## Contents

Introduction ............................................................................................ 13
Fortinet products .......................................................................................... 13
Before you begin ......................................................................................... 14
How this guide is organized ....................................................................... 14
Document conventions ................................................................................ 15
  - IP addresses .......................................................................................... 15
  - Cautions, Notes and Tips ...................................................................... 15
  - Typographical conventions .................................................................. 15
  - CLI command syntax ........................................................................... 16
Registering your Fortinet product ............................................................ 18
Fortinet products End User License Agreement ......................................... 18
Customer service and technical support .................................................... 18
Training ........................................................................................................ 18
Fortinet documentation ............................................................................. 18
  - Tools and Documentation CD ............................................................. 18
  - Fortinet Knowledge Base ..................................................................... 19
  - Comments on Fortinet technical documentation ................................ 19
Web-based manager .................................................................................. 21
Web-based manager overview ................................................................. 21
Web-based manager menus and pages ...................................................... 21
  - Main menus in the web-based manager .............................................. 23
  - Using web-based manager lists ......................................................... 23
  - Using column settings to control the columns displayed ................. 26
  - Using filters with column settings .................................................... 27
Common web-based manager tasks .......................................................... 27
  - Connecting to the web-based manager .............................................. 27
  - Modifying current settings ................................................................. 28
  - Changing your administrator password ........................................... 28
  - Changing the web-based manager language ..................................... 29
  - Changing administrative access to the unit ...................................... 29
  - Changing the web-based manager idle timeout ............................... 29
  - Switching VDOMs ............................................................................. 29
  - Connecting to the CLI from the web-based manager ....................... 30
  - Contacting Customer Support ........................................................... 30
  - Logging out ......................................................................................... 30
Using online help ....................................................................................... 30
  - Searching the online help ................................................................. 32
System .................................................................................................................. 35
Dashboard ............................................................................................................... 35
  Adding dashboards ............................................................................................. 36
  Adding widgets to a dashboard ............................................................................ 37
  System Information widget ................................................................................ 37
  License Information widget ................................................................................ 41
  Unit Operation widget ......................................................................................... 43
  System Resources widget ..................................................................................... 44
  Alert Message Console widget .......................................................................... 45
  Log and Archive Statistics widget ..................................................................... 46
  CLI Console widget ............................................................................................ 48
  Top Sessions widget ........................................................................................... 49
  Top Viruses widget ............................................................................................. 51
  Top Attacks widget ............................................................................................. 51
  Traffic History widget ......................................................................................... 51
  Top Policy Usage widget .................................................................................... 52
  DLP Archive Usage widget ................................................................................ 53
  RAID monitor ..................................................................................................... 53
  Top Application Usage widget .......................................................................... 56
  Storage widget .................................................................................................... 56
  P2P Usage widget ............................................................................................... 56
  Per-IP Bandwidth Usage widget ....................................................................... 57
  VoIP Usage widget ............................................................................................. 57
  IM Usage widget ................................................................................................. 57
  FortiGuard widget ............................................................................................... 57
## Contents

**Network**
- Interface configuration and settings .......................................................... 58
- Switch Mode .................................................................................................. 63
- Adding VLAN interfaces .............................................................................. 64
- Adding loopback interfaces ............................................................................ 64
- Adding 802.3ad aggregate interfaces .............................................................. 64
- Adding redundant interfaces .......................................................................... 65
- Configuring DHCP on an interface ................................................................. 65
- Configuring PPPoE on an interface ................................................................. 66
- Configuring Dynamic DNS on an interface ..................................................... 67
- Configuring virtual IPSec interfaces ............................................................... 68
- Configuring administrative access to an interface .......................................... 68
- Configuring interface status detection for gateway load balancing .................. 69
- Changing interface MTU packet size .............................................................. 70
- Adding secondary IP addresses to an interface .............................................. 71
- Adding software switch interfaces ................................................................. 72
- Adding an sFlow agent to a FortiGate interface .............................................. 73
- Configuring zones ......................................................................................... 74
- Configuring the modem interface .................................................................. 75
- Configuring Networking Options ................................................................. 79
- DNS Servers .................................................................................................. 80
- FortiGate DNS services .................................................................................. 80
- Configuring the explicit web proxy ............................................................... 85
- Configuring WCCP ....................................................................................... 88
- Routing table (Transparent Mode) ................................................................. 88

