter, you can select one or multiple severity levels.
4. Select OK.

Configuring predefined signatures

For each signature, configure the action the FortiGate IPS takes when it detects an attack. The FortiGate IPS can pass, drop, reset or clear packets or sessions. Enable or disable packet logging. Select a severity level to be applied to the signature.

You can also specify the traffic by source and destination addresses to be exempted from IPS filtering.
Fine tuning IPS predefined signatures for enhanced system performance

By default, the FortiGate unit will have most of the predefined signatures enabled and will log all of them. To meet your specific network requirements, you need to fine tune the signature settings.

By fine tuning the signatures and log settings you can provide the best protection available but also free up valuable FortiGate resources. Fine tuning allows you to turn off features that you are not using. By turning off signatures and logs that you do not use, you allow the FortiGate unit to perform tasks faster thus improving overall system performance.

Not all systems require you to scan for all signatures of the IPS suite all the time. For example, if you have a FortiGate unit that is controlling computers that only have access to an internal database and do not have access to the internet or email, there is no point having the Fortigate unit scanning for certain types of signatures such as email, IM, and P2P.

By telling the FortiGate unit not to look for these signatures, you will maintain a high level of security and increase overall performance.

You should also review exactly how you use the information provided by the logging feature. If you find that you do not review the information, it is best to turn off the logging feature. Logging is best used to provide actionable intelligence.
To disable a signature

1. Go to Intrusion Protection > Signatures > Predefined.
2. Clear the Enable box for the signatures you want to disable.

To turn off logging for a signature

1. Go to Intrusion Protection > Signatures > Predefined.
2. Select the Configure icon on the right hand side of the signature you want to change.
3. Clear the Logging check box.

Custom signatures

Custom signatures provide the power and flexibility to customize the FortiGate IPS for diverse network environments. The FortiGate predefined signatures cover common attacks. If an unusual or specialized application or an uncommon platform is being used, add custom signatures based on the security alerts released by the application and platform vendors.

You can also create custom signatures to help you block P2P protocols.

For more details about custom signatures, see the FortiGate Intrusion Protection System (IPS) Guide.

Note: If virtual domains are enabled on the FortiGate unit, the IPS is configured globally. To access the IPS, select Global Configuration on the main menu.

Viewing the custom signature list

To view the custom signature list, go to Intrusion Protection > Signature > Custom.

Figure 282: The custom signature list

View custom signatures with severity

Select filters then select Go to view only those custom signatures that match the filter criteria. Sort criteria can be <=, =, >= to All, Information, Low, Medium, High, or Critical.

Create New

Select to create a new custom signature.

Clear all custom signatures icon

Remove all the custom signatures.

Reset to recommended settings icon

Reset all the custom signatures to the recommended settings.
Custom signatures

Use custom signatures to block or allow specific traffic. For example, to block traffic containing pornography, add custom signatures similar to the following:

F-SBID (--protocol tcp; --flow established; --content "nude cheerleader"; --no_case)

When adding the signature, set action to Drop Session.

For more information on custom signature syntax, see the FortiGate Intrusion Protection System (IPS) Guide.

Note: Custom signatures are an advanced feature. This document assumes the user has previous experience creating intrusion detection signatures.

To create a custom signature, go to Intrusion Protection > Signature > Custom.

Figure 283: Edit Custom Signature

Name The custom signature name.
Enable The status of each custom signature. A check mark in the box indicates the signature is enabled.
Logging The logging status of each custom signature. A check mark in the box indicates logging is enabled for the custom signature.
Action The action set for each custom signature. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session. If logging is enabled, the action appears in the status field of the log message generated by the signature. See Table 36 for descriptions of the actions.
Severity The severity level set for each custom signature. Severity level can be Information, Low, Medium, High, or Critical. Severity level is set for individual signatures.
Delete icon Select to delete the custom signature.
Edit icon Select to edit the following information: Name, Signature, Action, Packet Log, and Severity.

Creating custom signatures

Use custom signatures to block or allow specific traffic. For example, to block traffic containing pornography, add custom signatures similar to the following:

F-SBID (--protocol tcp; --flow established; --content "nude cheerleader"; --no_case)

When adding the signature, set action to Drop Session.

For more information on custom signature syntax, see the FortiGate Intrusion Protection System (IPS) Guide.

Note: Custom signatures are an advanced feature. This document assumes the user has previous experience creating intrusion detection signatures.

To create a custom signature, go to Intrusion Protection > Signature > Custom.

Figure 283: Edit Custom Signature

Name Enter a name for the custom signature.
Signature Enter the custom signature. For more information about custom signature syntax, see “Custom signature syntax” in the FortiGate Intrusion Protection System (IPS) Guide.
Action Select an action from the list. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Pass Session, or Clear Session. See Table 36 for descriptions of the actions.
Packet Log Enable packet logging.
Severity Select a severity level from the dropdown list. Severity level can be Information, Low, Medium, High, or Critical. Severity level is set for individual signatures.
Protocol Decoders

The FortiGate IPS uses protocol decoders to identify the abnormal traffic patterns that do not meet the protocol requirements and standards. For example, the HTTP decoder monitors the HTTP traffic to identify any HTTP packets that do not meet the HTTP protocol standards.

On the Intrusion Protection > Signature > Protocol Decoder page, you can view the decoders and configure the port numbers that the protocol decoders monitor. To configure other decoder settings, such as action and packet logging, you must go to Intrusion Protection > Signature > Predefined.

**Note:** If virtual domains are enabled on the FortiGate unit, the IPS is configured globally. To access the IPS, select Global Configuration on the main menu.

Viewing the protocol decoder list

To view the decoder list, go to Intrusion Protection > Signature > Protocol Decoder.

Figure 284: Portion of the protocol decoder list

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back Orifice</td>
<td>Auto</td>
</tr>
<tr>
<td>DCE RPC</td>
<td>135, 1026</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
</tr>
<tr>
<td>FTP</td>
<td>21</td>
</tr>
<tr>
<td>H323</td>
<td>1720</td>
</tr>
<tr>
<td>HTTP</td>
<td>Auto</td>
</tr>
<tr>
<td>Instant Messaging</td>
<td>Auto</td>
</tr>
<tr>
<td>IMAP</td>
<td>143</td>
</tr>
<tr>
<td>LDAP</td>
<td>389</td>
</tr>
<tr>
<td>MSSQL</td>
<td>1433</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>139, 445</td>
</tr>
<tr>
<td>Peer-to-Peer</td>
<td>Auto</td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
</tr>
<tr>
<td>Protocol (L3/4 Analyser)</td>
<td>Auto</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1012, 1013</td>
</tr>
<tr>
<td>Sun RPC</td>
<td>111, 32771</td>
</tr>
<tr>
<td>SIP</td>
<td>5060</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
</tr>
<tr>
<td>SNMP</td>
<td>161, 162</td>
</tr>
<tr>
<td>SSH</td>
<td>Auto</td>
</tr>
<tr>
<td>TCP Reassembler</td>
<td>Auto</td>
</tr>
<tr>
<td>TFN DoS</td>
<td>Auto</td>
</tr>
</tbody>
</table>

- **Name**: The protocol decoder name.
- **Ports**: The port number or numbers the decoder monitors.
- **Configure icon**: Click to modify the signature port settings. You cannot modify settings of some decoders used by the system.

Configuring IPS protocol decoders

On the Protocol Decoders page, you can modify the port numbers that the decoders monitor. You cannot modify port settings of some decoders used by the system.

On the Intrusion Protection > Signature > Predefined page, you can modify the decoders’ other settings, such as action and packet logging.
To configure the protocol decoder port settings

1. Go to **Intrusion Protection > Signature > Protocol Decoder**.
2. Select the Configure icon for the decoder.
3. Modify the port number or port numbers as required.
4. Select OK.

**Upgrading IPS protocol decoder list**

IPS protocol decoders are included in the IPS upgrade package available through the FortiGuard Distribution Network (FDN). There is no need to wait for firmware upgrades. The IPS upgrade package will keep the IPS decoder list up to date with new threats such as the latest versions of existing IM/P2P as well as new applications.

**Anomalies**

The FortiGate IPS uses anomaly detection to identify network traffic that does not fit known or common traffic patterns and behavior. For example, if one host keep sending a number of session within a second, the destination will experience traffic flooding. In this case, the FortiGate IPS uses session thresholds to prevent flooding.

The FortiGate IPS identifies the four statistical anomaly types for the TCP, UDP, and ICMP protocols.

- **Flooding**: If the number of sessions targeting a single destination in one second is over a specified threshold, the destination is experiencing flooding.
- **Scan**: If the number of sessions from a single source in one second is over a specified threshold, the source is scanning.
- **Source session limit**: If the number of concurrent sessions from a single source is over a specified threshold, the source session limit is reached.
- **Destination session limit**: If the number of concurrent sessions to a single destination is over a specified threshold, the destination session limit is reached.

Enable or disable logging for each traffic anomaly, and configure the IPS action in response to detecting an anomaly. In many cases, the thresholds the anomaly uses to detect traffic patterns that could represent an attack are configurable.

**Note:** It is important to know normal and expected network traffic before changing the default anomaly thresholds. Setting the thresholds too low could cause false positives, and setting the thresholds too high could miss some attacks.

Use the CLI to configure session control based on source and destination network address.

The traffic anomaly detection list can be updated only when the FortiGate firmware image is upgraded.

**Note:** If virtual domains are enabled on the FortiGate unit, the IPS is configured globally. To access the IPS, select **Global Configuration** on the main menu.
Viewing the traffic anomaly list

To view the anomaly list, go to Intrusion Protection > Anomaly.

Figure 285: A portion of the traffic anomaly list

<table>
<thead>
<tr>
<th>View traffic anomalies with severity</th>
<th>&lt;=</th>
<th>All</th>
<th>Action</th>
<th>&gt;=</th>
<th>All</th>
<th>Go</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>✔</td>
<td>✔</td>
<td>Pass</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Logging</td>
<td>✔</td>
<td>✔</td>
<td>Critical</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>icmp_dst_session</td>
<td>✔</td>
<td>✔</td>
<td>Pass</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>icmp_flood</td>
<td>✔</td>
<td>✔</td>
<td>Critical</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>icmp_land</td>
<td>✔</td>
<td>✔</td>
<td>Drop</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>icmp_spo_session</td>
<td>✔</td>
<td>✔</td>
<td>Pass</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>icmp_sweep</td>
<td>✔</td>
<td>✔</td>
<td>Clear Session</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>ip_land</td>
<td>✔</td>
<td>✔</td>
<td>Pass</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

View traffic anomalies with severity: Select filters then select Go to view only those anomalies that match the filter criteria. Sort criteria can be <=, =, >= to All, Information, Low, Medium, High, or Critical.

Name: The traffic anomaly name.
Enable: The status of the traffic anomaly. A check mark in the box indicates the anomaly signature is enabled.
Logging: The logging status for each traffic anomaly. A check mark in the box indicates logging is enabled for the anomaly.
Action: The action set for each traffic anomaly. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session. If logging is enabled, the action appears in the status field of the log message generated by the Anomaly. See Table 36 for descriptions of the actions.
Severity: The severity level set for each traffic anomaly. Severity level can be Information, Low, Medium, High, or Critical. Severity level is set for individual anomalies.
Edit icon: Select to edit the following information: Action, Severity, and Threshold.
Reset icon: The Reset icon is displayed only if an anomaly has been modified. Use the Reset icon to restore modified settings to the recommended values.

Configuring IPS traffic anomalies

Each IPS traffic anomaly is preset with a recommended configuration. Use the recommended configurations, or modify the recommended configurations to meet the needs of your network.

To configure IPS traffic anomalies, go to Intrusion Protection > Anomaly.

Figure 286: Edit IPS Traffic Anomaly: icmp_dst_session
IPS CLI configuration

This section describes the CLI commands that extend features available through the web-based manager. For complete descriptions and examples of how to enable additional features through CLI commands, see the FortiGate CLI Reference.

system autoupdate ips

When the IPS is updated, user-modified settings are retained. If recommended IPS signature settings have not been modified, and the updated settings are different, signature settings will be set according to accept-recommended-settings.

ips global fail-open

If for any reason the IPS should cease to function, it will fail open by default. This means crucial network traffic will not be blocked, and the firewall will continue to operate while the problem is being resolved.

ips global ip_protocol

Save system resources by restricting IPS processing to only those services allowed by firewall policies.

ips global socket-size

Set the size of the IPS buffer.

(config ips anomaly) config limit

Access the config limit subcommand using the config ips anomaly <name_str> command. Use this command for session control based on source and destination network address. This command is available for tcp_src_session, tcp_dst_session, icmp_src_session, icmp_dst_session, udp_src_session, udp_dst_session.
Web Filter

The three main sections of the web filtering function, the Web Filter Content Block, the URL Filter, and the FortiGuard Web filter, interact with each other in such a way as to provide maximum control and protection for the Internet users.

This section describes:
- Order of web filtering
- How web filtering works
- Web filter controls
- Content block
- URL filter
- FortiGuard - Web Filter

Order of web filtering

Web filters are applied in a specific order:

1. URL Exempt (Web Exempt List)
2. URL Block (Web URL Block)
3. URL Block (Web Pattern Block)
4. FortiGuard Web Filtering (Also called Category Block)
5. Content Block (Web Content Block)
6. Script Filter (Web Script Filter)
7. Antivirus scanning

The URL filter list is processed in order from top to bottom. (In FortiOS v2.80 the URL filter is processed as an unordered list.) An exempt match stops all further checking including AV scanning. An allow match exits the URL filter list and checks the other web filters.

Local ratings are checked prior to other FortiGuard Web Filtering categories.

The FortiGate unit applies the rules in this order and failure to comply with a rule will automatically block a site despite what the setting for later filters might be.

How web filtering works

The following information shows how the filters interact with each other and how to use them to your advantage.

The first section, the URL exempt and block filters, will allow you to decide what action to take for specific addresses. For example, if you want to exempt www.google.com from being scanned, you can add it to the URL exempt list. Then no web filtering or virus scanning will be taken to this web site.
If you have blocked a pattern but want certain users to have access to URLs within that pattern, you can use the Override within the FortiGuard Web Filter. This will allow you to specify which users have access to which blocked URLs and how long they have that access. For example, you want User1 to be able to access www.fakeland.com for 1 hour. You can use this section to set up the exemption. Any user listed in an override must fill out an online authentication form before the FortiGuard unit will grant access to the blocked URL.

FortiGuard Web Filter also lets you create local categories to block groups of URLs. Once you have created the category, you can use the local rating to add specific sites to the local category you have created. You then use the Firewall > Protection Profile to tell the FortiGuard Unit what action to take with the Local category. The local ratings overwrite the FortiGuard ratings.

Finally the FortiGuard unit applies script filtering for ActiveX, Cookie, and Java applet, which can be configured in Firewall > Protection Profile > Web Filtering.

Once you have finished configuring all of these settings, you still have to turn them all on in the Firewall > Protection Profile > Web filtering and Firewall > Protection Profile > FortiGuard Web Filtering. By enabling them here, you are telling the FortiGate unit to start using the filters as you have configured them.

This section describes how to configure web filtering options. Web filtering functions must be enabled in the active protection profile for the corresponding settings in this section to have any effect.

### Web filter controls

As a general rule you go to Web Filter to configure the web filtering settings and to enable the filters for use in a protection profile. To actually activate the enabled filters you go to Firewall > Protection Profile.

**Note:** Enabled means that the filter will be used when you turn on web filtering. It does not mean that the filter is turned on. To turn on all enabled filters you must go to Firewall > Protection Profile.

FortiGuard - Web Filter is described in detail in “FortiGuard Web Filtering options” on page 334. Rating corrections as well as suggesting ratings for new pages can be submitted on the FortiGuard Center web page. Visit the Fortinet Knowledge Center for details and a link to the FortiGuard Center.

The following tables compare web filtering options in protection profiles and the web filter menu.

<table>
<thead>
<tr>
<th>Protection Profile web filtering options</th>
<th>Web Filter setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Content Block</td>
<td>Web Filter &gt; Content Block</td>
</tr>
<tr>
<td>Enable or disable web page blocking based on the banned words and patterns in the content block list for HTTP traffic.</td>
<td>Add words and patterns to block web pages containing those words or patterns.</td>
</tr>
</tbody>
</table>
### Table 38: Web filter and Protection Profile web URL filtering configuration

<table>
<thead>
<tr>
<th>Protection Profile web filtering options</th>
<th>Web Filter setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web URL Filter</td>
<td>Web Filter &gt; URL Filter</td>
</tr>
<tr>
<td>Enable or disable web page filtering for HTTP traffic based on the URL filter list.</td>
<td>Add URLs and URL patterns to exempt or block web pages from specific sources.</td>
</tr>
</tbody>
</table>

### Table 39: Web filter and Protection Profile web script filtering and download configuration

<table>
<thead>
<tr>
<th>Protection Profile web filtering options</th>
<th>Web Filter setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active X Filter, Cookie Filter, Java Applet Filter</td>
<td>n/a</td>
</tr>
<tr>
<td>Enable or disable blocking scripts from web pages for HTTP traffic.</td>
<td>n/a</td>
</tr>
<tr>
<td>Web resume Download Block</td>
<td>n/a</td>
</tr>
<tr>
<td>Enable to block downloading the remainder of a file that has already been partially downloaded. Enabling this option prevents the unintentional download of virus files, but can cause download interruptions.</td>
<td>n/a</td>
</tr>
</tbody>
</table>

### Table 40: Web filter and Protection Profile web category filtering configuration

<table>
<thead>
<tr>
<th>Protection Profile web filtering options</th>
<th>Web Filter setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable FortiGuard Web Filtering (HTTP only).</td>
<td>FortiGuard Web Filter &gt; Configuration</td>
</tr>
<tr>
<td>Enable FortiGuard Web Filtering Overrides (HTTP only).</td>
<td>FortiGuard Web Filtering &gt; Overrides</td>
</tr>
<tr>
<td>Provide details for blocked HTTP 4xx and 5xx errors (HTTP only.)</td>
<td>FortiGuard Web Filtering &gt; Configuration</td>
</tr>
<tr>
<td>Rate images by URL (Blocked images will be replaced with blanks) (HTTP only).</td>
<td>FortiGuard Web Filtering &gt; Overrides</td>
</tr>
<tr>
<td>Allow web sites when a rating error occurs (HTTP only).</td>
<td>FortiGuard Web Filtering &gt; Configuration</td>
</tr>
<tr>
<td>Strict Blocking (HTTP only)</td>
<td>FortiGuard Web Filtering &gt; Overrides</td>
</tr>
<tr>
<td>Category / Action</td>
<td>FortiGuard Web Filtering &gt; Configuration</td>
</tr>
<tr>
<td>FortiGuard Web Filtering service provides many categories by which to filter web traffic. Set the action to take on web pages for each category. Choose from allow, block, log, or allow override.</td>
<td>FortiGuard Web Filtering &gt; Overrides</td>
</tr>
<tr>
<td>Local Categories can be configured to best suit local requirements.</td>
<td>FortiGuard Web Filtering &gt; Local Categories</td>
</tr>
<tr>
<td>Classification/Action</td>
<td>FortiGuard Web Filtering &gt; Local Categories</td>
</tr>
<tr>
<td>When selected, users can access web sites that provide content cache, and provide searches for image, audio, and video files. Choose from allow, block, log, or allow override.</td>
<td>FortiGuard Web Filtering &gt; Local Categories</td>
</tr>
</tbody>
</table>
To access protection profile web filter options

1. Go to **Firewall > Protection Profile**.
2. Select edit or Create New.
3. Select Web Filtering or Web Category Filtering.

**Note:** If virtual domains are enabled on the FortiGate unit, web filtering features are configured globally. To access these features, select **Global Configuration** on the main menu.

### Content block

Control web content by blocking specific words or patterns. If enabled in the protection profile, the FortiGate unit searches for words or patterns in on requested web pages. If matches are found, values assigned to the words are totalled. If a user-defined threshold value is exceeded, the web page is blocked.

Use Perl regular expressions or wildcards to add banned word patterns to the list.

**Note:** Perl regular expression patterns are case sensitive for Web Filter content block. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` blocks all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

### Viewing the web content block list catalog

You can add multiple web content block lists and then select the best web content block list for each protection profile. To view the web content block list catalog, go to **Web Filter > Content Block**. To view any individual web content block list, select the edit icon for the list you want to see.

**Figure 287:** Sample web content block list catalog

<table>
<thead>
<tr>
<th>Name</th>
<th># Entries</th>
<th>Profiles</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>inappropriate_words</td>
<td>5</td>
<td>web</td>
<td></td>
</tr>
<tr>
<td>other_bad_things</td>
<td>4</td>
<td>web</td>
<td>miss restricted words</td>
</tr>
</tbody>
</table>

The web content block list catalogue has the following icons and features:

- **Add** To add a new list to the catalog, enter a name and select Add. New lists are empty by default.
- **Name** The available web content block lists.
- **# Entries** The number of content patterns in each web content block list.
- **Profiles** The protection profiles each web content block list has been applied to.
- **Comment** Optional description of each web content block list. The comment text must be less than 63 characters long. Otherwise, it will be truncated. Spaces will also be replaced by the plus sign (+).
- **Delete icon** Select to remove the web content block list from the catalog. The delete icon is only available if the web content block list is not selected in any protection profiles.
- **Edit icon** Select to edit the web content block list, list name, or list comment.
Select web content block lists in protection profiles. For more information, see “Web filtering options” on page 333.

Creating a new web content block list

To add a web content block list to the web content block list catalog

1. Go to Web Filter > Content Block.
2. Select Create New.

Figure 288: New Web Content Block list dialog box

Viewing the web content block list

With web content block enabled, every requested web page is checked against the content block list. The score value of each pattern appearing on the page is added, and if the total is greater than the threshold value set in the protection profile, the page is blocked. The score for a pattern is applied only once even if it appears on the page multiple times.

To view the web content block list

1. Go to Web Filter > Content Block.
2. Select the edit icon of the web content block list you want to view.

Figure 289: Sample web content block list

Note: Enable Web Filtering > Web Content Block in a firewall Protection Profile to activate the content block settings.

The web content block list has the following icons and features:

- **Name**: Web content block list name. To change the name, edit text in the name field and select OK.
- **Comment**: Optional comment. To add or edit comment, enter text in comment field and select OK.
- **Create new**: Select to add a pattern to the web content block list.
Configuring the web content block list

Web content patterns can be one word or a text string up to 80 characters long. The maximum number of banned words in the list is 5000.

To add or edit a content block pattern

1. Go to Web Filter > Content Block.
2. Select Create New
   or
3. Select the edit icon of the web content block list you want to view.

**Figure 290: New content block pattern**

| **Banned Word** | Enter the content block pattern. For a single word, the FortiGate checks all web pages for that word. For a phrase, the FortiGate checks all web pages for any word in the phrase. For a phrase in quotation marks, the FortiGate unit checks all web pages for the entire phrase. |
| **Pattern Type** | Select a pattern type from the dropdown list: Wildcard or regular Expression. |
| **Language** | Select a language from the dropdown list. |
| **Score** | Enter a score for the pattern. |
| **Enable** | Select to enable the pattern. |
Viewing the web content exempt list catalog

You can add multiple web content exempt lists and then select the best web content exempt list for each protection profile.