**DHCP Server**
- DHCP servers and relays .............................................................................. 89
- Service ........................................................................................................... 90
- Viewing address leases .................................................................................. 92

**Config**
- HA .................................................................................................................. 92
- SNMP .............................................................................................................. 97
- Replacement messages .................................................................................. 99
- Operation mode and VDOM management access .......................................... 112

**Admin**
- Administrators ............................................................................................ 114
- Admin profiles .............................................................................................. 119
- Central Management ..................................................................................... 120
- Settings ......................................................................................................... 121

**Certificates**
- Local Certificates ......................................................................................... 124
- Remote Certificates ...................................................................................... 127
- CA Certificates ............................................................................................ 128
- CRL ................................................................................................................ 129
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless</td>
<td>129</td>
</tr>
<tr>
<td>FortiWiFi wireless interfaces</td>
<td>130</td>
</tr>
<tr>
<td>Wireless settings</td>
<td>130</td>
</tr>
<tr>
<td>Adding a wireless interface</td>
<td>132</td>
</tr>
<tr>
<td>MAC Filter</td>
<td>133</td>
</tr>
<tr>
<td>Wireless Monitor</td>
<td>134</td>
</tr>
<tr>
<td>Rogue AP detection</td>
<td>135</td>
</tr>
<tr>
<td>Viewing wireless access points</td>
<td>135</td>
</tr>
<tr>
<td>Maintenance</td>
<td>136</td>
</tr>
<tr>
<td>Configuration Revision</td>
<td>137</td>
</tr>
<tr>
<td>Firmware</td>
<td>138</td>
</tr>
<tr>
<td>FortiGuard</td>
<td>140</td>
</tr>
<tr>
<td>FortiGuard Distribution Network</td>
<td>140</td>
</tr>
<tr>
<td>FortiGuard services</td>
<td>140</td>
</tr>
<tr>
<td>Configuring the FortiGate unit for FDN and FortiGuard subscription services</td>
<td>141</td>
</tr>
<tr>
<td>Troubleshooting FDN connectivity</td>
<td>145</td>
</tr>
<tr>
<td>Updating antivirus and attack definitions</td>
<td>145</td>
</tr>
<tr>
<td>Enabling push updates</td>
<td>147</td>
</tr>
<tr>
<td>Enabling push updates when a unit’s IP address changes</td>
<td>147</td>
</tr>
<tr>
<td>Enabling push updates through a NAT device</td>
<td>148</td>
</tr>
<tr>
<td>Advanced</td>
<td>150</td>
</tr>
<tr>
<td>Adding VDOM Licenses</td>
<td>152</td>
</tr>
<tr>
<td>Disk</td>
<td>152</td>
</tr>
<tr>
<td>Using virtual domains</td>
<td>155</td>
</tr>
<tr>
<td>Virtual domains overview</td>
<td>155</td>
</tr>
<tr>
<td>VDOMs and global settings</td>
<td>156</td>
</tr>
<tr>
<td>Switching between VDOMs</td>
<td>156</td>
</tr>
<tr>
<td>Per-VDOM configurations</td>
<td>156</td>
</tr>
<tr>
<td>Global configurations</td>
<td>156</td>
</tr>
<tr>
<td>VDOM configuration settings</td>
<td>157</td>
</tr>
<tr>
<td>VDOM licenses</td>
<td>158</td>
</tr>
<tr>
<td>Global VDOM resource limits</td>
<td>158</td>
</tr>
<tr>
<td>Global resource usage for individual VDOMs</td>
<td>159</td>
</tr>
<tr>
<td>Firmware management practices</td>
<td>161</td>
</tr>
<tr>
<td>Backing up your configuration</td>
<td>161</td>
</tr>
<tr>
<td>Backing up your configuration through the web-based manager</td>
<td>162</td>
</tr>
<tr>
<td>Backing up your configuration through the CLI</td>
<td>162</td>
</tr>
<tr>
<td>Backing up your configuration to a USB key</td>
<td>163</td>
</tr>
<tr>
<td>Testing firmware before upgrading</td>
<td>164</td>
</tr>
</tbody>
</table>
Upgrading your FortiGate unit................................................................................... 165
  Upgrading to FortiOS 4.0 through the web-based manager............................... 165
  Upgrading to FortiOS 4.0 through the CLI ......................................................... 166
  Verifying the upgrade......................................................................................... 167
Reverting to a previous firmware image.............................................................. 168
  Downgrading to a previous firmware through the web-based manager .......... 168
  Verifying the downgrade................................................................................... 169
  Downgrading to a previous firmware through the CLI ..................................... 169
Restoring your configuration............................................................................... 171
  Restoring your configuration settings in the web-based manager ................. 171
  Restoring your configuration settings in the CLI ............................................. 171
Router.................................................................................................................... 173
  Static ................................................................................................................... 173
  Static Route ....................................................................................................... 173
  ECMP route failover and load balancing .......................................................... 177
  Policy Route ...................................................................................................... 183
  Dynamic ............................................................................................................ 186
  RIP ..................................................................................................................... 187
  OSPF ................................................................................................................ 189
  BGP ................................................................................................................. 195
  Multicast .......................................................................................................... 196
  Bi-directional Forwarding Detection (BFD) ....................................................... 198
Monitor..................................................................................................................... 199
  Viewing routing information ............................................................................ 199
  Searching the routing monitor table ................................................................. 200
Firewall.................................................................................................................... 203
  Policy ................................................................................................................ 203
  Policy ................................................................................................................. 203
  Identity-based firewall policies ...................................................................... 209
  Central NAT Table ............................................................................................ 212
  IPv6 Policy ....................................................................................................... 213
  DoS Policy ....................................................................................................... 213
  Protocol Options .............................................................................................. 214
  Sniffer Policy ................................................................................................... 216
Address.................................................................................................................... 217
  Address list ...................................................................................................... 218
  Address Group ................................................................................................. 219
Service ................................................................................................................... 220
  Predefined service list ..................................................................................... 220
  Custom services ............................................................................................... 224
  Custom service groups .................................................................................... 225
## Schedule
- Recurring schedule list ................................................................. 226
- One-time schedule list .................................................................... 227
- Schedule groups ............................................................................. 228

## Traffic Shaper
- Shared traffic shapers .................................................................... 229
- Per-IP traffic shaping ....................................................................... 230

## Virtual IP
- Virtual IP, load balance virtual server and load balance real server limitations ..... 231
- Virtual IP ....................................................................................... 231
- VIP group ..................................................................................... 232
- IP pools ......................................................................................... 233

## Load Balance
- Virtual servers ............................................................................... 234
- Real servers ................................................................................... 237
- Health check monitors .................................................................... 238
- Monitoring the servers ................................................................... 240

## UTM
- UTM overview .................................................................................. 241

## AntiVirus
- Profile ............................................................................................. 242
- File Filter ......................................................................................... 243
- Quarantine ........................................................................................ 246
- Virus Database ................................................................................. 247

## Intrusion Protection
- IPS Sensor ...................................................................................... 248
- DoS sensor ....................................................................................... 253
- Predefined ....................................................................................... 256
- Custom ............................................................................................. 257
- Protocol Decoder ............................................................................ 258

## Packet logging
- Packet logging configuration ............................................................ 258

## Web Filter
- Profile ............................................................................................. 259
- Web Content Filter ......................................................................... 261
- URL Filter ....................................................................................... 265
- Override ........................................................................................ 268
- Local Categories ............................................................................... 270
- Local Ratings ................................................................................. 271
- FortiGuard Quota ........................................................................... 271
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Filter</td>
<td>272</td>
</tr>
<tr>
<td>Profile</td>
<td>273</td>
</tr>
<tr>
<td>Banned Word</td>
<td>274</td>
</tr>
<tr>
<td>IP Address</td>
<td>276</td>
</tr>
<tr>
<td>E-mail Address</td>
<td>278</td>
</tr>
<tr>
<td><strong>Using wildcards and Perl regular expressions</strong></td>
<td>279</td>
</tr>
<tr>
<td>Data Leak Prevention</td>
<td>282</td>
</tr>
<tr>
<td>Sensor</td>
<td>282</td>
</tr>
<tr>
<td>Compound rules</td>
<td>284</td>
</tr>
<tr>
<td>Rule</td>
<td>286</td>
</tr>
<tr>
<td>DLP archiving</td>
<td>291</td>
</tr>
<tr>
<td><strong>Application Control</strong></td>
<td>291</td>
</tr>
<tr>
<td>Application Control List</td>
<td>292</td>
</tr>
<tr>
<td>Application List</td>
<td>295</td>
</tr>
<tr>
<td>VoIP</td>
<td>295</td>
</tr>
<tr>
<td>Profile</td>
<td>295</td>
</tr>
<tr>
<td><strong>VPN</strong></td>
<td>299</td>
</tr>
<tr>
<td>IPsec VPN</td>
<td>299</td>
</tr>
<tr>
<td>Auto Key (IKE)</td>
<td>300</td>
</tr>
<tr>
<td>Phase 1 configuration</td>
<td>300</td>
</tr>
<tr>
<td>Phase 2 configuration</td>
<td>304</td>
</tr>
<tr>
<td>Manual Key</td>
<td>306</td>
</tr>
<tr>
<td>Internet browsing</td>
<td>308</td>
</tr>
<tr>
<td>Concentrator</td>
<td>309</td>
</tr>
<tr>
<td>Monitoring VPNS</td>
<td>309</td>
</tr>
<tr>
<td>SSL VPN</td>
<td>310</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>311</td>
</tr>
<tr>
<td>Config</td>
<td>312</td>
</tr>
<tr>
<td>Portal</td>
<td>313</td>
</tr>
<tr>
<td>Virtual Desktop Application Control</td>
<td>316</td>
</tr>
<tr>
<td>Host Check</td>
<td>318</td>
</tr>
<tr>
<td>SSL VPN monitor list</td>
<td>319</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>321</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>321</td>