To view the web content block list catalog
- Go to Web Filter > Content Block > Web Content Exempt.

To view any individual web content exempt list
- Select the edit icon for the list you want to see.

Figure 291: Sample web content exempt list catalog

The web content exempt list catalogue has the following icons and features:

Add
To add a new list to the catalog, enter a name and select Add. New lists are empty by default.

Name
The available web content block lists.

# Entries
The number of content patterns in each web content block list.

Profiles
The protection profiles each web content block list has been applied to.

Comment
Optional description of each web content block list.

Delete icon
Select to remove the web content block list from the catalog. The delete icon is only available if the web content block list is not selected in any protection profiles.

Edit icon
Select to edit the web content block list, list name, or list comment.

Select web content block lists in protection profiles. For more information, see “Web filtering options” on page 333.

Creating a new web content exempt list

To add a web content exempt list to the web content exempt list catalog

1. Go to Web Filter > Content Block > Web Content Exempt.
2. Select Create New.

Figure 292: New Web Content Exempt list dialog box

Name
Enter the name of the new list.

Comment
Enter a comment to describe the list, if required.
Viewing the web content exempt list

Web content exempt allows overriding of the web content block feature. If any patterns defined in the web content exempt list appear on a web page, the page will not be blocked even if the web content block feature would otherwise block it.

To view the web content exempt list

1. Go to Web Filter > Content Block > Web Content Exempt.
2. Select the edit icon of the web content block list you want to view.

Figure 293: Sample web content exempt list

The web content exempt list has the following icons and features:

- **Name**: Web content exempt list name. To change the name, edit text in the name field and select OK.
- **Comment**: Optional comment. To add or edit comment, enter text in comment field and select OK.
- **Create new**: Select to add a pattern to the web content exempt list.
- **Total**: The number of patterns in the web content exempt list.
- **Page up icon**: Select to view the previous page.
- **Page down icon**: Select to view the next page.
- **Remove All Entries icon**: Select to clear the table.
- **Pattern**: The current list of patterns. Select the check box to enable all the patterns in the list.
- **Pattern type**: The pattern type used in the pattern list entry. Choose from wildcard or regular expression. See "Using Perl regular expressions" on page 455.
- **Language**: The character set to which the pattern belongs: Simplified Chinese, Traditional Chinese, French, Japanese, Korean, Thai, or Western.
- **Delete icon**: Select to delete an entry from the list.
- **Edit icon**: Select to edit the following information: Pattern, Pattern Type, Language, and Enable.

**Note**: Enable Web Filtering > Web Content Exempt in a firewall Protection Profile to activate the content exempt settings.
Configuring the web content exempt list

Web content patterns can be one word or a text string up to 80 characters long. The maximum number of banned words in the list is 5000.

To add or edit a content block pattern

1. Go to Web Filter > Content Exempt.
2. Select create New.
   or
3. Select the edit icon of the web content block pattern you want to view.

Figure 294: New content exempt pattern

<table>
<thead>
<tr>
<th>Pattern Word</th>
<th>Enter the content exempt pattern. For a single word, the FortiGate checks all web pages for that word. For a phrase, the FortiGate checks all web pages for any word in the phrase. For a phrase in quotation marks, the FortiGate unit checks all web pages for the entire phrase.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern Type</td>
<td>Select a pattern type from the dropdown list: Wildcard or regular Expression.</td>
</tr>
<tr>
<td>Language</td>
<td>Select a language from the dropdown list.</td>
</tr>
<tr>
<td>Enable</td>
<td>Select to enable the pattern.</td>
</tr>
</tbody>
</table>

URL filter

Allow or block access to specific URLs by adding them to the URL filter list. Add patterns using text and regular expressions (or wildcard characters) to allow or block URLs. The FortiGate unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message instead.

Note: Enable Web filtering > Web URL Filter in a firewall Protection Profile to activate the URL filter settings.

Note: URL blocking does not block access to other services that users can access with a web browser. For example, URL blocking does not block access to ftp://ftp.example.com. Instead, use firewall policies to deny FTP connections.

Viewing the URL filter list catalog

You can add multiple URL filter lists and then select the best URL filter list for each protection profile.

To view the URL filter list catalog

• Go to Web Filter > URL Filter.
To view any individual URL filter list

1. Go to Web Filter > URL Filter.
2. Select the edit icon for the list you want to see.

Figure 295: Sample URL filter list catalog

The URL filter list catalogue has the following icons and features:

- **Add**: To add a new list to the catalog, enter a name and select Add. New lists are empty by default.
- **Name**: The available URL filter lists.
- **# Entries**: The number of URL patterns in each URL filter list.
- **Profiles**: The protection profiles each URL filter list has been applied to.
- **Comment**: Optional description of each URL filter list.
- **Delete icon**: Select to remove the URL filter list from the catalog. The delete icon is only available if the URL filter list is not selected in any protection profiles.
- **Edit icon**: Select to edit the URL filter list, list name, or list comment.

Select URL filter lists in protection profiles. For more information, see “Web filtering options” on page 333.

Creating a new URL filter list

To add a URL filter list to the URL filter list catalog

1. Go to Web Filter > URL Filter.
2. Select Create New.

Figure 296: New URL Filter list dialog box

- **Name**: Enter the name of the new list.
- **Comment**: Enter a comment to describe the list, if required.

Viewing the URL filter list

Add specific URLs to block or exempt. Add the following items to the URL filter list:
- complete URLs
- IP addresses
- partial URLs to allow or block all sub-domains
To view the URL filter list
1. Go to Web Filter > URL Filter.
2. Select the edit icon of the URL filter list you want to view.

Figure 297: URL filter list

The URL filter list has the following icons and features:

- **Name**: URL filter list name. To change the name, edit text in the name field and select OK.
- **Comment**: Optional comment. To add or edit comment, enter text in comment field and select OK.
- **Create New**: Select to add a URL to the URL block list.
- **Page up icon**: Select to view the previous page.
- **Page down icon**: Select to view the next page.
- **Clear All URL Filters icon**: Select to clear the table.
- **URL**: The current list of blocked/exempt URLs. Select the check box to enable all the URLs in the list.
- **Type**: The type of URL: Simple or Regex (regular expression).
- **Action**: The action taken when the URL matches: Allow, Block, or Exempt. An allow match exits the URL filter list and checks the other web filters. An exempt match stops all further checking including AV scanning. A block match blocks the URL and no further checking will be done.
- **Delete icon**: Select to remove an entry from the list.
- **Edit icon**: Select to edit the following information: URL, Type, Action, and Enable.
- **Move icon**: Select to open the Move URL Filter dialog box.

### Configuring the URL filter list

The URL filter list can have up to 5000 entries.

**Note**: Type a top-level domain suffix (for example, “com” without the leading period) to block access to all URLs with this suffix.

### To add a URL to the URL filter list
1. Go to Web Filter > URL Filter.
2. Select Create New.
Type in a URL or IP address.

Select the type of expression.

Select the action to be taken.

Select the Enable check box.

Select OK.

**Figure 298: New URL Filter**

<table>
<thead>
<tr>
<th>URL</th>
<th>Type</th>
<th>Action</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**URL**
Enter the URL. Do not include http://

**Type**
Select a type from the dropdown list: Simple or Regex (regular expression).

**Action**
Select an action from the dropdown list: Allow, Block, or Exempt.

An allow match exits the URL filter list and checks the other web filters.

An exempt match stops all further checking including AV scanning.

A block match blocks the URL and no further checking will be done.

**Enable**
Select to enable the URL.

Type a top-level URL or IP address to control access to all pages on a web site. For example, www.example.com or 192.168.144.155 controls access to all pages at this web site.

Enter a top-level URL followed by the path and filename to control access to a single page on a web site. For example, www.example.com/news.html or 192.168.144.155/news.html controls the news page on this web site.

To control access to all pages with a URL that ends with example.com, add example.com to the filter list. For example, adding example.com controls access to www.example.com, mail.example.com, www.finance.example.com, and so on.

Control access to all URLs that match patterns created using text and regular expressions (or wildcard characters). For example, example.* matches example.com, example.org, example.net and so on.

FortiGate web pattern blocking supports standard regular expressions.

**Note:** URLs with an action set to exempt are not scanned for viruses. If users on the network download files through the FortiGate unit from trusted websites, add the URL of this website to the URL filter list with an action set to exempt so the FortiGate unit does not virus scan files downloaded from this URL.

**Note:** Enable Web filtering > Web URL Filter in a firewall Protection Profile to activate the web URL filter settings.
Moving URLs in the URL filter list

To make the URL filter list easier to use, the entries can be moved to different positions in the list.

To move a URL in the URL filter list

1. Go to Web Filter > URL Filter.
2. Select the Edit icon for the URL list.
3. Drag and drop a URL or select the Move icon to the right of the URL to be moved.
4. Specify the location for the URL.
5. Select OK.

Figure 299: Move URL Filter

<table>
<thead>
<tr>
<th>URL</th>
<th>Move to</th>
</tr>
</thead>
<tbody>
<tr>
<td>fortinet.com</td>
<td>Before</td>
</tr>
</tbody>
</table>

Move to:
Select the location in the list to place the URL.

(URL)
Enter the URL before or after which the new URL is to be located in the list.

FortiGuard - Web Filter

FortiGuard Web Filtering is a managed web filtering solution provided by Fortinet. FortiGuard Web Filtering sorts hundreds of millions of web pages into a wide range of categories users can allow, block, or monitor. The FortiGate unit accesses the nearest FortiGuard Web Filtering Service Point to determine the category of a requested web page then follows the firewall policy configured for that user or interface.

FortiGuard Web Filtering includes over 60 million individual ratings of web sites applying to hundreds of millions of pages. Pages are sorted and rated into 56 categories users can allow, block, or monitor. Categories may be added to, or updated, as the Internet evolves. To make configuration simpler, users can also choose to allow, block, or monitor entire groups of categories. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

FortiGuard Web Filtering ratings are performed by a combination of proprietary methods including text analysis, exploitation of the Web structure, and human raters. Users can notify the FortiGuard Web Filtering Service Points if they feel a web page is not categorized correctly, and new sites are quickly rated as required.

Use the procedure "FortiGuard Web Filtering options" on page 334 to configure FortiGuard category blocking in a protection profile. To configure the FortiGuard Web service, see "Configuring the FortiGate unit for FDN and FortiGuard services" on page 188.
Configuring FortiGuard Web Filtering

To configure the FortiGuard Web Filtering service

- Go to System > Maintenance > FortiGuard Center.

For additional information, see “Configuring the FortiGate unit for FDN and FortiGuard services” on page 188.

Viewing the override list

Users may require access to web sites that are blocked by a policy. In this case, an administrator can give the user the ability to override the block for a specified period of time.

When a user attempts to access a blocked site, if override is enabled, a link appears on the block page directing the user to an authentication form. The user must provide a correct user name and password or the web site remains blocked. Authentication is based on user groups and can be performed for local, RADIUS, and LDAP users. For more information about authentication and configuring user groups, see “User groups” on page 386.

To view the override list

- Go to Web Filter > FortiGuard - Web Filter > Override.

Figure 300: Override list

The override list has the following icons and features:

Create New
Select to add a new override rule to the list.

Page up icon
Select to view the previous page.

Page down icon
Select to view the next page.

Clear All icon
Select to clear the table.

URL/Category
The URL or category to which the override applies.

Scope
The user or user group who may use the override.

Off-site URLs
A green check mark indicates that the off-site URL option is set to Allow, which mean that the overwrite web page will display the contents from off-site domains. A gray cross indicates that the off-site URL option is set to Block, which means that the overwrite web page will not display the contents from off-site domains. For details, see “Configuring override rules” on page 437.

Initiator
The creator of the override rule.

Expiry Date
The expiry date of the override rule.

Delete icon
Select to remove the entry from the list.

Edit icon
Select to edit the following information: Type, URL, Scope, User, Off-site URLs, and Override Duration.
Configuring override rules

Override rules can be configured to allow access to blocked web sites based on directory, domain name, or category.

To create an override rule for a directory or domain

1. Go to Web Filter > FortiGuard - Web Filter > Override.
2. Select Create New.
3. Select the Type.
4. Select the Scope.
5. Select the information that corresponds with Scope.
6. Select Allow or Block for the off-site URLs.
7. Set the duration of the override.
8. Select OK.

Figure 301: New Override Rule - Directory or Domain

| Type       | Select Directory or Domain. |
| URL        | Enter the URL or the domain name of the website. |
| Scope      | Select one of the following: User, User Group, IP, or Profile. Depending on the option selected, a different option appears below Scope. |
| User       | Enter the name of the user selected in Scope. |
| User Group | Select a user group from the dropdown list. User groups must be configured before FortiGuard Web Filtering configuration. For more information, see “User groups” on page 386. |
| IP         | Enter the IP address of the computer initiating the override. |
| Profile    | Select a protection profile from the dropdown list. |
Off-site URLs

This option defines whether the override web page will display the images and other contents from the blocked offsite URLs. For example, all FortiGuard categories are blocked, and you want to visit a site whose images are served from a different domain. You can create a directory override for the site and view the page. If the offsite feature was set to deny, all the images on the page will appear broken because they come from a different domain for which the existing override rule does not apply. If you set the offsite feature to allow, the images on the page will then show up. Only users that apply under the scope for the page override can see the images from the temporary overrides. The users will not be able to view any pages on the sites where the images come from (unless the pages are served from the same directory as the images themselves) without having to create a new override rule.

Override Duration

Enter the duration in days, hours, and minutes. When displayed in the override list, the expiry date of the override is calculated.

To create an override for categories, go to Web Filter > FortiGuard - Web Filter > Override.

Figure 302: New Override Rule - Categories

<table>
<thead>
<tr>
<th>Type</th>
<th>Categories</th>
<th>Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Potentially Liabilities (6)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controversial (5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Potentially Non-productive (7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Potentially Bandwidth Consuming (3)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Potential Security Violating (2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>General Interest (21)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business-oriented (5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Others (3)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local Categories (0)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classifications</th>
<th>Classification</th>
<th>Override</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cached Content</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multimedia Search</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Image Search</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audio Search</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Video Search</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spam URL</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scope</th>
<th>User</th>
<th>Off-site URLs</th>
<th>Override Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User</td>
<td>Allow</td>
<td>0 (days) 0 (hours) 15 (minutes)</td>
</tr>
</tbody>
</table>

Type

Select Categories.

Categories

Select the categories to which the override applies. A category group or a subcategory can be selected. Local categories are also displayed.

Classifications

Select the classifications to which the override applies. When selected, users can access web sites that provide content cache, and provide searches for image, audio, and video files.
Creating local categories

User-defined categories can be created to allow users to block groups of URLs on a per-profile basis. The categories defined here appear in the global URL category list when configuring a protection profile. Users can rate URLs based on the local categories.

Figure 303: Local categories list

<table>
<thead>
<tr>
<th>Local Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conflicts of Interest</td>
</tr>
<tr>
<td>Offensive Images</td>
</tr>
<tr>
<td>Unofficial Sources</td>
</tr>
</tbody>
</table>

Add Enter the name of the category then select Add.
Delete icon Select to remove the entry from the list

Viewing the local ratings list

To view the local ratings list

- Go to Web Filter > FortiGuard - Web Filter > Local Ratings.

Figure 304: Local ratings list

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>![Create New]</td>
<td>![Search]</td>
</tr>
<tr>
<td>![1 - 3 of 3]</td>
<td>![Category]</td>
</tr>
<tr>
<td>![1] example.com</td>
<td>![Sports]</td>
</tr>
<tr>
<td>![2] example.net</td>
<td>![Adult Materials...]</td>
</tr>
<tr>
<td>![3] example.org</td>
<td>![Hacking]</td>
</tr>
</tbody>
</table>

The local ratings list has the following icons and features:

Create New Select to add a rating to the list.
Search Enter search criteria to filter the list.
1 - 3 of 3 The total number of local ratings in the list.
Page up icon Select to view the previous page.
Page down icon Select to view the next page.
Clear All icon Select to clear the table.
URL The rated URL. Select the green arrow to sort the list by URL.
Configuring local ratings

Users can create user-defined categories then specify the URLs that belong to the category. This allows users to block groups of web sites on a per profile basis. The ratings are included in the global URL list with associated categories and compared in the same way the URL block list is processed.

The local ratings override the FortiGuard server ratings and appear in reports as “Local Category”.

To create a local rating

- Go to Web Filter > FortiGuard - Web Filter > Local Ratings.
Category block CLI configuration

Use the `hostname` keyword for the `webfilter fortiguard` command to change the default host name (URL) for the FortiGuard Web Filtering Service Point. The FortiGuard Web Filtering Service Point name cannot be changed using the web-based manager. Configure all FortiGuard Web Filtering settings using the CLI. For more information, see the FortiGate CLI Reference for descriptions of the `webfilter fortiguard` keywords.

FortiGuard Web Filtering reports

**Note:** FortiGuard Web Filtering reports are only available on FortiGate units with a hard disk.

Generate a text and pie chart format report on FortiGuard Web Filtering for any protection profile. The FortiGate unit maintains statistics for allowed, blocked, and monitored web pages for each category. View reports for a range of hours or days, or view a complete report of all activity.

**To create a web filter report**

- Go to Web Filter > FortiGuard - Web Filter > Reports.
Figure 307: Sample FortiGuard Web Filtering report

The following table describes the options for generating reports:

<table>
<thead>
<tr>
<th>Category</th>
<th>Allowed</th>
<th>Blocked</th>
<th>Monitored</th>
<th>Overridden</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potentially Unlawful</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>Offensive</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>Violence</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Controversial</td>
<td>0</td>
<td>61</td>
<td>61</td>
<td>0</td>
</tr>
<tr>
<td>SPAM/Malicious</td>
<td>0</td>
<td>19</td>
<td>19</td>
<td>0</td>
</tr>
<tr>
<td>Advertising</td>
<td>0</td>
<td>42</td>
<td>42</td>
<td>0</td>
</tr>
<tr>
<td>Potentially Non-productive</td>
<td>146</td>
<td>17</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>Peerware Downloads</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>Internet Communication</td>
<td>1</td>
<td>11</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>Web-based Email</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>File Sharing and Storage</td>
<td>140</td>
<td>8</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Potential Security Violating</td>
<td>302</td>
<td>33</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>Arts and Entertainment</td>
<td>302</td>
<td>33</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>Business Oriented</td>
<td>630</td>
<td>0</td>
<td>0</td>
<td>829</td>
</tr>
<tr>
<td>Information and Computer Security</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Government and Legal Organizations</td>
<td>113</td>
<td>0</td>
<td>113</td>
<td>0</td>
</tr>
<tr>
<td>Information Technology</td>
<td>511</td>
<td>0</td>
<td>0</td>
<td>511</td>
</tr>
<tr>
<td>Other</td>
<td>159</td>
<td>0</td>
<td>0</td>
<td>159</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>163</td>
<td>0</td>
<td>0</td>
<td>163</td>
</tr>
<tr>
<td>Web Hosting</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
</tbody>
</table>

Profile: Select the protection profile for which to generate a report.
Report Type: Select the time frame for the report. Choose from hour, day, or all historical statistics.
Report Range: Select the time range (24 hour clock) or day range (from six days ago to today) for the report. For example, for an ‘hour’ report type with a range of 13 to 16, the result is a category block report for 1 pm to 4 pm today. For a ‘day’ report type with a range of 0 to 3, the result is a category block report for 3 days ago to today.
Get Report: Select to generate the report.

A generated report includes a pie chart and the following information:

Category: The category for which the statistic was generated.
Allowed: The number of allowed web addresses accessed in the selected time frame.
Blocked: The number of blocked web addresses accessed in the selected time frame.
Monitored: The number of monitored web addresses accessed in the selected time frame.
Antispam

This section explains how to configure the spam filtering options associated with a firewall protection profile.

This section describes:

- Antispam
- Banned word
- Black/White List
- Advanced antispam configuration
- Using Perl regular expressions

Antispam

Antispam can be configured to manage unsolicited commercial email by detecting spam email messages and identifying spam transmissions from known or suspected spam servers.

FortiGuard Antispam is one of the features designed to manage spam. FortiGuard is an antispam system from Fortinet that includes an IP address black list, a URL black list, and spam filtering tools. The FortiGuard Center accepts submission of spam email messages as well as reports of false positives. Visit the Fortinet Knowledge Center for details and a link to the FortiGuard Center.

Order of Spam Filtering

The order in which incoming mail is passed through the FortiGate Antispam filters is determined by the protocol used to transfer the mail:

For SMTP
1. IP address BWL check on last hop IP
2. DNSBL & ORDBL check on last hop IP, FortiGuard Antispam IP check on last hop IP, HELO DNS lookup
3. MIME headers check, E-mail address BWL check
4. Banned word check on email subject
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Banned word check on email body
7. Return e-mail DNS check, FortiGuard Anti Spam check, DNSBL & ORDBL check on public IP extracted from header

For POP3 and IMAP
1. MIME headers check, E-mail address BWL check
2. Banned word check on email subject
3. IP BWL check
4. Banned word check on email body
5. Return e-mail DNS check, FortiGuard AntiSpam check, DNSBL & ORDBL check

For SMTP, POP3, and IMAP

Filters requiring a query to a server and a reply (FortiGuard Antispam Service and DNSBL/ORDBL) are run simultaneously. To avoid delays, queries are sent while other filters are running. The first reply to trigger a spam action takes effect as soon as the reply is received.

Each spam filter passes the email to the next if no matches or problems are found. If the action in the filter is Mark as Spam, the FortiGate unit will tag or discard (SMTP only) the email according to the settings in the protection profile. If the action in the filter is Mark as Clear, the email is exempt from any remaining filters. If the action in the filter is Mark as Reject, the email session is dropped. Rejected SMTP email messages are substituted with a configurable replacement message.

Anti-spam filter controls

Spam filters are configured for system-wide use, but enabled on a per profile basis.

Table 41 describes the AntiSpam settings and where to configure and access them.

<table>
<thead>
<tr>
<th>Protection Profile spam filtering options</th>
<th>AntiSpam setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address FortiGuard Antispam check</td>
<td>System &gt; Maintenance &gt; FortiGuard Centre</td>
</tr>
<tr>
<td>Enable or disable Fortinet's antispam service called FortiGuard Antispam. FortiGuard Antispam is Fortinet's own DNSBL server that provides spam IP address and URL blacklists. Fortinet keeps the FortiGuard Antispam IP and URLs up-to-date as new spam source are found.</td>
<td>Enable FortiGuard Antispam, check the status of the FortiGuard Antispam server, view the license type and expiry date, and configure the cache. For details, see “Configuring the FortiGate unit for FDN and FortiGuard services” on page 188</td>
</tr>
<tr>
<td>IP address BWL check</td>
<td>AntiSpam &gt; Black/White List &gt; IP Address</td>
</tr>
<tr>
<td>Black/white list check. Enable or disable checking incoming IP addresses against the configured spam filter IP address list. (SMTP only.)</td>
<td>Add to and edit IP addresses to the list. You can configure the action to take as spam, clear, or reject for each IP address. You can place an IP address anywhere in the list. The filter checks each IP address in sequence. (SMTP only.)</td>
</tr>
<tr>
<td>DNSBL &amp; ORDBL check</td>
<td>Command line only</td>
</tr>
<tr>
<td>Enable or disable checking email traffic against configured DNS Blackhole List (DNSBL) and Open Relay Database List (ORDBL) servers.</td>
<td>Add or remove DNSBL and ORDBL servers to and from the list. You can configure the action to take as spam or reject for email identified as spam from each server (SMTP only). DNSBL and ORDBL configuration can only be changed using the command line interface. For more information, see the FortiGate CLI Reference.</td>
</tr>
<tr>
<td>HELO DNS lookup</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Table 41: AntiSpam and Protection Profile spam filtering configuration
Table 41: AntiSpam and Protection Profile spam filtering configuration (Continued)

<table>
<thead>
<tr>
<th>Protection Profile spam filtering options</th>
<th>AntiSpam setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable checking the source domain name against the registered IP address in the Domain Name Server. If the source domain name does not match the IP address the email is marked as spam and the action selected in the protection profile is taken.</td>
<td></td>
</tr>
<tr>
<td>E-mail address BWL check</td>
<td>AntiSpam &gt; Black/White List &gt; E-mail Address</td>
</tr>
<tr>
<td>Enable or disable checking incoming email addresses against the configured spam filter email address list.</td>
<td>Add to and edit email addresses to the list, with the option of using wildcards and regular expressions. You can configure the action as spam or clear for each email address. You can place an email address anywhere in the list. The filter checks each email address in sequence.</td>
</tr>
<tr>
<td>Return e-mail DNS check</td>
<td>n/a</td>
</tr>
<tr>
<td>Enable or disable checking incoming email return address domain against the registered IP address in the Domain Name Server. If the return address domain name does not match the IP address the email is marked as spam and the action selected in the protection profile is taken.</td>
<td></td>
</tr>
<tr>
<td>MIME headers check</td>
<td>Command line only</td>
</tr>
<tr>
<td>Enable or disable checking source MIME headers against the configured spam filter MIME header list.</td>
<td>Add to and edit MIME headers, with the option of using wildcards and regular expressions. You can configure the action for each MIME header as spam or clear. DNSBL and ORDBL configuration can only be changed using the command line interface. For more information, see the FortiGate CLI Reference.</td>
</tr>
<tr>
<td>Banned word check</td>
<td>AntiSpam &gt; Banned Word</td>
</tr>
<tr>
<td>Enable or disable checking source email against the configured spam filter banned word list.</td>
<td>Add to and edit banned words to the list, with the option of using wildcards and regular expressions. You can configure the language and whether to search the email body, subject, or both. You can configure the action to take as spam or clear for each word.</td>
</tr>
<tr>
<td>Spam Action</td>
<td>n/a</td>
</tr>
<tr>
<td>The action to take on email identified as spam. POP3 and IMAP messages are tagged. Choose Tagged or Discard for SMTP messages. You can append a custom word or phrase to the subject or MIME header of tagged email. You can choose to log any spam action in the event log.</td>
<td></td>
</tr>
<tr>
<td>Append to: Choose to append the tag to the subject or MIME header of the email identified as spam.</td>
<td></td>
</tr>
<tr>
<td>Append with: Enter a word or phrase (tag) to append to email identified as spam. The maximum length is 63 characters.</td>
<td></td>
</tr>
<tr>
<td>Add event into the system log</td>
<td></td>
</tr>
<tr>
<td>Enable or disable logging of spam actions to the event log</td>
<td></td>
</tr>
</tbody>
</table>
To access protection profile Antispam options go to Firewall > Protection Profile, edit or Create New, Spam Filtering.

**Note:** If virtual domains are enabled on the FortiGate unit, spam filtering features are configured globally. To access these features, select *Global Configuration* on the main menu.

**Banned word**

Control spam by blocking email messages containing specific words or patterns. If enabled in the protection profile, the FortiGate unit searches for words or patterns in email messages. If matches are found, values assigned to the words are totalled. If a user-defined threshold value is exceeded, the message is marked as spam. If no match is found, the email message is passed along to the next filter.

Use Perl regular expressions or wildcards to add banned word patterns to the list.

**Note:** Perl regular expression patterns are case sensitive for antispam banned words. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

**Viewing the antispam banned word list catalog**

You can add multiple antispam banned word lists and then select the best antispam banned word list for each protection profile. To view the antispam banned word list catalog, go to *AntiSpam > Banned Word*. To view any individual antispam banned word list, select the edit icon for the list you want to see.

**Figure 308: Sample antispam banned word list catalog**

<table>
<thead>
<tr>
<th>Name</th>
<th># Entries</th>
<th>Profiles</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>bad_sites</td>
<td>3</td>
<td>web</td>
<td>offensive content</td>
</tr>
<tr>
<td>public_email_sites</td>
<td>4</td>
<td>web</td>
<td></td>
</tr>
<tr>
<td>tracking_cookie_sites</td>
<td>7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The antispam banned word list catalogue has the following icons and features:

**Add**
To add a new list to the catalog, enter a name and select Add. New lists are empty by default.

**Name**
The available antispam banned word lists.

**# Entries**
The number of entries in each antispam banned word list.

**Profiles**
The protection profiles each antispam banned word list has been applied to.

**Comment**
Optional description of each antispam banned word list.

**Delete icon**
Select to remove the antispam banned word list from the catalog. The delete icon is only available if the antispam banned word list is not selected in any protection profiles.

**Edit icon**
Select to edit the antispam banned word list, list name, or list comment.

Select antispam banned word lists in protection profiles. For more information, see “Spam filtering options” on page 336.
Creating a new antispam banned word list

To add an antispam banned word list to the antispam banned word list catalog, go to AntiSpam > Banned Word and select Create New.

Figure 309: New AntiSpam Banned Word list dialog box

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name of the new list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Enter a comment to describe the list, if required.</td>
</tr>
</tbody>
</table>

Viewing the antispam banned word list

Each email message is checked against the antispam banned word list. Add one or more banned words to sort email messages containing those words in the subject, body, or both. The score value of each banned word appearing in the message is added, and if the total is greater than the threshold value set in the protection profile, the message is processed according to the Spam Action setting in the protection profile. The score for a pattern is applied only once even if it appears in the message multiple times.

To view the banned word list, go to AntiSpam > Banned Word and select the edit icon of the banned word list you want to view.

Figure 310: Sample banned word List

<table>
<thead>
<tr>
<th>Name</th>
<th>Comment</th>
<th>Total</th>
<th>Pattern</th>
<th>Pattern Type</th>
<th>Language</th>
<th>Where</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>spamvertizing</td>
<td></td>
<td>5</td>
<td>&quot;load request&quot;</td>
<td>Wildcard</td>
<td>Western</td>
<td>Subject</td>
<td>10</td>
</tr>
<tr>
<td>&quot;replica watches&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;weight while you sleep&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;discount software&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;discount prescriptions&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The banned word list has the following icons and features:

<table>
<thead>
<tr>
<th>Name</th>
<th>Banned word list name. To change the name, edit text in the name field and select OK.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Optional comment. To add or edit comment, enter text in comment field and select OK.</td>
</tr>
<tr>
<td>Create new</td>
<td>Select to add a word or phrase to the banned word list.</td>
</tr>
<tr>
<td>Total</td>
<td>The number of items in the list.</td>
</tr>
<tr>
<td>Page up icon</td>
<td>Select to view the previous page.</td>
</tr>
<tr>
<td>Page down icon</td>
<td>Select to view the next page.</td>
</tr>
<tr>
<td>Remove All Entries icon</td>
<td>Select to clear the table.</td>
</tr>
<tr>
<td>Pattern</td>
<td>The list of banned words. Select the check box to enable all the banned words in the list.</td>
</tr>
</tbody>
</table>
Configuring the antispam banned word list

Words can be marked as spam or clear. Banned words can be one word or a phrase up to 127 characters long.

For a single word, the FortiGate unit blocks all email containing the word. For a phrase, the FortiGate unit blocks all email containing the exact phrase. To block any word in a phrase, use Perl regular expressions.

To add or edit a banned word, go to **Antispam > Banned Word**.

**Figure 311:Add Banned Word**

| Pattern | Enter the word or phrase you want to include in the banned word list. |
| Pattern Type | Select the pattern type for the banned word. Choose from wildcard or regular expression. See “Using Perl regular expressions” on page 455. |
| Language | Select the character set for the banned word. Choose from: Chinese Simplified, Chinese Traditional, French, Japanese, Korean, Thai, or Western. |
| Where | Select the location to search for the banned word. Choose from: subject, body, or all. |
| Enable | Select to enable scanning for the banned word. |
Black/White List

The FortiGate unit uses both an IP address list and an email address list to filter incoming email, if enabled in the protection profile.

When doing an IP address list check, the FortiGate unit compares the IP address of the message’s sender to the IP address list in sequence. If a match is found, the action associated with the IP address is taken. If no match is found, the message is passed to the next enabled spam filter.

When doing an email list check, the FortiGate unit compares the email address of the message’s sender to the email address list in sequence. If a match is found, the action associated with the email address is taken. If no match is found, the message is passed to the next enabled antispam filter.

Viewing the antispam IP address list catalogue

You can add multiple antispam IP address lists and then select the best antispam IP address list for each protection profile. To view the antispam IP address list catalog, go to AntiSpam > Black/White List > IP Address. To view any individual antispam IP address list, select the edit icon for the list you want to see.

Figure 312: Sample antispam IP address list catalog

<table>
<thead>
<tr>
<th>Name</th>
<th># Entries</th>
<th>Profiles</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad traffic</td>
<td>11</td>
<td>Probes, DOS, and others</td>
<td></td>
</tr>
<tr>
<td>Unwanted_connections</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our_default</td>
<td>5</td>
<td>Standard list for remote offices</td>
<td></td>
</tr>
</tbody>
</table>

The antispam IP address list catalogue has the following icons and features:

- **Add** To add a new list to the catalog, enter a name and select Add. New lists are empty by default.
- **Name** The available antispam IP address lists.
- **# Entries** The number of entries in each antispam IP address list.
- **Profiles** The protection profiles each antispam IP address list has been applied to.
- **Comment** Optional description of each antispam IP address list.
- **Delete icon** Select to remove the antispam IP address list from the catalog. The delete icon is only available if the antispam IP address list is not selected in any protection profiles.
- **Edit icon** Select to edit the antispam IP address list, list name, or list comment.

Select antispam banned word lists in protection profiles. For more information, see “Spam filtering options” on page 336.
Creating a new antispam IP address list

To add an antispam IP address list to the antispam IP address list catalog, go to AntiSpam > Black/White List and select Create New.

Figure 313: New AntiSpam IP Address list dialog box

Viewing the antispam IP address list

Configure the FortiGate unit to filter email from specific IP addresses. The FortiGate unit compares the IP address of the sender to the list in sequence. Mark each IP address as clear, spam, or reject. Filter single IP addresses or a range of addresses at the network level by configuring an address and mask.

To view the antispam IP address list, go to AntiSpam > Black/White List > IP Address and select the edit icon of the antispam IP address list you want to view.

Figure 314: Sample IP address list

The antispam IP address list has the following icons and features:

- **Name**: Antispam IP address list name. To change the name, edit text in the name field and select OK.
- **Comment**: Optional comment. To add or edit comment, enter text in comment field and select OK.
- **Create New**: Select to add an IP address to the antispam IP address list.
- **Total**: The number if items in the list.
- **Page up icon**: Select to view the previous page.
- **Page down icon**: Select to view the next page.
- **Remove All Entries**: Select to clear the table.
- **IP address/Mask**: The current list of IP addresses.
Configuring the antispam IP address list

To add an IP address to the IP address list, go to **AntiSpam > Black/White List > IP Address** and select Create New. Enter an IP address or a pair of IP address and mask in the following formats:

- x.x.x.x, for example, 62.128.69.100.
- x.x.x.x/x.x.x.x, for example, 62.128.69.100/255.255.255.0
- x.x.x.x/x, for example, 62.128.69.100/24

**Figure 315: Add IP Address**

| Action   | The action to take on email from the configured IP address. Actions are: Mark as Spam to apply the configured spam action, Mark as Clear to bypass this and remaining spam filters, or Mark as Reject (SMTP only) to drop the session. If an IP address is set to reject but mail is delivered from that IP address via POP3 or IMAP, the e-mail messages will be marked as spam.
| Delete icon | Select to remove the address from the list.
| Edit icon | Select to edit address information: IP Address/Mask, Insert, Action, and Enable.
| Move To icon | Select to move the entry to a different position in the list. The firewall executes the list from top to bottom. For example, if you have IP address 1.1.1.1 listed as spam and 1.1.1.0 listed as clear, you must put 1.1.1.1 above 1.1.1.0 for 1.1.1.1 to take effect.

**Viewing the antispam email address list catalog**

You can add multiple antispam email address lists and then select the best antispam email address list for each protection profile. To view the antispam email address list catalog, go to **AntiSpam > Black/White List > E-mail Address**. To view any individual antispam email address list, select the edit icon for the list you want to see.

**Figure 316: Sample antispam email address list catalog**

<table>
<thead>
<tr>
<th>Name</th>
<th>Entries</th>
<th>Profiles</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>9</td>
<td>Default: Branch office email block list</td>
<td></td>
</tr>
<tr>
<td>Harassors</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub_130</td>
<td>5</td>
<td>Blocks for subnet 130</td>
<td></td>
</tr>
</tbody>
</table>
The antispam email address list catalogue has the following icons and features:

**Add**
To add a new list to the catalog, enter a name and select Add. New lists are empty by default.

**Name**
The available antispam email address lists.

**# Entries**
The number of entries in each antispam email address list.

**Profiles**
The protection profiles each antispam email address list has been applied to.

**Comment**
Optional description of each antispam email address list.

**Delete icon**
Select to remove the antispam email address list from the catalog. The delete icon is only available if the antispam email address list is not selected in any protection profiles.

**Edit icon**
Select to edit the antispam email address list, list name, or list comment.

Select antispam banned word lists in protection profiles. For more information, see “Spam filtering options” on page 336.

### Creating a new antispam email address list

To add an antispam email address list to the antispam email address list catalog, go to *AntiSpam > Black/White List > E-mail Address* and select Create New.

![New AntiSpam E-mail Address list dialog box](image)

**Name**
Enter the name of the new list.

**Comment**
Enter a comment to describe the list, if required.

### Viewing the antispam email address list

The FortiGate unit can filter email from specific senders or all email from a domain (such as example.net). Mark each email address as clear or spam.

To view the antispam email address list, go to *AntiSpam > Black/White List > E-mail Address* and select the edit icon of the antispam email address list you want to view.

![Sample email address list](image)

The antispam email address list has the following icons and features:
Configuring the antispam email address list

To add an email address or domain to the list, go to Antispam > Black/White List > E-mail Address.

Figure 319: Add E-mail Address

<table>
<thead>
<tr>
<th>E-Mail Address</th>
<th>Enter the email address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern Type</td>
<td>Select a pattern type: Wildcard or Regular Expression. For more information, see “Using Perl regular expressions” on page 455.</td>
</tr>
<tr>
<td>Insert</td>
<td>Select the location in the list to insert the email address.</td>
</tr>
</tbody>
</table>
| Action         | Select an action:  
|                | • To apply the spam action configured in the protection profile, select Mark as Spam.  
|                | • Select Mark as Clear to allow the email message bypass this and remaining spam filters. |
| Enable         | Enable the email address. |
To add an email address or pattern
1. Enter the email address or pattern.
2. Select a pattern type for the list entry.
3. If required, select before or after another email address in the list to place the new email address in the correct position.
4. Select the action to take on email from the configured address or domain.
5. Select Enable.
6. Select OK.

Advanced antispam configuration

Advanced antispam configuration covers only command line interface (CLI) commands not represented in the web-based manager. For complete descriptions and examples of how to use CLI commands, see the FortiGate CLI Reference.

**config spamfilter mheader**

Use this command to configure email filtering based on the MIME header. MIME header filtering is enabled within each protection profile.

The FortiGate unit compares the MIME header key-value pair of incoming email to the list pair in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed on to the next spam filter.

MIME (Multipurpose Internet Mail Extensions) headers are added to email to describe content type and content encoding, such as the type of text in the email body or the program that generated the email. Some examples of MIME headers include:

- X-mailer: outgluck
- X-Distribution: bulk
- Content_Type: text/html
- Content_Type: image/jpg

The first part of the MIME header is called the header key, or just header. The second part is called the value. Spammers often insert comments into header values or leave them blank. These malformed headers can fool some spam and virus filters.

Use the MIME headers list to mark email from certain bulk mail programs or with certain types of content that are common in spam messages. Mark the email as spam or clear for each header configured.

**config spamfilter dnsbl**

Use this command to configure email filtering using DNS-based Blackhole List (DNSBL), and Open Relay Database List (ORDBL) servers. DNSBL and ORDBL filtering is enabled within each protection profile.

The FortiGate unit compares the IP address or domain name of the sender to any database lists configured, in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed on to the next spam filter.
Some spammers use unsecured third party SMTP servers to send unsolicited bulk email. Using DNSBLs and ORDBLs is an effective way to tag or reject spam as it enters the network. These lists act as domain name servers that match the domain of incoming email to a list of IP addresses known to send spam or allow spam to pass through.

There are several free and subscription servers available that provide reliable access to continually updated DNSBLs and ORDBLs. Please check with the service being used to confirm the correct domain name for connecting to the server.

Note: Because the FortiGate unit uses the server domain name to connect to the DNSBL or ORDBL server, it must be able to look up this name on the DNS server. For information on configuring DNS, see “Network Options” on page 99.

Using Perl regular expressions

Email address list, MIME headers list, and banned word list entries can include wildcards or Perl regular expressions.

See http://perldoc.perl.org/perlretut.html for detailed information about using Perl regular expressions.

Regular expression vs. wildcard match pattern

A wildcard character is a special character that represents one or more other characters. The most commonly used wildcard characters are the asterisk (*) which typically represents zero or more characters in a string of characters, and the question mark (?), which typically represents any one character.

In Perl regular expressions, the ‘.’ character refers to any single character. It is similar to the ‘?’ character in wildcard match pattern. As a result:

• fortinet.com not only matches fortinet.com but also fortinetacom, fortinetbcom, fortinetccom, and so on.

To match a special character such as ‘.’ and ‘*’ use the escape character ‘\’. For example:

• To match fortinet.com, the regular expression should be: fortinet\.com

In Perl regular expressions, ‘*’ means match 0 or more times of the character before it, not 0 or more times of any character. For example:

• forti*.com matches fortiiii.com but does not match fortinet.com

To match any character 0 or more times, use ‘.*’ where ‘.’ means any character and the ‘*’ means 0 or more times. For example, the wildcard match pattern forti*.com should therefore be fort.*\.com.

Word boundary

In Perl regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression “test” not only matches the word “test” but also any word that contains “test” such as “atest”, “mytest”, “testimony”, “atestb”. The notation “\b” specifies the word boundary. To match exactly the word “test”, the expression should be ‘\b\test\b’.
Case sensitivity

Regular expression pattern matching is case sensitive in the web and antispam filters. To make a word or phrase case insensitive, use the regular expression /i. For example, /bad language/i will block all instances of "bad language", regardless of case.

Perl regular expression formats

Table 42 lists and describes some example Perl regular expression formats.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td>&quot;abc&quot; (the exact character sequence, but anywhere in the string)</td>
</tr>
<tr>
<td>^abc</td>
<td>&quot;abc&quot; at the beginning of the string</td>
</tr>
<tr>
<td>abc$</td>
<td>&quot;abc&quot; at the end of the string</td>
</tr>
<tr>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>^abc</td>
<td>abc$</td>
</tr>
<tr>
<td>ab[2,4]c</td>
<td>&quot;a&quot; followed by two, three or four &quot;b&quot;s followed by a &quot;c&quot;</td>
</tr>
<tr>
<td>ab[2,]c</td>
<td>&quot;a&quot; followed by at least two &quot;b&quot;s followed by a &quot;c&quot;</td>
</tr>
<tr>
<td>ab*c</td>
<td>&quot;a&quot; followed by any number (zero or more) of &quot;b&quot;s followed by a &quot;c&quot;</td>
</tr>
<tr>
<td>ab+c</td>
<td>&quot;a&quot; followed by one or more b's followed by a c</td>
</tr>
<tr>
<td>ab?c</td>
<td>&quot;a&quot; followed by an optional &quot;b&quot; followed by a &quot;c&quot;; that is, either &quot;abc&quot; or &quot;ac&quot;</td>
</tr>
<tr>
<td>a.c</td>
<td>&quot;a&quot; followed by any single character (not newline) followed by a &quot;c&quot;</td>
</tr>
<tr>
<td>a\c</td>
<td>&quot;a.c&quot; exactly</td>
</tr>
<tr>
<td>[abc]</td>
<td>Any one of &quot;a&quot;, &quot;b&quot; and &quot;c&quot;</td>
</tr>
<tr>
<td>[Aa]bc</td>
<td>Either of &quot;Abc&quot; and &quot;abc&quot;</td>
</tr>
<tr>
<td>[abc]+</td>
<td>Any (nonempty) string of &quot;a&quot;s, &quot;b&quot;s and &quot;c&quot;s (such as &quot;a&quot;, &quot;abba&quot;, &quot;acababcacaas&quot;)</td>
</tr>
<tr>
<td>[*abc]+</td>
<td>Any (nonempty) string which does not contain any of &quot;a&quot;, &quot;b&quot;, and &quot;c&quot; (such as &quot;defg&quot;)</td>
</tr>
<tr>
<td>\d\d</td>
<td>Any two decimal digits, such as 42; same as \d(2)</td>
</tr>
<tr>
<td>/i</td>
<td>Makes the pattern case insensitive. For example, /bad language/i blocks any instance of bad language regardless of case.</td>
</tr>
<tr>
<td>\w+</td>
<td>A &quot;word&quot;: A nonempty sequence of alphanumeric characters and low lines (underscores), such as foo and 12bar8 and foo_1</td>
</tr>
<tr>
<td>100</td>
<td>a*mk</td>
</tr>
</tbody>
</table>
### Example regular expressions

**To block any word in a phrase**

```
/block|any|word/>
```

**To block purposely misspelled words**

Spammers often insert other characters between the letters of a word to fool spam blocking software.

```
/^.*v.*i.*a.*g.*r.*o.*$/
cr[éêëé][\+-]  
\*=<>\.,;\!?%&§@^°$£€\{\}()\[\]\|\_01]dit/i
```

**To block common spam phrases**

The following phrases are some examples of common phrases found in spam messages.

```
/try it for free/i
/student loans/i
/you’re already approved/i
/special\[\+-]  
\*=<>\.,;\!?%&~#§@^°$£€\{\}()\[\]\|\_1]offer/i
```
IM, P2P & VoIP

The IM, P2P & VoIP menu provides IM user management tools and statistics for network IM, P2P, and VoIP usage. IM, P2P, and VoIP protocols must be enabled in the active protection profile for the settings in this section to have any effect.