</tr>
<tr>
<td>Local user accounts</td>
<td>321</td>
</tr>
<tr>
<td>IM users</td>
<td>322</td>
</tr>
<tr>
<td>Authentication settings</td>
<td>323</td>
</tr>
<tr>
<td><strong>User Group</strong></td>
<td>324</td>
</tr>
<tr>
<td>Firewall user groups</td>
<td>325</td>
</tr>
<tr>
<td>Directory Service user groups</td>
<td>326</td>
</tr>
<tr>
<td>SSL VPN user groups</td>
<td>326</td>
</tr>
<tr>
<td>Dynamically assigning VPN client IP addresses from a user group</td>
<td>327</td>
</tr>
</tbody>
</table>
Remote ................................................................. 327
  RADIUS ................................................................. 327
  LDAP ................................................................. 329
  TACACS+ ............................................................... 331
Directory Service ...................................................... 331
PKI ........................................................................ 333
  Peer users and peer groups ........................................ 334
Monitor ...................................................................... 334
  Firewall user monitor list ........................................... 335
  IM user monitor list .................................................. 335
  The Banned User list .................................................. 336
WAN optimization and web caching .......................... 337
  WAN optimization rules ............................................ 337
  WAN optimization peers ............................................ 340
  Peer authentication groups ........................................ 340
  WAN optimization monitoring .................................. 341
  Web cache settings ................................................... 342
  Cache exempt list ...................................................... 344
Endpoint ................................................................... 345
  Endpoint configuration overview ................................ 345
NAC ......................................................................... 346
  Configuring Endpoint profiles .................................. 346
  Configuring application sensors ................................ 347
  Viewing the application database ................................ 348
  Configuring FortiClient installer download and version enforcement .................................... 349
Network Vulnerability Scan ....................................... 350
  Configuring assets ................................................... 350
  Schedule a scan ....................................................... 351
Monitoring endpoints ............................................... 351
Wireless Controller .................................................. 355
  Configuration overview ............................................ 355
  Enabling the wireless controller .................................. 356
  Configuring FortiWiFi units as managed access points .......................................................... 356
  Configuring a virtual wireless access point .................. 356
  Configuring a physical access point ......................... 358
  Configuring DHCP for your wireless LAN .................. 359
  Configuring firewall policies for the wireless LAN .......................................................... 359
  Monitoring wireless clients ....................................... 359
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring rogue APs</td>
<td>360</td>
</tr>
<tr>
<td>Log&amp;Report</td>
<td>363</td>
</tr>
<tr>
<td>Log&amp;Report overview</td>
<td>363</td>
</tr>
<tr>
<td>How a FortiGate unit stores logs</td>
<td>364</td>
</tr>
<tr>
<td>Remote logging to a FortiAnalyzer unit</td>
<td>364</td>
</tr>
<tr>
<td>Remote logging to the FortiGuard Analysis and Management Service</td>
<td>366</td>
</tr>
<tr>
<td>Remote logging to a syslog server</td>
<td>366</td>
</tr>
<tr>
<td>Local logging to memory</td>
<td>367</td>
</tr>
<tr>
<td>Local logging to disk</td>
<td>367</td>
</tr>
<tr>
<td>Local archiving</td>
<td>367</td>
</tr>
<tr>
<td>Event Log</td>
<td>368</td>
</tr>
<tr>
<td>Alert E-mail</td>
<td>369</td>
</tr>
<tr>
<td>Accessing and viewing log messages</td>
<td>370</td>
</tr>
<tr>
<td>Archived logs</td>
<td>371</td>
</tr>
<tr>
<td>Quarantine</td>
<td>371</td>
</tr>
<tr>
<td>Reports</td>
<td>372</td>
</tr>
<tr>
<td>FortiOS reports</td>
<td>373</td>
</tr>
<tr>
<td>Executive Summary reports from SQL logs</td>
<td>378</td>
</tr>
<tr>
<td>FortiAnalyzer report schedules</td>
<td>378</td>
</tr>
<tr>
<td>Index</td>
<td>381</td>
</tr>
</tbody>
</table>
Introduction

Ranging from the FortiGate®-50 series for small businesses to the FortiGate-5000 series for large enterprises, service providers and carriers, the FortiGate line combines the FortiOS™ security operating system with FortiASIC™ processors and other hardware to provide a high-performance array of security and networking functions including:

- firewall, VPN, and traffic shaping
- Intrusion Prevention system (IPS)
- antivirus/antispyware/antimalware
- web filtering
- antivirus
- application control (for example, IM and P2P)
- VoIP support (H.323, SIP, and SCCP)
- Layer 2/3 routing
- multiple redundant WAN interface options

FortiGate appliances provide cost-effective, comprehensive protection against network, content, and application-level threats, including complex attacks favored by cybercriminals, without degrading network availability and uptime. FortiGate platforms include sophisticated networking features, such as high availability (active/active, active/passive) for maximum network uptime, and virtual domain capabilities to separate various networks requiring different security policies.

The following topics are included in this section:

- Fortinet products
- Before you begin
- How this guide is organized
- Registering your Fortinet product
- Fortinet products End User License Agreement
- Customer service and technical support
- Training
- Fortinet documentation

Fortinet products

Fortinet's portfolio of security gateways and complementary products offers a powerful blend of ASIC-accelerated performance, integrated multi-threat protection, and constantly updated, in-depth threat intelligence. This unique combination delivers network, content, and application security for enterprises of all sizes, managed service providers, and telecommunications carriers, while providing a flexible, scalable path for expansion. For more information on the Fortinet product family, go to www.fortinet.com/products.
Before you begin

This FortiGate Version 4.0 MR2 Administration Guide provides detailed information for system administrators about FortiGate™ web-based manager and FortiOS options and how to use them. It is assumed that you have already successfully installed a FortiGate unit by following the instructions in the FortiGate Installation Guide for your model.

At this stage:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.

Once that basic installation is complete, you can use this document. This document explains how to use the web-based manager to:

- maintain the FortiGate unit, including backups
- reconfigure basic items that were configured during installation
- configure advanced features.

This guide also contains some information about the FortiGate command line interface (CLI), but not all the commands. For detailed information on the CLI, see the FortiGate CLI Reference.

This document is intended for administrators, not end users.

How this guide is organized

This section of the guide contains a brief explanation of the structure of the guide and provides a chapter-by-chapter summary. The first chapters provide an overview to help you start using the product or to learn what’s new. Following these chapters, the guide describes web-based manager functions in the same order as the web-based manager (or GUI) menu, and then 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.

You can also learn more about the FortiOS product from the same FortiGate page, as well as from the Fortinet Knowledge Base.

This administration guide contains the following chapters:

- Web-based manager introduces the features of the FortiGate web-based manager, and explains how to connect to it. It also explains how to use the web-based manager online help.
- System introduces you to the System menu.
- Firmware management practices describes upgrading and managing firmware versions. You should review this section before upgrading your FortiGate firmware because it contains important information about how to properly back up your current configuration settings and what to do if the upgrade is unsuccessful.
- Using virtual domains introduces you to how VDOMs are configured and work on the unit.
• **Router** introduces you to the Router menu, which provides settings for configuring dynamic, policy and static routes.

• **Firewall** introduces you to the Firewall menu.

• **UTM** introduces you to the UTM menu, which includes antivirus, data leak prevention and web filtering.

• **VPN** introduces you to the VPN menu, which includes settings for configuring IPSec and SSL. PPTP VPNs are configured in the CLI.