This section describes:

- Overview
- Configuring IM/P2P protocols
- Statistics
- User

Overview

Instant Messenger (IM), Peer to Peer (P2P), and Voice over Internet Protocol (VoIP) protocols are gaining in popularity as an essential way to communicate between two or more individuals in real time. Some companies even rely on IM protocols for critical business applications such as Customer/Technical Support.

The most common IM protocols in use today include AOL Instant Messenger, Yahoo Instant Messenger, MSN messenger, and ICQ. Although these are the most common currently in use, there are always new protocols being developed as well as newer versions of older ones.

P2P protocols are most commonly used to transfer files from one user to another and can use large amounts of bandwidth.

VoIP is increasingly being used by businesses to cut down on the cost of long distance voice communications.

Some organizations need to control or limit the use of IM/P2P and VoIP protocols in order to more effectively manage bandwidth use.

With FortiOS firmware, you can control and monitor the usage of IM/P2P applications and VoIP protocols.

FortiOS supports two VoIP protocols: Session Initiation Protocol (SIP) and Skinny Client Control Protocol (SCCP).

Fortinet Inc. recognizes that IM/P2P applications are becoming part of doing business but also, if abused, can seriously decrease productivity and network performance.

FortiGate systems allow you to set up user lists that either allow or block the use of applications, to determine which applications are allowed and how much bandwidth can be used by the applications.

By combining comprehensive protection policies and easy-to-view statistical reports, you can see which applications are being used and for what purpose, making it easy to control IM/P2P applications and to maximize productivity.
The FortiOS system comes with an impressive list of supported IM/P2P protocols and can be kept up-to-date with upgrades available for download from the Fortinet Distribution Network. There is no need to wait for firmware upgrade to stay ahead of the latest protocols. FortiOS also provides ways for you to deal with unknown protocols even before upgrades are available.

Table 43 on page 460 lists the IM/P2P applications that are currently recognized by FortiOS. The table includes the decoders, the applications associated with the decoders and the location of the decoders in the FortiGate interface.

Table 43: IM/P2P applications covered by FortiOS 3.0

<table>
<thead>
<tr>
<th>IPS</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instant Messaging</strong></td>
<td></td>
</tr>
<tr>
<td>AIM (Firewall &gt; Protection Profile &gt; IM/P2P)</td>
<td>AIM, AIM Triton</td>
</tr>
<tr>
<td>ICQ (Firewall &gt; Protection Profile &gt; IM/P2P)</td>
<td>ICQ</td>
</tr>
<tr>
<td>MSN (Firewall &gt; Protection Profile &gt; IM/P2P)</td>
<td>MSN Messenger</td>
</tr>
<tr>
<td>qq (Intrusion Protection &gt; Signatures &gt; Protocol decoder &gt; im_decoder)</td>
<td>QQ</td>
</tr>
<tr>
<td>Yahoo! (Firewall &gt; Protection Profile &gt; IM/P2P)</td>
<td>Yahoo Messenger</td>
</tr>
<tr>
<td>msn_web_messenger (Intrusion Protection &gt; Signatures &gt; Protocol decoder &gt; im_decoder)</td>
<td>MSN web Messenger</td>
</tr>
<tr>
<td>google_talk (Intrusion Protection &gt; Signatures &gt; Protocol decoder &gt; im_decoder)</td>
<td>Google Instant Messenger</td>
</tr>
<tr>
<td>rediff (Intrusion Protection &gt; Signatures &gt; Protocol decoder &gt; im_decoder)</td>
<td>Rediff Instant Messenger</td>
</tr>
<tr>
<td><strong>P2P</strong></td>
<td></td>
</tr>
<tr>
<td>BitTorrent (Firewall &gt; Protection Profile &gt; IM/P2P)</td>
<td>BitComet</td>
</tr>
<tr>
<td></td>
<td>BitSpirit</td>
</tr>
<tr>
<td></td>
<td>Azureus</td>
</tr>
<tr>
<td></td>
<td>Shareaza</td>
</tr>
<tr>
<td>eDonkey (Firewall &gt; Protection Profile &gt; IM/P2P)</td>
<td>eMule</td>
</tr>
<tr>
<td></td>
<td>Overnet</td>
</tr>
<tr>
<td></td>
<td>Edonkey2K</td>
</tr>
<tr>
<td></td>
<td>Shareaza</td>
</tr>
<tr>
<td></td>
<td>BearShare</td>
</tr>
<tr>
<td></td>
<td>MLdonkey</td>
</tr>
<tr>
<td></td>
<td>iMesh</td>
</tr>
</tbody>
</table>

Note: Applications in Table 43 on page 460 marked as bold can connect to multiple P2P networks. Turning on IM and P2P decoders and signatures will help improve IPS performance. For example, if you want to use IPS, but you do not want to block IM or P2P applications, you should leave IM/P2P decoders and signatures enabled. Normally, if you turn off other signatures, the performance will be better, but for IM/P2P, it's the opposite.
Configuring IM/P2P protocols

Different organizations require different policies regarding IM/P2P. The FortiGate unit allows you to configure your unit in the way that best serves your needs.

How to enable and disable IM/P2P options

This section will tell you the four main locations to enable or disable the IM/P2P options. This section includes how to enable predefined signatures, custom signatures and unknown user policies.

To enable predefined IM/P2P signatures in intrusion protection

1. Go to Intrusion Protection > Signatures > Predefined.
2. Use the signature group filter to search for the IM and P2P signatures.
3. Enable the signature by selecting the Enable box.
4. Enable logging for a signature by selecting the Logging box.
5. In the row that corresponds to the signature you want to edit, select the Edit icon.
6. Set the action and severity.
7. Select OK.

To create custom IM/P2P signatures for unknown protocols

1. Go to Intrusion Protection > Signature > Custom > Create New.

### Table 43: IM/P2P applications covered by FortiOS 3.0

<table>
<thead>
<tr>
<th>IPS</th>
<th>Applications</th>
</tr>
</thead>
</table>
| Gnutella (Firewall > Protection Profile > IM/P2P) | BearShare  
Shareaza  
LimeWire  
Xolox  
Swapper  
iMesh  
MLdonkey  
Gnucleus  
Morpheus  
Openext  
Mutella  
Qtella  
Qcquisition  
Acquisition  
NapShare  
gtk-gnutella |
| KaZaA (Firewall > Protection Profile > IM/P2P) | KaZaA |
| Skype (Firewall > Protection Profile > IM/P2P) | Skype |
| WinNY (Firewall > Protection Profile > IM/P2P) | WinNY |
| ares (Intrusion Protection > Signatures > Protocol decoder > p2p_decoder) | Ares Galaxy |
| direct_connect (Intrusion Protection > Signatures > Protocol decoder > p2p_decoder) | DC++ |
2 Enter a name for the signature.
3 Enter the signature.
4 Select the severity and what action to perform.
5 Select OK.

To set up the policy for unknown IM users
1 Go to IM, P2P & VoIP > User > Config.
2 Select Allow or Block for each of the four IM applications.
3 Select Apply.

How to configure IM/P2P/VoIP options within a protection profile

There are several areas within a protection profile where you can configure the IM/P2P/VoIP settings. For more detailed information, see the Firewall Profile chapter of this guide and the IP, P2P and VoIP Technical Note.

How to configure older versions of IM/P2P applications

Some older versions of IM protocols are able to bypass file blocking because the message types are not recognized.

Supported IM protocols include:
• MSN 6.0 and above
• ICQ 4.0 and above
• AIM 5.0 and above
• Yahoo 6.0 and above

If you want to block a protocol that is older than the ones listed above, use the CLI command: For details see the FortiGate CLI Reference.

config imp2p old-version.

How to configure protocols that are not supported

If you find a protocol that is not supported, please ensure that the IPS package is up to date. If the IPS package is up to date and the protocol is still not supported you can use the custom signature.

To create a custom signature
1 Go to Intrusion Protection > Signature > Custom > Create New.
2 Enter a name for the signature.
3 Enter the signature.
4 Use the drop down boxes to select an action and the severity for the signature.
5 Select apply.

Note: To detect new IM/P2P applications or new versions of the existing applications, you only need update the IPS package, available through the FortiNet Distribution Network (FDN). No firmware upgrade is needed.
Statistics

You can view the IM, P2P and VoIP statistics to gain insight into how the protocols are being used within the network. Overview statistics are provided for all supported IM, P2P and VoIP protocols. Detailed individual statistics are provided for each IM protocol.

Note: If virtual domains are enabled on the FortiGate unit, IM, P2P and VoIP features are configured globally. To access these features, select Global Configuration on the main menu.

Viewing overview statistics

The Summary tab provides a summary of statistics for all IM, P2P and VoIP protocols.

To view IM/P2P statistics, go to IM/P2P&VoIP > Statistics > Summary.

Figure 320:IM, P2P and VoIP statistics summary

The Summary tab has the following icons and features:

- **Automatic Refresh Interval**: Select the automatic refresh interval for statistics. Set the interval from none to 30 seconds.
- **Refresh**: Click to refresh the page with the latest statistics.
- **Reset Stats**: Click to reset the statistics to zero.
- **Users**
  - **Current Users**
  - **Since Last Reset**
  - **Blocked**: For each IM protocol, the following user information is listed:
    - Current Users
    - (Users) Since Last Reset
    - (Users) Blocked.
- **Chat**
  - **Total Chat Sessions**
  - **Total Messages**
  - **File Transfers**
    - **Since Last Reset**: For each IM protocol, the following chat information is listed:
      - Total Chat Sessions
    - **Blocked**: For each IM protocol, the following file transfer information is listed:
      - (File transfers) Since Last Reset
      - (File transfers) Blocked.
Statistics

**Voice Chat**
For each IM protocol, the following voice chat information is listed:
- (Voice chats) Since Last Reset
- (Voice chats) Blocked

**P2P Usage**
For each P2P protocol, the following usage information is listed:
- Total Bytes transferred
- Average Bandwidth

**VoIP Usage**
For SIP and SCCP protocol, the following information is listed:
- Active Sessions (phones connected)
- Total calls (since last reset)
- Calls failed/Dropped
- Calls Succeeded

**Viewing statistics by protocol**
The protocol tab provides detailed statistics for individual IM protocols.

To view protocol statistics, go to **IM, P2P & VoIP > Statistics > Protocol**.

You can log IM chat information and the limitations placed on it, by enabling **Archive full IM chat info to FortiAnalyzer** in the protection profile.

Figure 321: IM statistics by Protocol

<table>
<thead>
<tr>
<th>Automatic Refresh Interval</th>
<th>Refresh</th>
<th>Protocol: AIM</th>
</tr>
</thead>
</table>

The IM/P2P Protocol tab has the following icons and features:

**Automatic Refresh Interval**
Select the automatic refresh interval for statistics. Set the interval from none to 30 seconds.

**Protocol**
Select the protocol for which statistics are to be displayed: AIM, ICQ, MSN, or Yahoo.

**Users**
For the selected protocol, the following user information is displayed: Current Users, (Users) Since Last Reset, and (Users) Blocked.

**Chat**
For the selected protocol, the following chat information is displayed: Total Chat Sessions, Server-based Chat, Group Chat, and Direct/Private Chat.
User

After IM users connect through the firewall, the FortiGate unit displays which users are connected in the Current Users list. You can analyze the list and decide which users to allow or block. A policy can be configured to deal with unknown users.

Note: If virtual domains are enabled on the FortiGate unit, IM features are configured globally. To access these features, select Global Configuration on the main menu.

Viewing the Current Users list

The Current User list displays information about instant messaging users who are currently connected. The list can be filtered by protocol.

To view current users, go to IM, P2P & VoIP > Users > Current User.

Figure 322: Current Users list

<table>
<thead>
<tr>
<th>Protocol</th>
<th>User Name</th>
<th>Source IP</th>
<th>Last Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>User Name</td>
<td>Source IP</td>
<td>Last Login</td>
</tr>
</tbody>
</table>

The Current Users list has the following features:

- **Protocol**: Filter the list by selecting the protocol for which to display current users: AIM, ICQ, MSN, or Yahoo. All current users can also be displayed.
- **Protocol**: The protocol being used.
- **User Name**: The name selected by the user when registering with an IM protocol. The same user name can be used for multiple IM protocols. Each user name/protocol pair appears separately in the list.
- **Source IP**: The Address from which the user initiated the IM session.
- **Last Login**: The last time the current user used the protocol.
- **Block**: Select to add the user name to the permanent black list. Each user name/protocol pair must be explicitly blocked by the administrator.
Viewing the User List

The User List displays information about users who have been allowed access to (white list) or have been blocked from (black list) instant messaging services. Users can be added using Create New or from the temporary users list.

To view the User List, go to **IM, P2P & VoIP > Users > User List**.

**Figure 323: User List**

The user list has the following icons and features:

- **Create New** Select to add a new user to the list.
- **Protocol** Filter the list by selecting a protocol: AIM, ICQ, MSN, Yahoo, or All.
- **Policy** Filter the list by selecting a policy: Allow, Deny, or All.
- **Username** The name selected by the user when registering with an IM protocol. The same user name can be used for multiple IM protocols. Each user name/protocol pair appears separately in the list.
- **Policy** The protocol associated with the user.
- **Policy** The policy applied to the user when attempting to use the protocol: Block or Deny.
- **Edit icon** Change the following user information: Protocol, Username, and Policy.
- **Delete icon** Permanently remove users from the User List.

Adding a new user to the User List

Add users to the User List to allow them to access instant messaging services or to block them from these services.

Go to **IM, P2P & VoIP > User > User List** and select Create New.

**Figure 324: Edit User**

- **Protocol** Select a protocol from the dropdown list: AIM, ICQ, MSN, or Yahoo!
- **Username** Enter a name for the user.
- **Policy** Select a policy from the dropdown list: Allow or Block.
Configuring a policy for unknown IM users

The User Policy determines the action to be taken with unknown users. Unknown users can be either allowed to use some or all of the IM protocols and added to a white list, or blocked from using some or all of the IM protocols and added to a black list. You can later view the white and black lists and add the users to the user list.

To configure the IM policy, go to IM, P2P & VoIP > User > Config.

Figure 325: IM User policy

Configure or view the following settings for the IM user policy:

- **Automatically Allow**: Select the protocols that unknown users are allowed to use. The unknown users are added to a temporary white list.
- **Automatically Block**: Select the protocols to which unknown users are denied access. The unknown users are added to a temporary black list.
- **List of Temporary Users**: New users who have been added to the temporary white or black lists. User information includes Protocol, Username, and the Policy applied to the user. **Note**: If the FortiGate unit is rebooted, the list is cleared.
- **Protocol**: Select a protocol by which to filter the list of temporary users.
- **Username**: The name selected by the user when registering with an IM protocol. The same user name can be used for multiple IM protocols. Each user name/protocol pair appears separately in the list.
- **Policy**: The policy applied to the user when attempting to use the protocol: Block or Deny.
- **Permanently Allow**: Select to add the user to the permanent white list. The user remains online and is listed in IM, P2P & VoIP > Users > User List.
- **Permanently Block**: Select to add the user to the permanent black list. The user is listed in IM, P2P & VoIP > Users > User List.
- **Apply**: Click to apply the global user policy.
Log&Report

This section provides information on how to enable logging, viewing of log files and the viewing of reports available through the web-based manager. FortiGate units provide extensive logging capabilities for traffic, system and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network misuse and abuse.

This section describes:

- FortiGate Logging
- FortiGuard Analysis Service
- Log severity levels
- High Availability cluster logging
- Storing Logs
- Configuring FortiGuard Analysis Service
- Log types
- Accessing Logs
- Viewing log information
- Customizing the display of log messages
- Content Archive
- Alert Email
- Reports

Note: VDOMs may affect logging and reporting features in FortiOS 3.0MR5. Before configuring logging and reporting features in FortiOS 3.0MR5, make sure these features are accessible in the VDOM where you want to configure logging and reporting features.

FortiGate Logging

A FortiGate unit can log many different network activities and traffic including:

- overall network traffic
- system-related events including system restarts, HA and VPN activity
- anti-virus infection and blocking
- web filtering, URL and HTTP content blocking
- signature and anomaly attack and prevention
- spam filtering
- Instant Messaging and Peer-to-Peer traffic
- VoIP telephone calls
You can customize the level that the FortiGate unit logs these events at as well as where the FortiGate unit stores the logs. The level these events are logged at, or the severity level, is defined when configuring the logging location. There are six severity levels to choose from. See “Log severity levels” on page 471 for more information.

For better log storage and retrieval, the FortiGate unit can send log messages to a FortiAnalyzer™ unit. FortiAnalyzer units are network appliances that provide integrated log collection, analysis tools and data storage. Detailed log reports provide historical as well as current analysis of network and email activity. Detailed log reports also help identify security issues, reducing network misuse and abuse. The FortiGate unit can send all log message types, as well as quarantine files, to a FortiAnalyzer unit for storage. The FortiAnalyzer unit can upload log files to an FTP server for archival purposes. See “Logging to a FortiAnalyzer unit” on page 472 for details on configuring the FortiGate unit to send log messages to a FortiAnalyzer unit.

The FortiGate unit can send log messages to either a Syslog server or WebTrends server for storage and archival purposes. You can also configure the FortiGate unit to send logs messages to its hard disk, if available. Configuring the FortiGate unit to send log messages to the hard disk is only available in the CLI. See the FortiGate CLI Reference for configuring logging to the hard disk.

The FortiGate unit enables you to view log messages available in memory, on a FortiAnalyzer unit running firmware version 3.0 or higher, including the hard disk if available. Customizable filters enable you to easily locate specific information within the log files.

See the FortiGate Log Message Reference for details and descriptions of log messages and formats.

FortiGuard Analysis Service

FortiGuard Analysis Service is a subscription-based service that provides logging and reporting solutions for FortiGate-100A units and lower. The FortiGuard Analysis Service is available on FortiGate-100A units and lower running FortiOS 3.0MR4 and higher.

The FortiGuard Analysis network is made up of two types of servers, the primary analysis server and the secondary analysis server. The primary analysis server stores logs generated from the FortiGate unit. The secondary analysis server provides redundancy, ensuring log data is available at all times. There are several secondary analysis servers available for redundancy for each FortiGate unit. The network also includes the main analysis server, which is responsible for monitoring and maintaining the primary and secondary analysis servers.

When the FortiGate unit connects for the first time to the FortiGuard Analysis network, the FortiGate unit retrieves its assigned primary analysis server, contract term, and storage space quota from the main analysis server. The main analysis server contains this information so it can maintain and monitor the status of each of the servers.

After configuring logging to the assigned primary analysis server, the FortiGate unit begins logging to that primary analysis server. The FortiGate unit sends encrypted logs to the primary analysis server using TCP port 514. The connection to the main analysis server is secured by SSL using port 443.
**FortiGuard Analysis Service portal website**

The portal website provides a central location for registering your contract information as well as viewing logs and reports.

Contracts provide access to the FortiGuard Analysis Service and are purchased through your sales representative. Before purchasing a contract, you require registering for a trial contract. The trial contract provides the contract number for registering for the FortiGuard Analysis Service on the FortiGuard Analysis Service website. After the trial contract expires, you can then purchase a full contract from your sales representative.

After purchasing a full contract, you only require registering at the portal.

See the *FortiGuard Analysis and Management Services Administration Guide* if you require more information about FortiGuard Analysis Service.

**Note:** The portal also includes FortiGuard Management Services features. See “System Maintenance” on page 179 for more information about FortiGuard Management Services.

---

**Log severity levels**

You can define what severity level the FortiGate unit records logs at when configuring the logging location. The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select Error, the unit logs Error, Critical, Alert and Emergency level messages.

<table>
<thead>
<tr>
<th>Levels</th>
<th>Description</th>
<th>Generated by</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - Emergency</td>
<td>The system has become unstable.</td>
<td>Event logs, specifically administrative events, can generate an emergency severity level.</td>
</tr>
<tr>
<td>1 - Alert</td>
<td>Immediate action is required.</td>
<td>Attack logs are the only logs that generate an Alert severity level.</td>
</tr>
<tr>
<td>2 - Critical</td>
<td>Functionality is affected.</td>
<td>Event, Antivirus, and Spam filter logs.</td>
</tr>
<tr>
<td>3 - Error</td>
<td>An error condition exists and functionality could be affected.</td>
<td>Event and Spam filter logs.</td>
</tr>
<tr>
<td>4 - Warning</td>
<td>Functionality could be affected.</td>
<td>Event and Antivirus logs.</td>
</tr>
<tr>
<td>5 - Notification</td>
<td>Information about normal events.</td>
<td>Traffic and Web Filter logs.</td>
</tr>
<tr>
<td>6 - Information</td>
<td>General information about system operations.</td>
<td>Content Archive, Event, and Spam filter logs.</td>
</tr>
</tbody>
</table>

The Debug severity level, not shown in Table 44, is rarely used. It is the lowest log severity level and usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly. Debug log messages are only generated if the log severity level is set to Debug. Debug log messages are generated by all types of FortiGate features.
High Availability cluster logging

When configuring logging with a High Availability (HA) cluster, configure the primary unit to send logs to a FortiAnalyzer unit or a Syslog server. The settings will apply to the subordinate units. The subordinate units send the log messages to the primary unit, and the primary unit sends all logs to the FortiAnalyzer unit or Syslog server.

If you configured a secure connection via an IPSec VPN tunnel between a FortiAnalyzer unit and a HA cluster, the connection is between the FortiAnalyzer unit and the HA cluster primary unit.

See the FortiGate High Availability User Guide for more information.

Storing Logs

The type and frequency of log messages you intend to save dictates the type of log storage to use. For example, if you want to log traffic and content logs, you need to configure the FortiGate unit to log to a FortiAnalyzer unit or Syslog server. The FortiGate system memory is unable to log traffic and content logs because of their frequency and large file size.

Storing log messages to one or more locations, such as a FortiAnalyzer unit or Syslog server, may be a better solution for your logging requirements than the FortiGate system memory. Configuring your FortiGate unit to log to a FortiGuard Analysis server may also be a better log storage solution if you have a FortiGate-100A unit or lower. Logging to a FortiGuard Analysis server will be available for all FortiGate units in future releases. See “Logging to a FortiGuard Analysis server” on page 479 for more information.

If your FortiGate unit has a hard disk, you can also enable logging to the hard disk from the CLI. See the FortiGate CLI Reference for more information before enabling logging to the hard disk.

If you require logging to multiple FortiAnalyzer units or Syslog servers, see the FortiGate CLI Reference for more information.

Note: Daylight Saving Time (DST) is now extended by four weeks in accordance to the U.S. Energy Policy Act of 2005 and only affects North America. It is recommended to check if your location observes this change, since it affects the accuracy and schedule of logs. See the Fortinet Knowledge Center article, New Daily Saving Time support, for more information.