• **User** describes how to control access to network resources through user authentication.

• **WAN optimization and web caching** introduces you to the WAN Opt. & Web Cache menu, which provides settings for helping you to improve performance and security of traffic passing between locations on your wide area network (WAN) or over the Internet.

• **Endpoint** introduces you to the Endpoint menu, which provides settings for enforcing the use of FortiClient End Point Security (Enterprise Edition) in your network.

• **Wireless Controller** introduces you to the Wireless Controller menu.

• **Log&Report** introduces you to the Log&Report menu, which includes reports as well as logging information.

---

**Document conventions**

Fortinet technical documentation uses the conventions described below.

**IP addresses**

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

**Cautions, Notes and Tips**

Fortinet technical documentation uses the following guidance and styles for cautions, notes and tips.

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

- **Note:** Presents useful information, usually focused on an alternative, optional method, such as a shortcut, to perform a step.

- **Tip:** Highlights useful additional information, often tailored to your workplace activity.

**Typographical conventions**

Fortinet documentation uses the following typographical conventions:
Table 1: Typographical conventions in Fortinet technical documentation

<table>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button, menu, text box, field, or check box label</td>
<td>From Minimum log level, select Notification.</td>
</tr>
<tr>
<td>CLI input*</td>
<td>config system dns</td>
</tr>
<tr>
<td></td>
<td>set primary &lt;address_ipv4&gt;</td>
</tr>
<tr>
<td></td>
<td>end</td>
</tr>
<tr>
<td>CLI output</td>
<td>FGT-602803030703 # get system settings</td>
</tr>
<tr>
<td></td>
<td>comments : (null)</td>
</tr>
<tr>
<td></td>
<td>opmode : nat</td>
</tr>
<tr>
<td>Emphasis</td>
<td>HTTP connections are not secure and can be intercepted by a third party.</td>
</tr>
<tr>
<td>File content</td>
<td>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt;&lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</td>
</tr>
<tr>
<td>Keyboard entry</td>
<td>Type a name for the remote VPN peer or client, such as Central Office_1.</td>
</tr>
<tr>
<td>Navigation</td>
<td>Go to VPN &gt; IPSEC &gt; Auto Key (IKE).</td>
</tr>
<tr>
<td>Publication</td>
<td>For more information, see the FortiGate Administration Guide.</td>
</tr>
<tr>
<td></td>
<td>Note: Links typically go to the most recent version. To access earlier releases, go to <a href="http://docs.fortinet.com/">http://docs.fortinet.com/</a>. This link appears at the bottom of each page of this document.</td>
</tr>
</tbody>
</table>

* For conventions used to represent command syntax, see “CLI command syntax” on page 16.

**CLI command syntax**

This guide uses the following conventions to describe syntax to use when entering commands in the Command Line Interface (CLI).

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as &lt;address_ipv4&gt;, indicate which data types or string patterns are acceptable value input.

For more information, see the FortiGate CLI Reference.

Table 2: Command syntax

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Square brackets { }</td>
<td>A non-required word or series of words. For example:</td>
</tr>
<tr>
<td></td>
<td>[verbose {1</td>
</tr>
<tr>
<td></td>
<td>verbose 3</td>
</tr>
</tbody>
</table>
Table 2: Command syntax

| **Angle brackets < >** | A word constrained by data type.
To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (\_) and suffix that indicates the valid data type. For example:
<retries_int>
indicates that you should enter a number of retries, such as 5.
Data types include:
• <xxx_name>: A name referring to another part of the configuration, such as policy_A.
• <xxx_index>: An index number referring to another part of the configuration, such as 0 for the first static route.
• <xxx_pattern>: A regular expression or word with wild cards that matches possible variations, such as *@example.com to match all email addresses ending in @example.com.
• <xxx_fqdn>: A fully qualified domain name (FQDN), such as mail.example.com.
• <xxx_email>: An email address, such as admin@mail.example.com.
• <xxx_ipv4>: An IPv4 address, such as 192.168.1.99.
• <xxx_ipv4range>: An IPv4 address range.
• <xxx_v4mask>: A dotted decimal IPv4 netmask, such as 255.255.255.0.
• <xxx_ipv4mask>: A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0.
• <xxx_ipv4/mask>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as 192.168.1.99/24.
• <xxx_ipv6>: An IPv6 address.
• <xxx_v6mask>: A dotted decimal IPv6 netmask.
• <xxx_ipv6mask>: A dotted decimal IPv6 address and netmask separated by a space.
• <xxx_str>: A string of characters that is not another data type, such as P@ssw0rd. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences.
• <xxx_int>: An integer number that is not another data type, such as 15 for the number of minutes. |