Logging to a FortiAnalyzer unit

FortiAnalyzer units are network appliances that provide integrated log collection, analysis tools and data storage. Detailed log reports provide historical as well as current analysis of network and email activity to help identify security issues and reduce network misuse and abuse.
To configure the FortiGate unit to send logs to the FortiAnalyzer unit

2. Select FortiAnalyzer.
3. Select the blue arrow to expand the FortiAnalyzer options.
4. Set the level of the log messages to send to the FortiAnalyzer unit.
5. Enter the Server IP address of the FortiAnalyzer unit.
6. Select Apply.

The FortiAnalyzer unit needs to be configured to receive logs from the FortiGate unit after configuring log settings on the FortiGate unit. Contact a FortiAnalyzer administrator to complete the configuration.

**Note:** The FortiGate unit can log up to three FortiAnalyzer units. The FortiGate unit sends logs to all three FortiAnalyzer units where the logs are stored on each of the FortiAnalyzer units. This provides real-time backup protection in the event one of the FortiAnalyzer units fails. This feature is only available through the CLI. See the FortiGate CLI Reference for more information.

**Connecting to FortiAnalyzer using Automatic Discovery**

You can connect to a FortiAnalyzer unit by using the Automatic Discovery feature. Automatic discovery is a method of establishing a connection to a FortiAnalyzer unit.

When you select Automatic Discovery, the FortiGate unit uses HELLO packets to locate any FortiAnalyzer units available on the network within the same subnet. When the FortiGate unit discovers the FortiAnalyzer unit, the FortiGate unit automatically enables logging to the FortiAnalyzer unit and begins sending log data, if logging is configured for traffic and so on, to the FortiAnalyzer unit.

The Automatic Discovery feature is disabled by default on the FortiAnalyzer unit and must be enabled on the FortiAnalyzer unit. The FortiAnalyzer unit requires 3.0 firmware to use this feature. It is recommended to contact a FortiAnalyzer administrator to verify that the Automatic Discovery feature is enabled on the FortiAnalyzer unit before using this feature.

**To enable automatic discovery**

2. Select the blue arrow for FortiAnalyzer to expand the options.
3. Select Automatic Discovery.
4 Select Discover.
The FortiGate unit searches within the same subnet for a response from any available FortiAnalyzer units.

5 Select a FortiAnalyzer unit from the Connect To list.

6 Select Apply.

**Note:** If your FortiGate unit is in Transparent mode, the interface using the automatic discovery feature will not carry traffic. Use the Fortinet Knowledge center article, *Fortinet Discovery Protocol in Transparent mode*, to enable the interface to also carry traffic when using the automatic discovery feature.

### Testing the FortiAnalyzer configuration

After configuring FortiAnalyzer settings, test the connection between the FortiGate unit and FortiAnalyzer unit to verify both devices are communicating properly. When testing the connection, specific settings for transmitting and receiving logs, reports, content archive and quarantine files display.

The FortiGate unit must learn the IP address of the FortiAnalyzer unit before testing the connection. A false test report failure may occur if testing the connection before the FortiGate unit learns the IP address of the FortiAnalyzer unit.

**To test the connection**

1. Go to *Log&Report > Log Config > Log Setting*.
2. Select the blue arrow for FortiAnalyzer to expand the options.
3. Select Test Connectivity.

*Figure 327: Test Connectivity with FortiAnalyzer*

<table>
<thead>
<tr>
<th>FortiAnalyzer (Hostname)</th>
<th>FortiGate (Device ID)</th>
<th>Registration Status</th>
<th>Connection Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiAnalyzer-400</td>
<td>FWFG60N396400005</td>
<td>Registered</td>
<td></td>
</tr>
</tbody>
</table>

### Table

<table>
<thead>
<tr>
<th>Disk Space (MB)</th>
<th>Allocated Space</th>
<th>Used Space</th>
<th>Total Free Space</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>100</td>
<td>1</td>
<td>49/137</td>
</tr>
</tbody>
</table>

#### Privileges

<table>
<thead>
<tr>
<th>Log</th>
<th>Report</th>
<th>Content Archive</th>
<th>Quarantine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx</td>
<td>Rx</td>
<td>Tx</td>
<td>Rx</td>
</tr>
</tbody>
</table>

**FortiAnalyzer (Hostname)** The name of the FortiAnalyzer unit. The default name of a FortiAnalyzer unit is its product name, for example, FortiAnalyzer-400.

**FortiGate (Device ID)** The serial number of the FortiGate unit.

**Registration Status** The registration status of the FortiGate unit.

**Connection Status** The connection status between FortiGate and FortiAnalyzer units. A checkmark indicates there is a connection and an X indicates there is no connection.
You can also test the connection status between the FortiGate unit and the FortiAnalyzer unit by using the following CLI command:

```
execute log fortianalyzer test-connectivity
```

The command displays the status and the amount of disk usage in percent. See the FortiGate CLI Reference for more information.

**Note:** In FortiOS 3.0MR5, the test connectivity feature also provides a warning when a FortiGate unit requires a higher-end FortiAnalyzer unit.

### Logging to memory

The FortiGate system memory has a limited capacity for log messages. It displays the most recent log entries. The FortiGate unit does not store Traffic and Content logs in memory due to their size and frequency of log entries. When the memory is full, the FortiGate unit overwrites the oldest messages. All log entries are cleared when the FortiGate unit restarts.

If your FortiGate unit has a hard disk, use the CLI to enable logging to the FortiGate hard disk. You can also upload logs stored on the hard disk to a FortiAnalyzer unit. See the FortiGate CLI Reference for more information.

**To configure the FortiGate unit to save logs in memory**

2. Select Memory.
3. Select the blue arrow to expand the Memory options.
4. Select the severity level.

The FortiGate unit logs all messages at and above the logging severity level you select. For details on the logging levels, see Table 44, “Log severity levels,” on page 471.
Logging to a Syslog server

A Syslog server is a remote computer running Syslog software and is an industry standard for logging. Syslog is used to capture log information provided by network devices. The Syslog server is both a convenient and flexible logging device, since any computer can run syslog software, such as Linux, Unix, and intel-based Windows systems.

When configuring logging to a Syslog server, you need to configure the facility and log file format, normal or Comma Separated Values (CSV). The CSV format contains commas whereas the normal format contains spaces. Configuring a facility easily identifies the device that recorded the log file.

Figure 328: Logging to a Syslog server

To configure the FortiGate unit to send logs to a syslog server

2. Select Syslog.
3. Select the blue arrow to expand the Syslog options.
4. Set the following syslog options and select Apply:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/IP</td>
<td>The domain name or IP address of the syslog server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number for communication with the syslog server, typically port 514.</td>
</tr>
<tr>
<td>Level</td>
<td>The FortiGate unit logs all messages at and above the logging severity level you select. For details on the logging levels, see Table 44, “Log severity levels,” on page 471.</td>
</tr>
<tr>
<td>Facility</td>
<td>Facility indicates to the syslog server the source of a log message. By default, FortiGate reports Facility as local7. You may want to change Facility to distinguish log messages from different FortiGate units.</td>
</tr>
<tr>
<td>Enable CSV Format</td>
<td>If you enable CSV format, the FortiGate unit produces the log in Comma Separated Value (CSV) format. If you do not enable CSV format the FortiGate unit produces plain text files.</td>
</tr>
</tbody>
</table>

Note: If more than one Syslog server is configured, the Syslog servers and their settings display on the Log Settings page. Configuring multiple Syslog servers is done in the CLI. See the FortiGate CLI Reference for more information.
Logging to WebTrends

WebTrends is a remote computer running a NetIQ WebTrends firewall reporting server. FortiGate log formats comply with WebTrends Enhanced Log Format (WELF) and are compatible with NetIQ WebTrends Security Reporting Center and Firewall Suite 4.1.

Use the command line interface to configure the FortiGate unit to send log messages to WebTrends. After logging into the CLI, enter the following commands:

```plaintext
config log webtrends setting
    set server <address_ipv4>
    set status {disable | enable}
end
```

Example

This example shows how to enable logging to a WebTrends server and to set an IP address for the server.

```plaintext
config log webtrends setting
    set status enable
    set server 220.210.200.190
end
```

See the Log chapter in the FortiGate CLI Reference for details on setting the options for the types of logs sent to WebTrends.

Configuring FortiGuard Analysis Service

You need to register for a FortiGuard Analysis Service trial contract before enabling and configuring your FortiGate unit to use the service. A trial contract provides the contract number for registering the service on the portal. When the contract number is entered at the portal, an account is established. A trial contract is available on the Fortinet support website, at http://support.forticare.com.

After logging into the Fortinet support website, select View Products and then select the FortiGate unit you want associated with your contract. After selecting the Log and Analysis option, the contract number and other contract information displays.

**Caution:** Before logging out of the support website, write down the contract number. You need to have the contract number when registering on the FortiGuard Analysis Service website.
Configuring FortiGuard Analysis Service

Registering an account

After registering for a trial contract, you can then register the contract number and other information on the portal. Before registering on portal, you need to enter a name that uniquely identifies the account from the web-based manager of the FortiGate unit you registered on the support website.

The account ID cannot be changed after entering it in the Account ID field from the FortiGate web-based manager.

To register your contract

1. Log into the FortiGate web-based manager.
2. Select System > Maintenance > FortiGuard Center.
3. Select the blue arrow to expand Management and Analysis Service Options.
4. Enter a name in the Account ID field.
5. Select Apply.
6. Select To launch the service portal, please click here, to go directly to the portal website.
7. Select the Register a new account link.
8. Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account ID</td>
<td>Enter the identification name for the device contract you specified in step</td>
</tr>
<tr>
<td>Account Name</td>
<td>Enter a name for the account, for example, XYN_Company.</td>
</tr>
<tr>
<td>Email</td>
<td>Enter the email address that will enable you to log into the FortiGate Analysis server.</td>
</tr>
<tr>
<td>Re-type Email</td>
<td>Re-enter the email address.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password for accessing your account information.</td>
</tr>
<tr>
<td>Re-type Password</td>
<td>Re-enter the password.</td>
</tr>
<tr>
<td>Security Question 1</td>
<td>Enter a security question for when you need to obtain your password or email address for logging into the website.</td>
</tr>
<tr>
<td>Your Answer</td>
<td>Enter an answer for Security Question One.</td>
</tr>
<tr>
<td>Security Question 2</td>
<td>Enter a second security question for when you need to obtain your password or email address for logging into the website.</td>
</tr>
<tr>
<td>You Answer</td>
<td>Enter an answer for Security Question Two.</td>
</tr>
<tr>
<td>Device SN</td>
<td>Enter the serial number of the FortiGate unit you want associated with the account.</td>
</tr>
<tr>
<td>Contract Number</td>
<td>Enter the contract number you received in the email sent from Fortinet.</td>
</tr>
</tbody>
</table>

9. Select Register.

After the registration process is complete, you are redirected to the FortiGuard Analysis server. It is recommended to verify your connections before configuring your FortiGate unit to log to the FortiGuard Analysis server.
Logging to a FortiGuard Analysis server

You can configure logging to a FortiGuard Analysis server after registering your account. It is recommended to ensure the connection between your FortiGate unit and FortiGuard Analysis server is working properly before configuring logging.

You can enable logging of FortiGate features from the FortiGate web-based manager. See "Log types" on page 481 for more information. Traffic and full content archiving will be supported in future releases.

To configure logging to a FortiGuard Analysis server

1. Log into the web-based manager of the FortiGate unit you want registered.
2. Go to Log&Report > Log Config.
3. Select the FortiGuard Analysis Service checkbox.
4. Select the blue arrow to expand the FortiGuard Analysis Service options.
5. Select one of the following:
   - Overwrite: Select to delete the oldest log entry and continue logging when the maximum log disk space is reached.
   - Do not log: Select to stop log message going to the FortiGuard Analysis server when the maximum log disk space is reached.
6. Select a log severity level.
7. Select Apply.

Accessing logs on the FortiGuard Analysis server

The FortiGuard Analysis server provides both real-time and historical views of log messages. Real-time logs display log information and updates continually, providing recent updates and events occurring on the FortiGate unit. Historical logs display log information for a selected device and log type for a specific time range.

To access real-time logs

1. Log into the portal.
2. Go to Log > Log Viewer > Real-time.
3. Select a device in Devices.
4. Select a log type in Log types.
5. Select OK.

   If you want to change what log type you are currently viewing, select change, next to the Type name. You can also stop real-time logs by selecting Stop. When you want to start real-time logs again, select Start. The option Start only displays when you have selected Stop.

To access historical logs

1. Log into the portal.
2. Go to Log > Log Viewer > Historical.
3. Select the Historical tab.
4. Select a device in Devices.
5 Select a log type in Log Types.

6 Select the Start time by selecting the following:

- **Unspecified**: Select to view log messages from the earliest date and time available in the logs.
- **Specified**: Select to set a specific start date and time for the log messages.
- **Date**: Enter a start date. Use the format YYYY/MM/DD. Alternatively, select the Calendar icon and select a start date.
- **Time**: Select a starting time for the log messages. Leave the time at 00:00 to view log messages starting at 12:00 midnight for the selected date.

7 Select the End time by selecting the following:

- **Current**: Select to include up to the minute log messages.
- **Specified**: Select to set a specific end date and time for the log messages.
- **Date**: Enter a start date. Use the format YYYY/MM/DD. Alternatively, select the Calendar icon and select a start date.
- **Time**: Select an end time for the log messages. Leave the time at 00:00 to view log messages starting at 12:00 midnight for the selected date.

8 Select OK.

See “Accessing logs stored on the FortiGuard Analysis server” on page 487 if you want to view logs from the FortiGate web-based manager that are on the FortiGuard Analysis server.

**FortiGuard Analysis reports**

FortiGuard Analysis Service provides predefined summary reports that contain detailed summary information about network activity during a specific time period, in a graphical format. These predefined summary reports are automatically configured by the FortiGuard Analysis server for each FortiGate unit associated with the account.

A default predefined summary report contains summaries of log information. For example, the top viruses by name. All predefined summary reports can only be viewed from the FortiGuard Analysis server.

**To view FortiGuard Analysis reports**

1 Log into the portal.

2 Go to **Report > Browser**.

3 Select the report name in the Report files column to view the entire report.

You can also select the blue triangle and then select Summary.html to view the entire report. When you select the blue triangle, the size of the report displays.

**Refresh** Select to refresh the list. If the FortiGuard Analysis server is in the process of generating a report, use Refresh to update the status of the report.

**Delete** Select the reports from the listing by selecting the check box next to the report name.

**Device Type** Select the reports based on the type of device included in the report.
You can also view sample reports to see how log data is displayed in a report by selecting Sample Reports on the Report Browse page.

**Log types**

The FortiGate unit provides a wide range of FortiGate features to log, enabling you to better monitor activity that is occurring on your network. For example, you can enable logging IM/P2P. These log messages provide detailed information on the activity occurring on your network of IM/P2P programs and their users.

This topic also provides details on each log type and how to enable logging of the log type.

Before enabling FortiGate features, you need to configure what type of logging device will store the logs. See “Storing Logs” on page 472 for more information.

**Traffic log**

The Traffic Log records all the traffic to and through the FortiGate interfaces. You can configure logging of traffic controlled by firewall policies and for traffic between any source and destination addresses. You can apply the following filters:

- **Allowed traffic**
  - The FortiGate unit logs all traffic that is allowed according to the firewall policy settings.

- **Violation traffic**
  - The FortiGate unit logs all traffic that violates the firewall policy settings.

**Note:** You need to set the logging severity level to Notification when configuring a logging location to record traffic log messages. Traffic log messages generally have a severity level no higher than Notification. If VDOMs are enabled, make sure the VDOM you are currently in allows access for enabling traffic logs.
Enabling traffic logging
Traffic logging records any traffic to or from the interface or VLAN subinterface. You need to set the logging severity level to Notification or lower to record traffic logs.

To enable traffic logging for an interface or VLAN subinterface
1. Go to System > Network > Interface.
2. Select the Edit icon for an interface.
4. Select OK.

Enabling firewall policy traffic logging
Firewall policy traffic logging records the traffic that is both permitted and denied by the firewall policy, based on the protection profile.

To enable firewall policy traffic logging
1. Go to Firewall > Policy.
2. Select the blue arrow to expand the policy list for a policy.
3. Select the Edit icon.
   If required, create a new firewall policy by selecting Create.
5. Select OK.

Event log
The Event Log records management and activity events. For example, when a configuration has changed, or VPN and High Availability (HA) events occur.

To enable the event logs
2. Select from the following logs:
   - **System Activity event** The FortiGate unit logs all system-related events, such as ping server failure and gateway status.
   - **IPSec negotiation event** The FortiGate unit logs all IPSec negotiation events, such as progress and error reports.
   - **DHCP service event** The FortiGate unit logs all DHCP-events, such as the request and response log.
   - **L2TP/PPTP/PPPoE service event** The FortiGate unit logs all protocol-related events, such as manager and socket creation processes.
   - **Admin event** The FortiGate unit logs all administrative events, such as user logins, resets, and configuration updates.
   - **HA activity event** The FortiGate unit logs all high availability events, such as link, member, and state information.
   - **Firewall authentication event** The FortiGate unit logs all firewall-related events, such as user authentication.
Antivirus log

The Antivirus Log records virus incidents in Web, FTP, and email traffic. For example, when the FortiGate unit detects an infected file, blocks a file type, or blocks an oversized file or email that is logged, an antivirus log is recorded. You can apply the following filters:

Virtues: The FortiGate unit logs all virus infections.
Blocked Files: The FortiGate unit logs all instances of blocked files.
Oversized Files/Emails: The FortiGate unit logs all instances of files and email messages exceeding defined thresholds.
AV Monitor: The FortiGate unit logs all instances of viruses, blocked files, and oversized files and email. This applies to HTTP, FTP, IMAP, POP3, SMTP, and IM traffic.

To enable antivirus logs

1. Go to Firewall > Protection Profile.
2. Select the Edit icon beside the protection profile to enable logging of antivirus events.
3. Select the blue arrow to expand the Logging options.
4. Select the antivirus events you want logged.
5. Select OK.

Web filter log

The Web Filter Log records HTTP FortiGuard log rating errors including web content blocking actions.

To enable web filter logs

1. Go to Firewall > Protection Profile.
2. Select edit for a protection profile.
3. Select the blue arrow to expand the Logging options.
4. Select the web filtering events to log.
5. Select the FortiGuard Web Filtering Log rating errors (HTTP only), to log FortiGuard filtering.
6. Select OK.
**Attack log**

The Attack Log records attacks detected and prevented by the FortiGate unit. The FortiGate unit logs the following:

- **Attack Signature**: The FortiGate unit logs all detected and prevented attacks based on the attack signature, and the action taken by the FortiGate unit.
- **Attack Anomaly**: The FortiGate unit logs all detected and prevented attacks based on unknown or suspicious traffic patterns, and the action taken by the FortiGate unit.

**To enable the attack logs**

1. Go to **Firewall > Protection Profile**.
2. Select edit for a protection profile.
3. Select the blue arrow to expand the Logging options.
4. Select Log Intrusions
5. Select OK.

**Note**: Make sure attack signature and attack anomaly settings are enabled to log the attack. The logging options for the signatures included with the FortiGate unit are set by default. Ensure any custom signatures also have the logging option enabled. For details, see “Intrusion Protection” on page 411.

**Spam filter log**

The Spam Filter Log records blocking of email address patterns and content in SMTP, IMAP and POP3 traffic.

**To enable the Spam log**

1. Go to **Firewall > Protection Profile**.
2. Select edit for a protection profile.
3. Select the blue arrow to expand the Logging options.
4. Select the Log Spam.
5. Select OK.

**IM and P2P log**

The Instant Message (IM) and Peer-to-Peer (P2P) log records instant message text, audio communications, and file transfers attempted by users. This type of log file also records the time a transmission was attempted, the type of IM application used, and the content of the transmission.

**To enable IM and P2P logs**

1. Go to **Firewall > Protection Profile**.
2. Select the Edit icon for a protection profile.
3. Select the blue arrow to expand the Logging options.
4. Select Log IM Activity
5. Select Log P2P Activity
6. Select OK.
VoIP log

You can now log Voice over Internet Protocol (VoIP) calls. You can also configure VoIP rate limiting for Session Initiated Protocol (SIP) and Skinny Client Control Protocol (SCCP) or Skinny protocol. SIP and SCCP are two types of VoIP protocols.

Rate limiting is generally different between SCCP and SIP. For SIP, rate limiting is for that SIP traffic flowing through the FortiGate unit. For SCCP, the call setup rate is between the FortiGate unit and the clients because the call manager normally resides on the opposite side of the FortiGate unit from the clients.

To enable VoIP logs
1. Go to Firewall > Protection Profile.
2. Select the Edit icon for a protection profile.
3. Select the blue arrow to expand the Logging options.
4. Select Log VoIP Activity.
5. Select OK.

To configure VoIP activity
1. Go to Firewall > Protection Profile.
2. Select the Edit icon for a protection profile.
3. Select the blue arrow to expand the VoIP options.
4. Select the SIP and SCCP checkboxes.
5. Enter a number for requests per second in the Limit REGISTER request (requests/sec) (SIP only) field.
6. Enter a number for requests per second in the Limit INVITE request (requests/sec) (SIP only) field.
7. Enter a number for the maximum calls per minute in the Limit Call Setup (calls/min) (SCCP only) field.
8. Select OK.

Accessing Logs

The FortiGate unit enables you to view logs stored in memory, hard disk or stored on a FortiAnalyzer unit running FortiAnalyzer 3.0, or on the FortiGuard Analysis server.

Logs are accessed in the Log Access menu. The Log Access menu provides a tab for memory, hard disk, and FortiAnalyzer unit. Each tab provides options for viewing log messages, such as search and filtering options, including selecting the log type you want to view. The FortiGuard tab enables you to view logs stored on the FortiGuard Analysis server.

When accessing logs on a FortiAnalyzer unit, the FortiAnalyzer unit requires running firmware version 3.0 or higher for viewing logs from the FortiGate unit.
Accessing log messages stored in memory

From the Log Access page, you can access logs stored in the FortiGate system memory. Traffic logs are not stored in memory because of the amount of space required to store them.

To view log messages in the FortiGate memory buffer

2. Select the Memory tab.
3. Select a log type from the Log Type list.

Accessing log message stored on the hard disk

You can access logs stored on your FortiGate hard disk, if your FortiGate unit has a hard disk. The logs are accessible the same way as when accessing logs stored on the FortiGate system memory. You can view, navigate, and download logs stored on the hard disk.

To access log files on the hard disk

2. Select the Disk tab.
3. Select a log type from the Log Type list.

Figure 329: Viewing log files stored on the FortiGate hard disk

<table>
<thead>
<tr>
<th>Log Type</th>
<th>File name</th>
<th>Size (bytes)</th>
<th>Last access time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Log</td>
<td>alog.log</td>
<td>4000</td>
<td>Sun Oct 12 20:00 0000</td>
</tr>
<tr>
<td>Attack Log</td>
<td>alog.1</td>
<td>88933</td>
<td>Mon Dec 11 21:43:20 0000</td>
</tr>
</tbody>
</table>

Log Type
Select the type of log you want to view. Some log files, such as the traffic log, cannot be stored to memory due to the volume of information logged.

File name
The name(s) of the log file(s) of that type stored on the FortiGate hard disk.

When a log file reaches its maximum size, the FortiGate unit saves the log files with an incremental number, and starts a new log file with the same name. For example, the current attack log is alog.log. Any subsequent saved logs appear as alog.n, where n is the number of rolled logs.

Size (bytes)
The size of the log file in bytes.

Last access time
The time a log message was made on the FortiGate unit. The time is in the format name of day month date hh:mm:ss yyyy, for example Fri Feb 16 12:30:54 2007.

Clear log icon
Select to clear the current log file. When you select the Clear Log icon, you only delete the current log messages of that log file. The log file is not deleted.

Download icon
Select to download the log file or rolled log file. Select either Download file in Normal format link or Download file in CSV format link. Select the Return link to return to the Disk tab page. Downloading the log file only includes current log messages.
Accessing logs stored on the FortiAnalyzer unit

You can view and navigate through logs saved to the FortiAnalyzer unit. See “Logging to a FortiAnalyzer unit” on page 472 for information about configuring the FortiGate unit to send log files to the FortiAnalyzer unit.

To access log files on the FortiAnalyzer unit

2. Select the FortiAnalyzer tab.
3. Select a log type from the Log Type list.

Figure 330: Viewing log files stored on the FortiAnalyzer unit

| View icon | Display the log file through the web-based manager. |
| Delete icon | Select to delete rolled logs. It is recommended to download the rolled log file before deleting it because the rolled log file cannot be retrieved after deleting it. |

Accessing logs stored on the FortiGuard Analysis server

Log files stored on the FortiGuard Analysis server can also be accessed from the FortiGate web-based manager. After enabling logging to the FortiGuard Analysis server, a FortiGuard tab appears in the Log Access menu. See “Accessing logs on the FortiGuard Analysis server” on page 479 if you want to access logs stored on the portal.

To access log files on the FortiGuard Analysis server

2. Select the FortiGuard tab.

Log Type
Select the type of log you want to view. Some log files, such as the traffic log, cannot be stored to memory due to the volume of information logged.

Page Navigation
Select from the various arrows to go to the next page, previous page, last or first page. You can also enter a number to view that page of log messages. For example, entering the number 5 displays the fifth page.

Column Settings
Select to add or remove columns. See “Column settings” on page 489 for more information.

Raw
Select to view the current log messages in their non-formatted format. By default, the FortiGate unit displays log messages in formatted format.

Clear All Filters
Select to clear all filter settings. See “Filtering log messages” on page 490 for more information.

Note: The FortiAnalyzer unit must be running firmware version 3.0 or higher to view logs from the FortiGate unit.
3 Select a log type from the Log Type list.

Viewing log information

Log information displays in the Log Access menu. Each tab in the Log Access menu displays log information stored on the FortiAnalyzer unit, FortiGate system memory and hard disk if available, including the FortiGuard Analysis server.

The FortiGuard tab enables you to view log messages stored on the FortiGuard Analysis server. The columns that appear reflect the content found in the log file. The top portion of the Log Access page includes navigational features to help you move through the log messages and locate specific information.

Figure 331: Viewing log messages

Customizing the display of log messages

By customizing how log messages display, you can view certain parts of log messages or view different formats of log messages. For example, log messages can be viewed in Formatted view or Raw view. When log messages display in Formatted view, you can customize the columns, or filter log messages. When log messages display in Raw view, the log message displays as it would in the log file.
Filtering is also another way to customize the display of log messages. By using the filter icon, you can display specific information of log messages. For example, you want to display only event log messages that have a severity level of alert. You can only customize columns and filter log messages in Formatted view.

**Note:** If you are filtering log messages, see “Adding filters to web-based manager lists” on page 43 for more information.

**Column settings**

Column Settings enables you to customize the view of log messages in Formatted view. By adding columns, changed the order of columns, or removing columns, you are able to view only the log information you want displayed.

The Column Settings feature is only available when you are viewing logs in Formatted view.

**Figure 332: Column settings for viewing log messages**

![Column settings interface]

**To customize the columns**

2. Select the tab to view logs from, Memory, FortiAnalyzer or FortiGuard.
3. Select a log type from the Log Type list.
4. Select the View icon if you are viewing a log file on a FortiAnalyzer unit.
5. Select the Column Settings icon.
6. Select a column name and select one of the following to change the views of the log information:
   - Move up
   - Move down
   - Select the right arrow to move selected fields from Available fields list to Show these fields in this order list.
   - Select the left arrow to move selected fields from the Show these fields in this order list to the Available fields list.
7. Select OK.
Customizing the display of log messages

Filtering log messages

You can filter log messages by removing, adding or moving columns using the Filter icon. By using the filter icon, you can display specific information of log messages.

Figure 333: Log filters

The filter settings that are applied remain until you log out of the web-based manager. Log filters automatically reset to default settings when you log into the web-based manager.

Note: The Detailed Information column provides the entire raw log entry and is only needed if the log contains information not available in any of the other columns. The VDOM column displays which VDOM the log was recorded in.

Note: See “Adding filters to web-based manager lists” on page 43 for more information about using the filter icons to filter log messages.

To filter log messages

2. Select the tab to view logs from, Memory, FortiAnalyzer or FortiGuard.
3. Select a log type from the Log Type drop-down list.
4. Select the Filter icon in the column to view logs.
5. Select Enable to enable filtering for the column.
6. Enter the appropriate information in the appropriate fields.
7. Select OK.
8. Select the columns to filter in the Filter list.

You can also select the columns that display in the Filter list instead of selecting the actual column.

You can view log messages in Raw format only after configuring the filters. If you want to delete all filter settings, select the Clear All Filters link that displays at the bottom of all filter setting dialog boxes.
The Content Archive menu enables you to view archived logs stored on the FortiAnalyzer unit from the FortiGate web-based manager. The Content Archive menu has four tabs, HTTP, FTP, Email, and IM where you can view each of these archived log types.

Before viewing content archives, you need to enable this feature on your FortiGate unit. Content archiving is enabled from within a protection profile. See “Firewall Protection Profile” on page 329 for more information about enabling content archiving in a protection profile.

You need to enable the following in the protection profile when configuring content summary/archive:

- Antivirus for HTTP
- HTTPS
- Web URL Filter
- HTTPS for Web Filter HTTPS

The FortiGate unit only allows one sixteenth of its memory for transferring content archive files. For example, for FortiGate units with 128RAM, only 8MB of memory is used when transferring content archive files. It is recommended not to enable full content archiving if antivirus scanning is also configured.

**Note:** NNTP options will be supported in future releases.

**Configuring content archiving**

Content archiving is configured and enabled in the Firewall menu. Content archiving is only available when the FortiGate unit is configured to log to a FortiAnalyzer unit. The FortiGuard Analysis Service only provides content summary. If you are logging to the FortiGuard Analysis server, only None and Summary are available in the Archive to FortiAnalyzer/FortiGuard drop-down list.

**To enable content archiving for your FortiGate unit**

1. Go to Firewall > Protection Profile.
2. Select the Edit icon beside a protection profile.
3. Select the blue triangle to expand the Content Archive option.
4. Select the check boxes you require for Display content meta-information on the system dashboard.
5. Select None, Summary or Full from each drop-down list you require for Archive to FortiAnalyzer/FortiGuard.
6. Select the checkbox for Archive SPAMed email to FortiAnalyzer, if required.
7. Select OK.

If you are logging to a FortiGuard Analysis server, you can only select None or Summary for the option, Archive to FortiAnalyzer/FortiGuard. FortiGuard Analysis Service only allows summary content archiving.
Viewing content archives

The Content Archive menu enables you to view all archived logs in the web-based manager. You can view either content archive logs stored on a FortiAnalyzer unit or FortiGuard Analysis server from the Content Archive menu. The FortiGuard Analysis server only stores content summary of logs.

If you require to view logs in Raw format, select Raw beside the Column Settings icon. See “Column settings” on page 489 for more information about the Column Settings icon.

To view content archives

1. Go to Log&Report > Content Archive.
2. Select the tab of the archived log type to view.

To view content summary logs from the FortiGuard Analysis server

1. Go to Log&Report > Content Archive.
2. Select FortiGuard from Select Log Device.
3. Select the tab of the content summary log type to view.

Figure 334: Alert Email options

```
Alert E-mail

SMTP server: [ ]
Email from: [ ]
Email to: [ ]
Authentication: [ ] Enable
SMTP user: [ ]
Password: [ ]

Test Connectivity

Send alert email for the following

- Interval time: 5 (minutes)
- Intrusion detected
- Virus detected
- Web access blocked
- Host status changes
- Violation traffic detected
- Firewall authentication failure
- SSL-VPN login failure
- Administrator login/logout
- IPsec tunnel errors
- HTTPS/FTP/PPPoe errors
- Configuration changes
- FortiGuard license expiry time: 15 (days)
- Disk usage: 75 %
- FortiGuard log quota usage

Send alert email for logs based on severity

Minimum log level: Alert

Apply
```
Alert Email

The Alert Email feature enables the FortiGate unit to monitor logs for log messages, notifying by email of a specific activity or event logged. For example, if you require notification about administrator(s) logging in and out, you can configure an alert email that is sent whenever an administrator(s) logs in and out. This feature sends out an alert email based on the severity level logged as well.

Configuring Alert Email

When configuring alert email, you must configure at least one DNS server. The FortiGate unit uses the SMTP server name to connect to the mail server, and must look up this name on your DNS server.

To configure alert email

1. Go to Log&Report > Log Config > Alert E-mail.
2. Set the following options and select Apply.

   - **SMTP Server**: The name/address of the SMTP email server.
   - **Email from**: The SMTP user name.
   - **Email To**: Enter up to three email recipients for the alert email message.
   - **Authentication Enable**: Select the Authentication Enable check box to enable SMTP authentication.
   - **SMTP user**: Enter the user name for logging on to the SMTP server to send alert email messages. You only need to do this if you have enabled the SMTP authentication.
   - **Password**: Enter the password for logging on to the SMTP server to send alert email. You only need to do this if you selected SMTP authentication.
3. Select Test Connectivity to receive a test email message to the email account you configured in the above step.
4. Select Send alert email for the following if you require sending an email based on one or all of the following:
   - **Interval Time**: Enter the number of minutes before an alert email is sent to the recipient.
   - **Intrusion detected**: Select if you require an alert email message based on intrusion detection.
   - **Virus detected**: Select if you require an alert email message based on virus detection.
   - **Web access blocked**: Select if you require an alert email message based on blocked web sites that were accessed.
   - **HA status changes**: Select if you require an alert email message based on HA status changes.
   - **Violation traffic detected**: Select if you require an alert email message based on violated traffic the FortiGate unit detects.
   - **Firewall authentication device**: Select if you require an alert email message based on firewall authentication.
   - **SSL VPN login failure**: Select if you require an alert email message based on any SSL VPN logins that failed.
   - **Administrator login/logout**: Select if you require an alert email message based on whether the administrator(s) logs in and logs out.
Reports Log&Report

For IPSec tunnel errors, select if you require an alert email message based on whether there is an error in the IPSec tunnel configuration.

For L2TP/PPTP/PPPoE errors, select if you require an alert email message based on errors that occurred in L2TP, PPTP, or PPPoE.

For Configuration changes, select if you require an alert email message based on any changes made to the FortiGate configuration.

For FortiGuard license expiry time (in days), enter the number of days for notification of the FortiGuard license expiry time.

For Disk usage (in percent), enter a number for the percentage of disk usage that an alert email will be sent.

For FortiGuard log disk quota, select if you require an alert email message based on the FortiGuard Analysis server log disk quota.

5 Select Send an alert based on severity if you require sending an alert email based on log severity level. This enables the FortiGate unit to send an alert email whenever a specific log level appears in the log.

6 Select the minimum severity level in the Minimum severity level list.

7 Select Apply.

Note: The default minimum log severity level is Alert. If the FortiGate unit collects more than one log message before an interval is reached, the FortiGate unit combines the messages and sends out one alert email.

Reports

The FortiAnalyzer reporting features are now more integrated with the FortiGate unit. From the Log&Report menu, you can configure a simple FortiAnalyzer report, view the report, and print the report. You can even view content archive logs stored on the FortiAnalyzer unit.

You can configure basic traffic reports from the Log&Report menu. Basic traffic reports use the log information stored in your FortiGate memory to present basic traffic information in a graphical format.

Basic traffic reports

The FortiGate unit uses collected log information and presents it in graphical format to show network usage for a number of services. The charts show the bytes used for the service traffic.

You can view logs from Log&Report > Report Access > Memory.
Time Period

Select a time range to view for the graphical analysis. You can choose from one day, three days, one week or one month. The default is one day. When you refresh your browser or go to a different menu, the settings revert to default.

Services

By default all services are selected. When you refresh your browser or go to a different menu, all services revert to default settings. Deselect the services you do not want to include in the graphical analysis.

- Browsing
- DNS
- Email
- FTP
- Gaming
- Instant Messaging
- Newsgroups
- P2P
- Streaming
- TFTP
- VoIP
- Generic TCP
- Generic UDP
- Generic ICMP
- Generic IP

The report is not updated in real-time. You can refresh the report by selecting the Memory tab.

**Note:** The data used to present the graphs is stored in memory. When the FortiGate unit is reset or rebooted, the data is erased.

**Configuring the graphical view**

The FortiGate basic traffic report includes a wide range of services you can monitor. For example, you can view only email services for the last three days.
To change the graphical information
2. Select the time period to include in the graph from the Time Period list.
3. Deselect the services to not include in the graph. All services are selected by default.
4. Select Apply.

The graph refreshes and displays with the content you specified in the above procedure. The Top Protocols Ordered by Total Volume graph does not change.

Note: If you require a more specific and detailed report, configure a report from the FortiAnalyzer web-based manager or CLI. See “Configuring a FortiAnalyzer report” on page 496 if you require a simple FortiAnalyzer report. The FortiAnalyzer unit can generate over 140 different reports providing you with more options than the FortiGate unit provides.

FortiAnalyzer reports
You can configure a simple FortiAnalyzer report from FortiGate logs in the web-based manager or CLI. If you want to configure a report using the CLI interface, see the FortiGate CLI Reference for more information.

See the FortiAnalyzer Administration Guide for details on how to add and configure additional report profiles.

Note: FortiAnalyzer reports do not appear if the FortiGate unit is not connected to a FortiAnalyzer unit, or if the FortiAnalyzer unit is not running firmware 3.0 or higher.

Configuring a FortiAnalyzer report
You can configure a FortiAnalyzer report from the Report Config menu. The Report Config menu also includes the CLI command, `multi-report`, enabling you to configure multiple FortiAnalyzer reports. The `multi-report` command is disabled by default.

By default, only the default FortiAnalyzer report is available in the Report Config menu. The default FortiAnalyzer report is automatically configured by the FortiAnalyzer unit and is specific to your FortiGate unit. The report is also given a default name, for example, `Default_100281021024`. The default report name is taken from the FortiGate unit identification number.

You can edit either scheduled reports or the default FortiAnalyzer report. See “Editing FortiAnalyzer reports” on page 504 to edit a scheduled report or the default FortiAnalyzer report.

To configure the FortiAnalyzer report profile
1. Log into the CLI.
2. Enter the following commands:
   ```
   config log fortianalyzer settings
       set multi-report enable
   end
   ```
3. Log into the web-based manager.
5. Enter a name for the report.
6 Enter a title for the report.
7 Enter a description of what the report includes, if required.
8 Select the blue arrow next to the options you need to configure:
   - **Properties**: Select to customize the header and footer and include the company name. See “Configuring the report properties” on page 497 for more information.
   - **Report Scope**: Select the type of results to include in the report. See “Configuring the report scope” on page 497 for more information.
   - **Report Types**: Select the types of reports to include. See “Configuring the report types” on page 499 for more information.
   - **Report Format**: Select to resolve host names or rank reports using variables. See “Configuring the report format” on page 499 for more information.
   - **Output**: Select the file format for the reports. See “Configuring the report output” on page 500 for more information.
   - **Schedule**: Configure when the FortiAnalyzer unit runs the report, for example, weekly, or monthly. See “Configuring the report schedule” on page 502 for more information.
   - **Summary Layout**: Configure a customized layout of summarize categories. See “Configuring the summary layout” on page 502 for more information.
9 Select OK.

**Configuring the report properties**

Enter your company’s name, a header comment or a footer for the report. These are optional.

**Figure 336: Report properties options**

<table>
<thead>
<tr>
<th>Properties</th>
<th>Company Name</th>
<th>Header Comment</th>
<th>Footer Comment</th>
<th>Report Title</th>
<th>Custom</th>
</tr>
</thead>
</table>

**Configuring the report scope**

Select the time period and/or log filters for the report. You can select different time periods, for example, if you want the report to include log files from July 31, 2005 to September 9, 2005.

**Figure 337: Report configuration time period**

<table>
<thead>
<tr>
<th>Report Scope</th>
<th>Time Period</th>
<th>Time Period</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Today</td>
<td>From Date 2006 Jan 1 Hour 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To Date 2006 Jan 1 Hour 0</td>
</tr>
</tbody>
</table>
**Time Period**

Select the time period for the report. When you select last n hours, days or weeks, a field will appear. Enter a number in the field, for example, eight, for last n of hours, days of weeks.

**From Date**

Select to configure the start date of the report. For example, you may want to begin the report on May 5, 2005 at 13:00. The hours are in the 24-hour format.

**To Date**

Select to configure the end date of the report.

---

**Figure 338: Report configuration data log filter**

<table>
<thead>
<tr>
<th>Data Filter</th>
<th>None</th>
<th>Custom</th>
</tr>
</thead>
</table>

**Filter logs**

Select None to not apply a filter to the logs in the report. Select Custom to apply filters to the log report.

**Include logs that match**

Select the matching criteria for the filter.

- **Select all** to include logs in the report that match all filter settings. If information within a log does not match all the criteria, the FortiAnalyzer unit will not include the log in the report.
- **Select any** to include logs in the report that match any of the filter settings. If any of the filter content, even one filter setting, matches information in a log file, the log the FortiAnalyzer unit includes the log in the report.

**Priority**

Select the check box to enable the priority level filter options.

Set the priority level to look for in the logs, and set whether the information should be less than, greater than or equal to the priority level.

**Source(s)**

Enter the source IP address for the matching criteria. Use a comma to separate multiple sources.

Select Not to exclude the source IP address from the report. For example, do not include any information from a specific source IP address in the log report.
Configuring the report types

Select the type of information you want to include in the report:

- Select Basic to include the most common report types.
- Select All to include all report types. If data does not exist for a report type, that report will appear with the message “No matching log data for this report.”
- Select Custom to select the reports you want to include. Select the blue arrow to expand the report categories and select individual reports.

Configuring the report format

Select to resolve service names, host names or rank the top items for the report using variables.
Configuring the report output

Select a destination and format(s) for the report. You can select from several different formats, including Text format. You can also select a different format for file output and email output.
When configuring the FortiAnalyzer unit to email a report, you must configure the mail server on the FortiAnalyzer unit. See the FortiAnalyzer Administration Guide for more information or contact a FortiAnalyzer administrator.

**Note:** If you are emailing HTML reports to a user, and their email client does not support HTML, they will see the HTML code for each report in the message body.

**Figure 340: Report configuration output**

- **File output** Select the file format for the generated reports that are saved to the FortiAnalyzer hard disk.
- **Email output** Select the file formats for the generated reports that the FortiAnalyzer unit sends as an email attachment.
- **Email Subject** Enter to customize the subject line of the email.
- **Email attachment name** Enter the name of the attachment sent in the email.
- **Email body** Enter the body of the email message.
- **Email from** Enter the sender’s email address.
- **Email server** Select an email server from the drop-down list.
- **Email to** Enter the recipient’s email address.
- **Email list** Enter the email addresses of the recipients of the report. Add multiple recipients by selecting Add. Select Delete if you want to delete a recipient in the list.
- **Upload Report to FTP Server** Select to upload completed report files to an FTP server.
- **Server Type** Select the type of server to upload the report to. You can select to upload the report to an FTP server, SFTP server, or SCP server.
- **IP address** Enter the IP address of the FTP server.
- **Username** Enter the user name to log onto the FTP server.
- **Password** Enter the password to log onto the FTP server.
- **Upload report(s) in gzipped format** Select to compress the report files as gzip files before uploading to the FTP server.
- **Delete file(s) after uploading** Select to delete the report files from the FortiAnalyzer hard disk after the FortiAnalyzer unit completes the upload to the FTP server.
Configuring the report schedule

Set a schedule for when the FortiAnalyzer unit generates the reports. Choose a recurring schedule, for example, to generate weekly reports on mail traffic.

Figure 341: Report configuration schedule

<table>
<thead>
<tr>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Scheduled</td>
<td>Select to not generate a daily report. Use this setting when you want to run the report as needed.</td>
</tr>
<tr>
<td>Daily</td>
<td>Select to generate the report every day at the same time.</td>
</tr>
<tr>
<td>These Days</td>
<td>Select specific days of the week to generate the report.</td>
</tr>
<tr>
<td>These Dates</td>
<td>Select specific days of the month to generate the report. For example, to generate the report on the first and fifteenth of every month, enter 1, 15.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>Select the time of day when the FortiAnalyzer generates the report.</td>
</tr>
</tbody>
</table>

Configuring the summary layout

Select Customize List to configure a customized layout of charts from the specified categories.

Figure 342: Report summary layout
Viewing FortiAnalyzer reports from a FortiGate unit

The FortiAnalyzer unit can generate a number of specific reports for a FortiGate unit, and run these reports at scheduled times, or on demand. If you are using a FortiGate unit with FortiOS 3.0MR2 or higher, you can view any report generated from the FortiAnalyzer unit for that FortiGate unit on the Report Access page.

To view FortiAnalyzer reports

2. Select Historical Reports.
3. Select the report name to view the report.

Note: The FortiAnalyzer report that appears on the FortiAnalyzer page may not be the report you want to view. Always select Historical Reports to find the report you want to view.

Viewing parts of a FortiAnalyzer report

You can view different parts of a FortiAnalyzer report in the web-based manager. The following procedure enables you to view the Mail Activity section of a report.

To view Mail Filter Activity in a report

2. Select Historical Reports.
3. Select the blue arrow to expand the report.
4. Select MailFilter Activity.html.

Use the above procedure for viewing other sections of a report. For example, select Content Activity.html instead of selecting MailFilter Activity.html.
Editing FortiAnalyzer reports

After a scheduled FortiAnalyzer report is configured and generated, you can then edit the report from the Report Config menu. The FortiAnalyzer tab enables you to edit the report, and view information about other scheduled FortiAnalyzer reports. You can view and edit scheduled reports from the FortiAnalyzer tab. You can also edit the default FortiAnalyzer report that the FortiAnalyzer unit automatically generates for your FortiGate unit.