| **Curly braces {}** | A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets []. |

| **Options delimited by vertical bars |** Mutually exclusive options. For example:
{enable | disable}
indicates that you must enter either enable or disable, but must not enter both. |

| **Options delimited by spaces** | Non-mutually exclusive options. For example:
{http https ping snmp ssh telnet}
indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
ping https ssh
**Note:** To change the options, you must re-type the entire list. For example, to add snmp to the previous example, you would type:
ping https snmp ssh
If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted. |
Registering your Fortinet product

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, https://support.fortinet.com. Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration. For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

Fortinet products End User License Agreement

See the Fortinet products End User License Agreement.

Customer service and technical support

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

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at https://support.fortinet.com.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article FortiGate Troubleshooting Guide - Technical Support Requirements.

Training

Fortinet Training Services provides a variety of training programs to serve the needs of our customers and partners world-wide. Visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email training@fortinet.com.

Fortinet documentation

The Fortinet Technical Documentation web site, http://docs.fortinet.com, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Base.

Tools and Documentation CD

The documentation for your product is available on the Fortinet Tools and Documentation CD shipped with your product. The documents on this CD are current at shipping time. For the most current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, http://docs.fortinet.com.
Fortinet Knowledge Base
The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation
Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com
Web-based manager

This section describes the features of the user-friendly web-based manager administrative interface (sometimes referred to as a graphical user interface, or GUI) of your unit. This section also explains common web-based manager tasks that an administrator does on a regular basis, as well as online help.

The following topics are included in this section:

- Web-based manager overview
- Web-based manager menus and pages
- Common web-based manager tasks
- Using online help

Web-based manager overview

The web-based manager is a user-friendly interface for configuring settings as well as managing the unit. Accessing the web-based manager is easy; by using HTTP or a secure HTTPS connection from any management computer running a web browser, you can enter a user name and password to log in to the web-based manager. The recommended minimum screen resolution for properly displaying the web-based manager is 1280 by 1024. You should verify that you have the supported web browser because certain web browsers do not correctly display the information within the web-based manager interface. You can find which web browsers are supported in the Knowledge Base articles, Microsoft Windows WEB browsers supported by Fortinet products web-based manager (GUI) web browsers, and Mac OS browsers for use with Fortinet hardware web-based manager (GUI).

After logging in to the web-based manager, you can use the menus, lists and pages to configure most settings. The web-based manager also provides the CLI Console widget, which allows you to connect to the command line interface (CLI) without exiting out of the web-based manager. Configuration changes made within the web-based manager take effect immediately, without resetting the unit or interrupting service. The web-based manager also includes detailed context-sensitive online help, that displays for the current web-based manager page.

Web-based manager menus and pages

The web-based manager interface consists of main menus, menus and sub-menus. The navigation to get to them is as follows:

System > Dashboard > Status or UTM > Antivirus > Profile.

When you go to a submenu, for example UTM > Antivirus > Profile, you are on that submenu’s page. These pages contains the icons necessary to configure settings, create new lists, as well as customize the display of information.
In Figure 1, the Status page is shown, with Widget and Dashboard located at the top of the page. In Figure 1, you can also see the submenus that are available in the Dashboard menu, as well as the menus within the System main menu. A main menu that is not shown in Figure 1 is the Current VDOM main menu, which appears only when VDOMs are enabled. For more information about the Current VDOM menu, see “Switching VDOMs” on page 29.

Figure 1: Explanation of the web-based manager interface

This topic contains the following:

- Main menus in the web-based manager
- Using web-based manager lists
- Adding filters to web-based manager lists
Main menus in the web-based manager

The web-based manager provides access to configuration options for all major FortiGate features (see Figure 1 on page 22) from the main menus. The web-based manager contains the following main menus:

- **System**: Configure system settings, such as network interfaces, virtual domains, DHCP services, administrators, certificates, High Availability (HA), system time and set system options. The System menu also provides maintenance settings, such as manually updating FortiGuard services, as well as advanced settings. These advanced settings include uploading script files.

- **Router**: Configure static and dynamic routing and view the router monitor. You can also configure multicast routing.