After enabling the multi-report command from the CLI, the FortiAnalyzer page displays if there is a report currently being generated by the FortiAnalyzer unit, when the next scheduled report will be generated, and if the Report Engine is active or inactive.

To edit a scheduled or default FortiAnalyzer report

2. Select the Edit icon beside a report if you are not editing the default FortiAnalyzer report.
3. Edit the settings you want for the scheduled report.
4. Select OK.

Printing your FortiAnalyzer report

After the FortiAnalyzer unit generates the report, you may want to print the report to have as a hardcopy reference or for a presentation. You can print your report(s) from the web-based manager in the Report Access menu.

To print a FortiAnalyzer report

2. Select Historical Reports.
3. In the list of FortiAnalyzer reports, select the report you want to print.
4. Select Print.

Note: Make sure to check the Report Title of the report displayed on the FortiAnalyzer page before printing.
Index

Numerics
802.1X authentication 226
802.3ad aggregate interface
    creating 86

A
accept action
    firewall policy 273
access control
    access policies, viewing 222
    access policy, configuring 223
    client profile, configuring 221
    client profiles, viewing 221
accessing logs stored in hard disk 486
action
    firewall policy 269
    protection profile P2P option 340
    Spam filter banned word 448
    Spam filter IP address 451
action type
    Spam filter email address 453
active sessions
    HA statistics 141
ActiveX filter
    protection profile 333
add signature to outgoing email
    protection profile 333
address
    firewall address group 291
    list 290
address group 291
    adding 292
    create new 292
    list 291
Address Name
    firewall address 291
administrative access
    interface settings 85, 93, 97
    monitoring logins 177
administrative distance 232
administrator account
    netmask 167, 168
    trusted host 168
administrators, monitoring 177
ADSL 85
adware
    grayware category 408
age limit
    quarantine 406
aggregate interface
    creating 86
AH, predefined service 294
alert email
    options 493
    alert mail messages 154
    Alert Message Console
        clearing messages 57
    allow inbound
        IPSEC firewall policy 280
    allow outbound
        IPSEC firewall policy 280
    allow web sites when a rating error occurs
        protection profile 335
    allowed
        web category report 442
    AMC module 81
    amount, comfort clients
        protection profile 332
anomaly
    destination session limit 420
    flooding 420
    list 419, 421
    scan 420
    source session limit 420
    traffic 420
antispam
    port 53 192
    port 8888 192
antivirus 397
    adware grayware 408
    av_failopen 409
    BHO grayware 408
    CLI configuration 409
    configure antivirus heuristic 409
    dial grayware 408
    download grayware 408
    file block 400
    file block list 401
    game grayware 408
    grayware 193, 407
    heuristics 409
    hijacker grayware 408
    joke grayware 408
    keylog grayware 408
    misc grayware 409
    NMT grayware 409
    optimize 409
    P2P grayware 409
    plugin grayware 409
    quarantine 402
    quarantine files list 403
    RAT grayware 409
    scanning large files 410
    spy grayware 409
    system global av_failopen 409
    system global optimize 409
    toolbar grayware 409
    view virus list 407
Index

virus list 407
antivirus options
protection profile 332
antivirus updates 194
through a proxy server 195
ANY
service 294
AOL
service 294
append to
protection profile 337
append with
protection profile 337
archive content meta-information
protection profile 339
archive IM summary information
protection profile 339
area border routers 253
ARP 305
proxy ARP 305
AS
OSPF 248
ATM 86
attack updates
scheduling 194
through a proxy server 195
Authentication
IPSec VPN, phase 2 352
authentication
firewall policy 274, 276
RIP 248
Authentication Algorithm
IPSec VPN, manual key 355, 356
Authentication Key
IPSec VPN, manual key 356
Authentication Method
IPSec VPN, phase 1 347
authentication, 802.1X 226
Auto Key list
IPSec VPN 345
Autokey Keep Alive
IPSec VPN, phase 2 352
Autonomous System (AS) 256
AutoSubmit
quarantine 406
autosubmit list
configuring 404
enabling uploading 405
quarantine files 404
av_failopen
antivirus 409

B
back to HA monitor
HA statistics 141
backup (redundant) mode
modem 101
backup mode
modem 104
band
wireless setting 121
bandwidth
guaranteed 280
maximum 280
banned word
adding words to the Spam filter banned word list 448
catalog 446
web content block 428, 430
banned word (Spam filter)
action 448
language 448
list 447
pattern 447, 448
pattern type 448
where 448
banned word check
protection profile 337
beacon interval
wireless setting 121, 125
BGP
AS 256
flap 257
graceful restart 257
MED 257
RFC 1771 256
service 294
stabilizing the network 257
BHO
grayware category 408
blackhole routing 93, 234
blades
chassis monitoring 202
block audio (IM)
protection profile 340
block file transfers (IM)
protection profile 340
block login (IM)
protection profile 340
blocked
web category report 442
bookmark
online help icon 39
Boot Strap Router (BSR) 258
BOOTP 132
browsing log information 488

C
catalog
banned word 446
content block 426
content exempt 429
e-mail address back/white list 451
file pattern 400
IP address black/white list 449
URL filter 431
category
protection profile 335
web category report 442
category block
collection options 436
reports 441
Certificate Name
IPSec VPN, phase 1 347
channel
wireless setting 121
channel, wireless setting
FortiWiFi-60 124
chassis monitoring 201
blades 202
FortiGate-5000 modules 202
SMC 201
temperature 203
voltage 204
clear session
predefined signature action 415
CLI
config system global 83
CLI configuration
antivirus 409
web category block 441
cluster member 139
cluster members list 140
priority 140
role 140
cluster unit
connect to a cluster 142
disconnect from a cluster 142
code 298
column settings 489
comfort clients
protection profile 332
comments
firewall policy 275
on documentation, sending 34
concentrator
IPSec VPN, policy-based 357
Concentrator Name
IPSec VPN, concentrator 357
concentrator options
IPSec VPN, concentrator 357
concentrator, equivalent for route-based VPN 344
concentrator, IPSec tunnel mode 357
config antivirus heuristic
CLI command 409
config limit, CLI command for IPS 422
connect to server 86
contact information
SNMP 144
content archive options
protection profile 338
content block
catalog 426
web filter 426
content exempt
catalog 429
content streams, replacement messages 153
contents
online help icon 40
cookie filter
protection profile 333
CPU usage
HA statistics 141
Create New
firewall policy 269
custom service
adding 297
adding a TCP or UDP custom service 297
list 297
custom signature
IPS 417
customer service 35
D
dashboard 49
data encryption
wireless setting 123
date
quarantine files list 403
DC
quarantine files list 403
DCE-RPC
firewall service 294
Dead Peer Detection
IPSec VPN, phase 1 350
default gateway 236
delete after upload
report 501
deny action
firewall policy 273
Designated Routers (DR) 258
dest
firewall policy 269
destination
firewall policy 273
destination network address translation
translation
virtual IPs 307
destination port 298
destination port, custom services 298
destination session limit
anomaly type 420
device priority
HA 137
subordinate unit 142
DH Group
IPSec VPN, phase 1 349
IPSec VPN, phase 2 352
DHCP
and IP Pools 274
service 294
DHCP-IPSec
IPSec VPN, phase 2 352
diagram
topology viewer 67
dial
grayware category 408
dialup VPN
monitor 358
differentiated services
firewall policy 282
differentiated services code point 282
DiffServ
firewall policy 282
disk space
quarantine 406
display content meta-information on dashboard
Index

protection profile option 339
DNAT
  virtual IPs 307
DNS
  service 294
documentation
  commenting on 34
  Fortinet 33
download
  grayware category 408
  quarantine files list 404
drop
  predefined signature action 414
drop sessiondrop
  predefined signature action 415
DSCP 282
duplicates
  quarantine files list 404
Dynamic DNS
  IPSec VPN, phase 1 346
  monitor 358
  on network interface 91
  VPN IPSec monitor 358
dynamic IP pool NAT option
  firewall policy 274
dynamic policy 224
dynamic routing 243
  OSPF 248
  PIM 258

E
ECMP 234
e-mail
  online help icon 39
e-mail address
  action type 453
    adding to the e-mail address list 453
    back/white list catalog 451
    BWL check, protection profile 337
    list, Spam filter 452
    pattern type 453
  e-mail blocked as spam 154
Enable category block (HTTP only)
  protection profile 334
Enable FortiGuard Web Filtering overrides protection profile 334
Enable perfect forward secrecy (PFS)
  IPSec VPN, phase 1 352
Enable replay detection
  IPSec VPN, phase 2 352
enable session pickup
  HA 138
Encryption
  IPSec VPN, phase 2 352
Encryption Algorithm
  IPSec VPN, manual key 355, 356
Encryption Key
  IPSec VPN, manual key 356
end IP
  IP pool 326
EOA 85, 86
Equal Cost Multipath (ECMP) 234
ESP
  service 294
Ethernet over ATM 86
exclude range
  adding to DHCP server 132
expire
  system status 63
Expired 190
external interface
  virtual IP 309
external IP address
  virtual IP 309
external service port
  virtual IP 310

F
fail open 422
FDN
  disruption in traffic 194
  FortiGuard Distribution Network 186
  HTTPS 193
  override server 191
  port 443 193
  port 53 192
  port 8888 192
  port forwarding connection 196
  proxy server 195
  push update 191, 195
  troubleshooting 193
  update center 188
FDN, attack updates 160
FDS
  FortiGuard Distribution Server 186
file block
  antivirus 400
  default list of patterns 402
  list, antivirus 401
  pattern 401
  protection profile 332
file name
  quarantine files list 403
file pattern
  catalog 400
  quarantine autosubmit list 404
filter
  filtering information on web-based manager lists 43
  quarantine files list 403
  web-based manager lists 43
FINGER
  service 294
firewall 267, 289, 293, 301, 305, 329
  address list 290
  configuring 267, 289, 293, 301, 305, 329
  custom service list 297
  one-time schedule 301
  overview 267, 289, 293, 301, 305, 329
  policies for switch ports 275
  policy list 268
  policy matching 268
  predefined services 293
  recurring schedule 302
virtual IP list 308
firewall address
  adding 291
  address group 291
  address name 291
  create new 290
  IP range/subnet 291
  list 290
  name 290
  subnet 291
firewall address group
  adding 292
  available addresses 292
  group name 292
  members 292
firewall IP pool list 326
firewall IP pool options 327
firewall policy
  accept action 273
  action 269
  adding 271
  adding a protection profile 342
  allow inbound 280
  allow outbound 280
  authentication 274, 276
  changing the position in the policy list 270
  comments 275
  configuring 271
  create new 269
  deleting 270
  deny action 273
  dest 269
  destination 273
  differentiated services 282
  DiffServ 282
  dynamic IP pool NAT option 274
  fixed port NAT option 274
  guaranteed bandwidth 280
  ID 269
  inbound NAT 280
  insert policy before 270
  ipsec action 273
  log traffic 274
  maximum bandwidth 280
  modem 106
  move to 270
  moving 270
  outbound NAT 280
  protection profile 274
  schedule 269, 273
  service 269, 273
  source 269, 272
  traffic priority 280
  traffic shaping 275, 278
firewall protection profile
  default protection profiles 330
  list 330
  options 331
firewall service
  AH 294
  ANY 294
  AOL 294
  BGP 294
  DCE-RPC 294
  DHCP 294
  DNS 294
  ESP 294
  FINGER 294
  FTP 294
  FTP_GET 294
  FTP_PUT 294
  Gopher 294
  GRE 294
  H323 294
  HTTP 295
  HTTPS 295
  ICMP_ANY 295
  IKE 295
  IMAP 295
  INFO_ADDRESS 295
  INFO_REQUEST 295
  Internet-Locator-Service 295
  IRC 295
  L2TP 295
  LDAP 295
  NetMeeting 295
  NFS 295
  NNTP 295
  NTP 295
  OSPF 295
  PC-Anywhere 295
  PING 295
  PING6 295
  POP3 295
  PPTP 296
  QUAKE 296
  RAUDIO 296
  REXEC 296
  RLOGIN 296
  RSH 296
  SAMBA 296
  SCCP 296
  SCCP 296
  SIP 296
  SIP-MSNmessenger 296
  SMTP 296
  SNMP 296
  SSH 296
  SYSLOG 296
  TALK 296
  TCP 296
  TELNET 296
  TFTP 296
  TIMESTAMP 296
  UDP 296
  UUCP 297
  VDOLIVE 297
  WAIS 297
  WINFRAME 297
  X-WINDOWS 297
firmware
  upgrading to a new version 59
fixed port
  firewall policy NAT option 274
  IP pool 325
flooding
  anomaly type 420
FortiAnalyzer 29, 473
accessing logs 487
configuring reports 496
editing reports 504
logging to 472
printing reports 504
reports, viewing 503
viewing parts of reports 503
FortiBridge 29
FortiClient 29, 179
FortiGate 4000 81
FortiGate documentation
commenting on 34
FortiGate logging 469
FortiGate MIB 146
FortiGate SNMP event 145
FortiGate traps 147
FortiGate unit
registering 38, 187
FortiGate-100A Rev2.0 82
FortiGate-200A Rev2.0, FortiGate-60B, FortiWiFi-60B 82
FortiGate-224B 26
FortiGate-5000
chassis monitoring 201
FortiGate-5001FA2
introduction 22
FortiGate-5001SX
introduction 22
FortiGate-5002FB2
introduction 22
FortiGate-5020
chassis 21
FortiGate-5050
chassis 21
FortiGate-5140
chassis 21
FortiGate-ASM-FB4 81
FortiGuard 29
changing the host name 441
CLI configuration 441
configuration options 436
configuring 188
licensing 188
report allowed 442
report blocked 442
report category 442
report profiles 442
report range 442
report type 442
reports 441
service points 187
FortiGuard Analysis server
logging to 479
FortiGuard Analysis Service 470
FortiGuard Analysis services
configuring 477
FortiGuard Antispam
email checksum check 336
IP address check 336
Service Point 187
spam submission 336
URL check 336
FortiGuard Distribution Network 186
FortiGuard Distribution Network (FDN) 193
FortiGuard Distribution Server 186
FortiMail 29
FortiManager 29
Fortinet Analysis Service portal website 471
Fortinet customer service 35
Fortinet documentation 33
Fortinet Family Products 29
Fortinet Knowledge Center 34
Fortinet MIB 149
FortiReporter 29
FortiWiFi 60B 82
FortiWiFi-50B
POE 117
wireless settings 120
FortiWiFi-60A
wireless settings 120
FortiWiFi-60AM
wireless settings 120
FortiWiFi-60B
wireless settings 120
fragmentation threshold
wireless setting 124, 125
from IP
system status 63
from port
system status 63, 98
FTP
service 294
FTP.GET
service 294
FTP.PUT
service 294

G

game
grayware category 408
geography
wireless setting 121, 124
GOPHER
service 294
grazeful restart 257
grayware 193
adware 408
antivirus 407
BHO 408
dial 408
download 408
game 408
hijacker 408
joke 408
keylog 408
misc 409
NMT 409
P2P 409
plugin 409
RAT 409
spy 409
toolbar 409
GRE 248
service 294

group name
HA 138

grouping services 299
groups
user 386

guaranteed bandwidth
firewall policy 280
traffic shaping 280

H

H323
service 294

HA 135, 140
changing cluster unit host names 140
cluster logging 472
cluster member 140
cluster members list 139
configuration 135
connect a cluster unit 142
device priority 137
disconnect a cluster unit 142
enable session pickup 138
group name 138
heartbeat interface 138
host name 140
mode 137
out of band management 81
password 138
port monitor 138
router monitor 264
routes 264
session pickup 138
subordinate unit device priority 142
subordinate unit host name 142
VDOM partitioning 138
viewing HA statistics 141

HA statistics
active sessions 141
back to HA monitor 141
CPU usage 141
intrusion detected 141
memory usage 141
monitor 141
network utilization 141
refresh every 141
status 141
total bytes 141
total packets 141
unit 141
up time 141
virus detected 141
heartbeat, HA
interface 138
HELO DNS lookup
protection profile 337
help
navigate using keyboard shortcuts 41
searching the online help 40
heuristics
antivirus 409
quarantine 410
high availability See HA 135

hijacker
grayware category 408
host name
changing for a cluster 140
hostname
cluster members list 140
HTTP
service 295
virus scanning large files 410
HTTPS 37, 160
service 295

I

ICMP custom service 298
code 298
protocol type 298
type 298
ICMP_ANY
service 295
ID
firewall policy 269
IEEE 802.11a, channels 118
IEEE 802.11b, channels 119
IEEE 802.11g, channels 120
IGMP Snooping 218
IKE
service 295
IMAP
service 295
inbound NAT
IPSEC firewall policy 280
index
online help icon 40
INFO_ADDRESS
service 295
INFO_REQUEST
service 295
insert policy before
firewall policy 270
inspect non-standard port (IM)
protection profile 340
interface
administrative access 85, 93, 97
administrative status 81
inter-VDOM link 81
IP pool 327
loopback 81, 234
MTU 85
proxy ARP 305
WAN ports 208
wireless 117
WLAN 117
Interface Mode 82
internet browsing
IPSec VPN configuration 353
Internet-Locator-Service
service 295
interval, comfort clients
protection profile 332
inter-VDOM 75
inter-VDOM link 81
introduction
Fortinet documentation 33
intrusion detected
HA statistics 141
intrusion prevention system, see IPS
IP
virtual IP 309
IP address
Action, Antispam 451
antispam black/white list catalog 449
BWL check, protection profile 337
IPSec VPN, phase 1 346
list, Spam filter 450
Spam filter 449
IP custom service 299
protocol number 299
protocol type 299
IP pool 274
adding 327
configuring 327
create new 326
DHCP 274
end IP 326
fixed port 325
interface 327
IP range/subnet 327, 328
list 326
name 327, 328
options 327
PPPoE 274
proxy ARP 305
start IP 326
IP range/subnet
firewall address 291
IP pool 327, 328
IPOA 85
IPS
anomaly list 419, 421
anomaly, protection profile 338
custom signatures 417
options, protection profile 338
predefined signature action 414
predefined signature list 413
signature 413
signature, protection profile 338
traffic anomaly list 421
IPSec 248
ipsec action
firewall policy 273
ipsec firewall policy
allow inbound 280
allow outbound 280
inbound NAT 280
outbound NAT 280
IPSec Interface Mode
IPSec VPN, manual key 356
IPSec VPN, phase 1 349
IPSec VPN
authentication for user group 387
Auto Key 345
monitor 358
remote gateway 387
IPv6 115, 235
IRC
service 295
ISP 85
J
java applet filter
protection profile 333
joke
grayware category 408
K
Keepalive Frequency
IPSec VPN, phase 1 350
key
wireless setting 123, 125
keyboard shortcut
online help 41
Keylife
IPSec VPN, phase 1 349
IPSec VPN, phase 2 352
keylog
grayware category 408
L
L2TP 387
service 295
language
Spam filter banned word 448
web content block 428, 430
web-based manager 176
LDAP
service 295
license
FortiGuard 188
license key 199
limit (P2P)
protection profile 340
Local certificate
list 369
options 370
Local Gateway IP
IPSec VPN, phase 1 349
Local ID
IPSec VPN, phase 1 350
Local Interface
IPSec VPN, manual key 356
IPSec VPN, phase 1 346
Local SPI
IPSec VPN, manual key 355
log
attack anomaly 484
attack signature 484
column settings 489
messages 488
to FortiAnalyzer 473
traffic, firewall policy 274
log traffic
firewall policy 274
log types 481
antivirus 483
attack 484
event 482
IM, P2P 484
spam filter 484
traffic 481
VOIP 485
web filter 483
logging 486
accessing logs 485
accessing logs in memory 486
accessing logs on FortiAnalyzer unit 487
accessing logs, FortiGuard Analysis server 479
ActiveX filter 341
alert email, configuring 493
basic traffic reports 494
blocked files 341
browsing log messages 488
cluster, HA 472
configuring content archive 491
configuring FortiAnalyzer reports 496
configuring FortiGuard Analysis services 477
connecting using automatic discovery 473
tab content archive 491
tab content block 341
tab cookie filter 341
tab customizing display of log messages 488
tab editing FortiAnalyzer reports 504
FortiGuard Analysis reports 480
IM activity 341
intrusions 341
tab java applet filter 341
tab log severity levels 471
log types 481
oversized files/emails 341
P2P activity 341
predefined signature 414
printing FortiAnalyzer reports 504
rating errors 341
registering a contract, FortiGuard Analysis Service 478
reports 494
searching, filtering logs 490
spam 341
storing logs 472
testing FortiAnalyzer configuration 474
to a FortiAnalyzer unit 472
to FortiGuard Analysis server 479
to memory 475
to syslog server 476
to weebtrends 477
URL block 341
viewing content archives 492
viewing FortiAnalyzer reports 503
viewing parts of FortiAnalyzer reports 503
viewing raw or formatted logs 488
viruses 341
website, Fortinet Analysis Service 471
logs
raw or formatted 488
loopback 234
loopback interface 81, 234
low disk space
quarantine 406
M
MAC address
wireless setting 124
MAC filter
wireless 125
MAC table, switch
creating an entry 228
viewing 228
management VDOM 75
Manual Key list
IPSec VPN 354
map to IP
virtual IP 309
map to port
virtual IP 309, 310
matching
policy 268
max filesizes to quarantine
quarantine 406
maximum bandwidth 280
firewall policy 280
traffic shaping 280
MD5
OSPF authentication 254, 256
Members
IPSec VPN, concentrator 357
memory usage
HA statistics 141
messages, log 488
mheader 454
MIB 146, 149
FortiGate 146
RFC 1213 146
RFC 2665 146
misc
greayware category 409
Mode
HA 137
IPSec VPN, phase 1 347
modem
adding firewall policies 106
backup mode 104
configuring settings 102
redundant (backup) mode 101
standalone mode 101, 105
monitor
administrator logins 177
HA statistics 141
IPSec VPN 358
routing 263
monitoring 227
access results 227
MAC table 228
quarantine information 227
move to
firewall policy 270
MTU 85
MTU size 95, 213
multicast policy 268
Multi-Exit Discriminator (MED) 257
**Index**

**N**

Name
- IP pool 327, 328
- IPSec VPN, manual key 355
- IPSec VPN, Phase 1 346
- IPSec VPN, phase 2 351

NAT
- inbound, ipsec firewall policy 280
- outbound, ipsec firewall policy 280
- push update 196

NAT device
- port forwarding 196
- virtual IP 196

Nat-traversal
- IPSec VPN, phase 1 350

netmask
- administrator account 167, 168

NetMeeting
- service 295

network
- topology viewer 67

network utilization
- HA statistics 141

next
- online help icon 39

NFS
- service 295

NMT
- grayware category 409

NNTP
- service 295

Not Registered 190

Not-so-stubby Area (NSSA) 253

NTP
- service 295

**O**

one-time schedule
- adding 302
- configuring 302
- create new 301
- list 301
- start 302
- stop 302

online help
- keyboard shortcuts 41
- search 40

Operation Mode 159

operation mode
- wireless setting 121, 124

optimize
- antivirus 409

OSPF
- advanced options 252
- area ID 254
- AS 251
- authentication 254, 256
- Dead Interval 256
- Dead interval 256
- dead packets 256
- GRE 255
- Hello Interval 256
- interface definition 255
- IPSec 255
- link-state 248
- LSA 256
- metrics for redistributing routes 252
- multiple interface parameter sets 255
- neighbor 248
- Network 251
- network address space 256
- NSSA 253
- regular area 253
- service 295
- settings 250
- stub 253
- virtual lan 255
- virtual link 253
- VLAN 255
- OSPF AS 248
- defining 249

out of band 81

outbound NAT
- IPSec firewall policy 280
- oversized file/email protection profile 333

**P**

P1 Proposal
- IPSec Phase 1 349

P2 Proposal
- IPSec VPN, phase 2 352

P2P
- grayware category 409

pass
- predefined signature action 414
- pass fragmented email protection profile 332
- pass sessiondrop
- predefined signature action 415

password
- HA 138

PAT
- virtual IPs 308

pattern
- default list of file block patterns 402
- file block 401
- Spam filter banned word 447, 448

pattern type
- Spam filter banned word 448
- Spam filter email address 453
- web content block 428, 430

PC-Anywhere
- service 295

PD
- POE powered device 117

Peer option
- IPSec VPN, phase 1 347

Perl regular expressions
- Spam filter 455

Phase 1
- IPSec VPN 345
- IPSec VPN, phase 2 351
Index

Phase 1 advanced options
IPSec VPN 348

Phase 2
IPSec VPN 350

Phase 2 advanced options
IPSec VPN 351

PIM
BSR 258
dense mode 258
DR 258
RFC 2362 258
RFC 3973 258
RP 258
sparse mode 258

PING
service 295

PING6
firewall service 295

PKI 384
plugin
grayware category 409

POE
FortiWifi-50B 117
power over ethernet 117
wan 1 interface 117

policy
accept action 273
action 269
adding 271
authentication 274, 276
changing the position in the policy list 270
comments 275
configuring 271
create new 269
deleting 270
deny action 273
dest 269
differentiated services 282
DiffServ 282
dynamic IP pool NAT option 274
fixed port NAT option 274
guaranteed bandwidth 280
ID 269
inbound NAT 280
insert policy before 270
ipsec action 273
list 268
log traffic 274
matching 268
maximum bandwidth 280
move 270
move to 270
multicast 268
outbound NAT 280
protection profile 274
schedule 269, 273
service 269, 273
source 269
traffic priority 280
traffic shaping 275, 278
policy-based routing 239

POP3
service 295

port 53 192
port 8888 192
port 9443 196
port address translation
virtual IPs 308
port monitor
HA 138
port monitoring 213
port quarantine 220
power over ethernet
POE 117
PPPoE
and IP Pools 274
RFC 2516 90
PPTP 387
service 296
predefined services 293
predefined signature
action 414
actions 414
clear session action 415
drop action 414
drop session action 415
list 413
logging 414
pass action 414
pass session action 415
reset action 414
reset client action 415
reset server action 415
revision 414

Pre-shared Key
IPSec VPN, phase 1 347
wireless setting 123, 125

previous
online help icon 39
print
online help icon 39
priority
cluster members 140
product registration 38, 187
products, family 29
profile
category block reports 442
proposal
IPSec Phase 1 349
IPSec VPN, phase 2 352
protection profile
action (P2P) 340
ActiveX 333
add signature to outgoing email 333
adding to a firewall policy 342
allow web sites when a rating error occurs 335
amount, comfort clients 332
antivirus options 332
append to 337
append with 337
archive content meta-information 339
archive IM summary information 339
banned word check 337
block audio (IM) 340
block file transfers (IM) 340
Index

block login (IM) 340
category 335
comfort clients 332
content archive options 338
cookie filter 333
default protection profiles 330
display content meta-information on dashboard 339
e-mail address BWL check 337
enable category block (HTTP only) 334
enable FortiGuard Web Filtering overrides 334
file block 332
firewall policy 274
FortiGuard Antispam IP address check 336
FortiGuard Antispam URL check 336
FortiGuard email checksum check 336
FortiGuard spam submission 336
HELO DNS lookup 337
inspect non-standard port (IM) 340
interval, comfort clients 332
IP address BWL check 337
IPS anomaly 338
IPS options 338
IPS signature 338
java applet filter 333
limit (P2P) 340
list 330
logging, ActiveX filter 341
logging, blocked files 341
logging, content block 341
logging, cookie filter 341
logging, IM activity 341
logging, intrusions 341
logging, java applet filter 341
logging, oversized files/emails 341
logging, P2P activity 341
logging, rating errors 341
logging, spam 341
logging, URL block 341
logging, viruses 341
options 331
oversized file/email 333
pass fragmented email 332
provide details for blocked HTTP errors 334
quarantine 332
rate images by URL 335
rate URLs by domain and IP address 335
return email DNS check 337
scan (default protection profile) 330
spam action 337
spam filtering options 336
strict (default protection profile) 330
strict blocking (HTTP only) 335
threshold, banned word check 337
threshold, oversized file/email 333
threshold, web content block 333
unfiltered (default protection profile) 330
virus scan 332
web (default protection profile) 330
web content block 333
web content exempt 333
web filtering options 333
web resume download block 334
web URL block 333
protocol number, custom service 299
service 294
system status 63
type, custom service 298
virtual IP 310
Protocol Independent Multicast (PIM) 258
protocol type 299
provide details for blocked HTTP errors
protection profile 334
proxy ARP 305
FortiGate interface 305
IP pool 305
virtual IP 305
Proxy ID Destination
IPSec interface mode 359
Proxy ID Source
IPSec interface mode 358
proxy server 195
push updates 195
PSE
POE power sourcing equipment 117
push update 191, 195
configuring 195
external IP address changes 196
interface 196
IP addresses change 196
management IP address changes 196
NAT device 196
through a NAT device 196
through a proxy server 195
Q
QoS 218, 282
CoS-Map settings 219
DSCP-Map settings 219
rate limits 219
Qos
global settings 218
QUAKE
service 296
quality of service 282
quarantine
age limit 406
antivirus 402
autosubmit list 404
autosubmit list file pattern 404
configuration 405
configuring the autosubmit list 404
dynamic policy 224
enable AutoSubmit 406
enabling uploading autosubmit file patterns 405
heuristics 410
low disk space 406
max filesize to quarantine 406
monitoring 227
options 406
policies, viewing 224
policy, configuring 224
protection profile 332
quarantine files list
antivirus 403
apply 403
date 403
download 404
duplicates 404
file name 403
filter 403
service 403
sort by 403
status 403
status description 403
TTL 403
upload status 404
Quick Mode Selector
IPSec VPN, phase 2 353
R
RADIUS
WPA Radius 123
RADIUS server
wireless setting 123
RADIUS server name
wireless setting 125
range
web category reports 442
RAT
grayware category 409
rate images by URL
protection profile 335
rate URLs by domain and IP address
protection profile 335
RAUDIO
service 296
read & write access level
administrator account 58, 165, 181
read only access level
administrator account 58, 165, 167
reading log messages 488
reboot 58
recurring schedule
adding 303
configuring 303
create new 302
list 302
select 303
start 303
stop 303
refresh every
HA statistics 141
register
FortiGate unit 38, 187
remote administration 94, 160
Remote Gateway
IPSec manual key setting 356
IPSec VPN, phase 1 346
VPN IPSec monitor field 358
Remote gateway
IPSec VPN, manual key 354
remote peer
manual key configuration 355
Remote SPI
IPSec VPN, manual key 356
Rendezvous Point (RP) 258
report
delete after upload 501
FortiGuard 441
FortiGuard Analysis 480
gzip 501
type, category block 442
upload to FTP 501
web category block 441
reports
basic traffic 494
FortiAnalyzer, configuring 496
FortiAnalyzer, editing 504
FortiAnalyzer, printing 504
FortiAnalyzer, viewing from FortiGate unit 503
FortiAnalyzer, viewing parts of report 503
report scope, FortiAnalyzer 497
reset
predefined signature action 414
reset client
predefined signature action 415
reset server
predefined signature action 415
reset to factory default 58
restarting 186
return email DNS check
protection profile 337
Reverse Path Forwarding (RPF) 260
REXEC
firewall service 296
RFC 258
2474 282
2475 282
RFC 1058 244
RFC 1213 143, 146
RFC 1215 147
RFC 1771 256
RFC 2132 132
RFC 2362 258
RFC 2453 244
RFC 2516 90
RFC 2665 143, 146
RFC 3973 258
RIP
authentication 248
hop count 244
RFC 1058 244
RFC 2453 244
service 296
version 1 244
version 2 244
RLOGIN
service 296
role
cluster members 140
route
HA 264
router monitor
HA 264
routing
configuring 101
ECMP 234
<table>
<thead>
<tr>
<th>Loopback Interface 234</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor 263</td>
</tr>
<tr>
<td>Static 235</td>
</tr>
<tr>
<td>Routing Table 263</td>
</tr>
<tr>
<td>RSH</td>
</tr>
<tr>
<td>Firewall Service 296</td>
</tr>
<tr>
<td>RTS Threshold</td>
</tr>
<tr>
<td>Wireless Setting 124, 125</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAMBA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service 296</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomaly Type 420</td>
</tr>
<tr>
<td>Default Protection Profile 330</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SCCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Service 296</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Antivirus and Attack Definition Updates 194</td>
</tr>
<tr>
<td>Firewall Policy 269, 273</td>
</tr>
<tr>
<td>One-Time Schedule List 301</td>
</tr>
<tr>
<td>Recurring Schedule List 302</td>
</tr>
</tbody>
</table>

| Scheduled Antivirus and Attack Updates 195 |
| Scheduled Updates Through a Proxy Server 195 |
| Scheduling 194 |

<table>
<thead>
<tr>
<th>Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Help 40</td>
</tr>
<tr>
<td>Online Help Icon 40</td>
</tr>
<tr>
<td>Online Help Wildcard 40</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Setting 123, 124</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recurring Schedule 303</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log WebTrends Setting 477</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>AH 294</td>
</tr>
<tr>
<td>ANY 294</td>
</tr>
<tr>
<td>AOL 294</td>
</tr>
<tr>
<td>BGP 294</td>
</tr>
<tr>
<td>Custom Service List 297</td>
</tr>
<tr>
<td>DCE-RPC 294</td>
</tr>
<tr>
<td>DHCP 294</td>
</tr>
<tr>
<td>DNS 294</td>
</tr>
<tr>
<td>ESP 294</td>
</tr>
<tr>
<td>FINGER 294</td>
</tr>
<tr>
<td>Firewall Policy 269, 273</td>
</tr>
<tr>
<td>FTP 294</td>
</tr>
<tr>
<td>FTP_GET 294</td>
</tr>
<tr>
<td>FTP_PUT 294</td>
</tr>
<tr>
<td>Gopher 294</td>
</tr>
<tr>
<td>GRE 294</td>
</tr>
<tr>
<td>Group 299</td>
</tr>
<tr>
<td>HTTPS 295</td>
</tr>
<tr>
<td>ICMP_ANY 295</td>
</tr>
<tr>
<td>IKE 295</td>
</tr>
<tr>
<td>IMAP 295</td>
</tr>
<tr>
<td>Info_Address 295</td>
</tr>
<tr>
<td>Info_Request 295</td>
</tr>
<tr>
<td>Internet-Locator-Service 295</td>
</tr>
<tr>
<td>IRC 295</td>
</tr>
<tr>
<td>L2TP 295</td>
</tr>
<tr>
<td>LDAP 295</td>
</tr>
<tr>
<td>NetMeeting 295</td>
</tr>
<tr>
<td>NFS 295</td>
</tr>
<tr>
<td>NNTP 295</td>
</tr>
<tr>
<td>NTP 295</td>
</tr>
<tr>
<td>Organizing Services into Groups 300</td>
</tr>
<tr>
<td>OSPF 295</td>
</tr>
<tr>
<td>PC-Anywhere 295</td>
</tr>
<tr>
<td>PING 295</td>
</tr>
<tr>
<td>PING6 295</td>
</tr>
<tr>
<td>POP3 295</td>
</tr>
<tr>
<td>PPTP 296</td>
</tr>
<tr>
<td>Predefined 293</td>
</tr>
<tr>
<td>QUAKE 296</td>
</tr>
<tr>
<td>Quarantine Files List 403</td>
</tr>
<tr>
<td>RAUDIO 296</td>
</tr>
<tr>
<td>REXEC 296</td>
</tr>
<tr>
<td>RIP 296</td>
</tr>
<tr>
<td>RLOGIN 296</td>
</tr>
<tr>
<td>RSH 296</td>
</tr>
<tr>
<td>SAMBA 296</td>
</tr>
<tr>
<td>SCCP 296</td>
</tr>
<tr>
<td>Service Name 294</td>
</tr>
<tr>
<td>SIP 296</td>
</tr>
<tr>
<td>SIP-MSN Messenger 296</td>
</tr>
<tr>
<td>SMTP 296</td>
</tr>
<tr>
<td>SNMP 296</td>
</tr>
<tr>
<td>SSH 296</td>
</tr>
<tr>
<td>SYSLOG 296</td>
</tr>
<tr>
<td>TALK 296</td>
</tr>
<tr>
<td>TCP 296</td>
</tr>
<tr>
<td>TELNET 296</td>
</tr>
<tr>
<td>TFTP 296</td>
</tr>
<tr>
<td>TIME-STAMP 296</td>
</tr>
<tr>
<td>UDP 296</td>
</tr>
<tr>
<td>UUCP 297</td>
</tr>
<tr>
<td>VDOLIVE 297</td>
</tr>
<tr>
<td>WAIS 297</td>
</tr>
<tr>
<td>WINFRAME 297</td>
</tr>
<tr>
<td>X-WINDOWS 297</td>
</tr>
</tbody>
</table>

| Service Group 299      |
| Adding 300             |
| Create New 299         |
| List 299               |

| Service Point          |
| FortiGuard 187         |

| Service Port           |
| Virtual IP 309         |

| Session Pickup         |
| HA 138                 |

| Shelf Manager          |
| Chassis Monitoring 201 |
| Shelf Monitoring       |
| Shelf Manager 201      |
| Shortest Path First (SPF) 249 |

| Show in Contents       |
| Online Help Icon 40    |
| Online Help Icon 39    |

| Shutdown               |

518
| **signature** | custom IPS signatures 417  
|              | IPS 413 |
| **SIP**     | service 296 |
| **SIP-MSNmessenger** | service 296 |
| **SMC**     | chassis monitoring 201 |
| **SMTP**   | service 296 |
| **SNMP**   | contact information 144  
|            | MIBs 146  
|            | RFC 12123 146  
|            | RFC 1215 147  
|            | RFC 2665 146  
|            | service 296  
|            | traps 147 |
| **SNMP Agent** | 143 |
| **SNMP communities** | 144 |
| **SNMP community, configuring** | 144 |
| **SNMP manager** | 143 |
| **SNMP managers** | 144 |
| **SNMP, event** | 145 |
| **SNMP, MIB** | 146, 149 |
| **SNMP, queries** | 145 |
| **SNMP, traps** | 145, 147 |
| **sort by** | quarantine files list 403 |
| **source** | firewall policy 269, 272 |
| **source port** | 298 |
| **source session limit** | anomaly type 420 |
| **spam action** | protection profile 337 |
| **Spam filter** | 443 |
|            | adding an email address or domain to the email address list 453 |
|            | adding words to the Spam filter banned word list 448 |
|            | banned word list 447  
|            | email address list 452  
|            | FortiGuard Antispam Service Point 187  
|            | IP address 449  
|            | IP address list 450  
|            | Perl regular expressions 455  
| **spam filtering options** | protection profile 336 |
| **SPAN**   | 213 |
| **Spanning-Tree Protocol** | 214  
|            | global configuration 214  
|            | VLAN configuration 216  
|            | VLAN port settings 218 |
| **spy**    | grayware category 409 |
| **SSH**    | 160  
|            | service 296 |
| **SSID**   | 122  
|            | wireless setting 123, 124  
|            | broadcast |
| **SSL**    | service definition 295 |
| **SSL VPN** | bookmark 366  
|            | bookmark group 367  
|            | checking client certificates 364  
|            | configuration settings 363  
|            | monitoring sessions 365  
|            | setting the cipher suite 364  
|            | specifying server certificate 364  
|            | specifying timeout values 365  
|            | terminating sessions 365  
|            | tunnel IP range 364 |
| **SSL VPN login message** | 157 |
| **Standalone mode** | modem 101, 105 |
| **start**  | one-time schedule 302  
|            | recurring schedule 303 |
| **start IP** | IP pool 326 |
| **static IP** | monitor 358 |
| **static route** | adding 238  
|            | adding policy 240  
|            | administrative distance 232  
|            | concepts 231  
|            | creating 235  
|            | default gateway 236  
|            | default route 236  
|            | editing 235  
|            | overview 231  
|            | policy 239  
|            | policy list 239  
|            | selecting 232  
|            | table building 232  
|            | table priority 233  
|            | table sequence 233 |
| **statistics** | viewing HA statistics 141 |
| **statistics, switch** | viewing 229 |
| **status** | HA statistics 141  
|            | interface 81  
|            | log webtrends setting 477  
|            | quarantine files list 403 |
| **status description** | quarantine files list 403 |
| **stop**   | one-time schedule 302  
|            | recurring schedule 303 |
| **Strict** | default protection profile 330 |
| **strict blocking (HTTP only)** | protection profile 335 |
| **stub**   | OSPF area 253 |
| **subnet** | firewall address 291 |
| **Subscription** | wireless setting 123, 124 |
Expired 190
Not Registered 190
Valid license 190
switch
overview 207
Switch mode 82
switch mode 82
switch-LAN
configuring ports 209, 210
VLAN 211
VLAN, configuring 212
syn interval 59
SYSLOG
service 296
system
chassis monitoring 201
system configuration 135
system global av_failopen
antivirus 409
system global optimize
antivirus 409
system idle timeout 160
T
TALK
service 296
TCP
service 296
TCP custom service 298
adding 297
destination port 298
protocol type 298
source port 298
technical support 35
TELNET
service 296
temperature
chassis monitoring 203
FortiGate-5000 module 203
TFTP
service 296
threshold
banned word check, protection profile 337
oversized file/email, protection profile 333
web content block, protection profile 333
TIMESTAMP
service 296
to IP
system status 63
toolbar
grayware category 409
topology viewer 67
total bytes
HA statistics 141
total packets
HA statistics 141
traffic anomaly 420
list 421
Traffic Priority 280
traffic priority
firewall policy 280
traffic shaping 280
traffic shaping
firewall policy 275, 278
guaranteed bandwidth 280
maximum bandwidth 280
traffic priority 280
transmission options 475
Transparent mode
VLANs 111
traps
SNMP 147
trusted host
administrator account 168
Administrators options 167
security issues 168
TTL
quarantine files list 403
Tunnel Name
IPSec VPN, manual key 354
Tx Power
wireless setting 121, 125
type 298
virtual IP 309
U
UDP custom service 298
adding 297
destination port 298
protocol type 298
source port 298
UDP service 296
Unfiltered
default protection profile 330
unit
HA statistics 141
up time
HA statistics 141
update
push 195
update center 188
upgrade
firmware 59
upload status
quarantine files list 404
URL block
add a URL to the web filter block list 433
web filter 431
URL filter
catalog 431
user authentication
PKI 384
user groups
configuring 386
UUCP
service 297
V
Valid license 190
VDOLIVE
service 297
VDOM
configuration settings 72
license key 199
management VDOM 75
multiple VDOMs 74
NAT/Route 71
Transparent 71
VDOM partitioning
HA 138
Virtual Circuit Identification (VCI) 86
Virtual Domain Configuration 74
virtual IP 305
configuring 309
create new 309, 323
destination network address translation 307
DNAT 307
external interface 309
external IP address 309
external service port 310
IP 309
list 308
map to IP 309
map to port 309, 310
PAT 308
port address translation 308
protocol 310
service port 309
type 309
virus detected
HA statistics 141
virus list 407
view, update 407
virus name 156
virus protection See also antivirus 397
virus scan
protection profile 332
virus-infected attachments 154
VLAN
jumbo frames 95
OSPF 255
overview 107
switch VLAN 211
switch VLAN, configuring 212
VLANs
WAN port 208
voltage
chassis monitoring 204
FortiGate-5000 module 204
VPN tunnel
IPSEC VPN, firewall policy 280
VPN, IPSec 343
auto key 345
concentrator 357
firewall policies 280
interface mode overview 343
manual key 354, 355
Phase 1 configuration 345
Phase 2 configuration 350
VPNs 361, 369
W
WAIS

service 297
WAN
configuring ports 208
VLANs 208
wan1 interface
POE 117
Web
default protection profile 330
web category block
changing the host name 441
CLI configuration 441
configuration options 436
report allowed 442
report blocked 442
report category 442
report profiles 442
report range 442
report type 442
reports 441
web content block
banned word 428, 430
language 428, 430
pattern type 428, 430
protection profile 333
web filter 428
web content block list
web filter 427
web content exempt
protection profile 333
web equivalent privacy 123
Web Filter
URL category 192
web filter 423
add a URL to the web URL block list 433
configuring the web content block list 428
configuring the web URL block list 433
content block 426
URL block 431
web content block list 427
web URL block list 432
web filtering options
protection profile 333
web filtering service 156
web resume download block
protection profile 334
web site, content category 155
web URL block
configuring the web URL block list 433
list 432
list, web filter 432
protection profile 333
web-based manager
language 176
WEP 123, 124
WEP128 118, 123
WEP64 118, 123
where
Spam filter banned word 448
Wi-Fi protected access 123
wildcard
online help search 40
WINFRAME
Index

service 297
wireless
  advanced settings 125
  band 121
  beacon interval 121, 125
  channel 121
  channel, FortiWiFi-60 124
  configuration 117
  data encryption 123
  fragmentation threshold 124, 125
  geography 121, 124
  interface 117
  key 123, 125
  MAC address 124
  MAC filter 125
  operation mode 121, 124
  pre-shared key 123, 125
  RADIUS server 123
  RADIUS server name 125
  RTS threshold 124, 125
  security mode 123, 124
  settings for WiFi-60 124
  settings FortiWiFi-50B 120
  settings FortiWiFi-60A 120
  settings FortiWiFi-60AM 120
  settings FortiWiFi-60B 120
  SSID 123, 124
  SSID broadcast 123, 124

  Tx power 121, 125

Wireless, geography 124
wireless, security 123, 124
Wireless, SSID 123, 124

WLAN
  interface 117
  interface, creating on WiFi-60 124
  wlan interface
    adding to a FortiWiFi-50B 122
    adding to a FortiWiFi-60A 122
    adding to a FortiWiFi-60AM 122
    adding to a FortiWiFi-60B 122
  WPA 118, 123, 124
  WPA Radius
    wireless security 123
  WPA2 118, 123
  WPA2 Auto 118, 123
  WPA2 Radius
    wireless security 123

X

  XAuth
    IPSec VPN, phase 1 350

X-WINDOWS
  service 297