- **Firewall**: Configure firewall policies that apply network protection features. You can also configure virtual IP addresses and IP pools. This menu includes settings for configuring traffic shaping, load balancing and DoS policies.

- **UTM**: Configure antivirus and email filtering, web filtering, intrusion protection, data leak prevention, and application control.

- **VPN**: Configure IPSec and SSL virtual private networking.

- **User**: Configure user accounts for use with firewall policies that require user authentication. Also configure external authentication servers such as RADIUS, LDAP, TACACS+, and Windows AD. Configure monitoring of Firewall, IPSec, SSL, IM, and Banned Users.

- **WAN Opt. & Cache**: Configure WAN optimization and web caching to improve performance and security of traffic passing between locations on your wide area network (WAN) or from the Internet to your web servers.

- **Endpoint**: Configure end points, view FortiClient configuration information, and configure application detection patterns. You can also configure a schedule that will run the network vulnerability scanner at the set times. This can be daily or weekly.

- **Wireless Controller**: Configure the unit to act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi and FortiAP units.

- **Log&Report**: Configure logging and alert email as well as reports. View log messages and reports.

- **Current VDOM**: Appears only when VDOMs are enabled on the unit. Allows you to quickly switch between VDOMs. To switch between VDOMs, select a VDOM from the drop-down list that is beside Current VDOM.

Using web-based manager lists

Many of the web-based manager pages contain lists. The information within these lists can be filtered, so that only specific information is displayed. Only an administrator with read and write access can filter web-based manager lists. Administrators with read-only access can only view web-based manager lists.

Web-based manager lists also contain page controls that help you to navigate through the information on each page.

This topic contains the following:

- **Adding filters to web-based manager lists**

- **Filters for columns that contain numbers**
Filters for columns containing text strings
Filters for columns that can contain only specific items
Custom filters
Using page controls on web-based manager lists

Adding filters to web-based manager lists
You can add filters to control the information that is displayed in complex lists. You can view the following web-based manager pages for examples of lists with filters:

- Firewall policy lists
- DoS policy lists
- Intrusion protection predefined signature lists
- IPSec VPN Monitor lists
- Application control lists (in UTM > Application Control > Application Control List)
- Sniffer policy lists
- IPv6 firewall policy lists
- Firewall user lists (in Endpoint > Monitor > Firewall)
- Log access lists (in Log&Report > Log Access)

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, viewing only log messages that were recorded between 8:00 and 9:00 am.

You add filters to 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 also add filters for one or more columns at a time. The filter icon remains gray 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 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 by selecting NOT to display information that does not match the filter.

Within the firewall policy, IPv6 policy, predefined signature and log and report log access lists, you can combine filters with column settings to provide even more control of the information displayed by the list.

Note: Filter settings are stored in the unit’s configuration and will be maintained the next time that you access any list for which you have added filters.

Filters for columns that contain numbers
If the column includes numbers (for example, IP addresses, firewall policy IDs, or port numbers) you can filter by a single number or a range of numbers. For example, you could configure a source address column to display only entries for a single IP address or for all addresses in a range of addresses. To specify a range, separate the top and bottom values of the range with a hyphen, for example 25-50.

To view the session list, go to System > Dashboard > Status. In the Statistics section, beside Sessions, select Details.
Filters for columns containing text strings

If the column includes text strings (for example, names and log messages) 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.

The text string can be blank and it can also be very long. The text string can also contain special characters such as <, >, \ and so on. However, filtering ignores characters following a < unless the < is followed by a space (for example, filtering ignores <string but not < string>). Filtering also ignores matched opening and closing < and > characters and any characters inside them (for example, filtering ignores <string> but does not ignore >string>).

Filters for columns that can contain only specific items

For columns that can contain only 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.

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 filter to display log messages with multiple severity levels.

Using page controls on web-based manager lists

The web-based manager includes page controls to make it easier to view lists that contain more items than you can display on a typical browser window. Web-based manager pages with page controls include:

- Application Database list (in Endpoint > NAC > Application Database)
- Monitoring routes list (in Router > Monitor > Routing Monitor)
- Predefined signatures list (in UTM > Intrusion Protection > Predefined)
- Application List (in UTM > Application Control > Application List)
- Wireless client list (in Wireless Controller > Wireless Client > Wireless Client)
- Firewall user monitor list (in User > Monitor > Firewall)
- Banned user list (in User > Monitor > Banned User)
- log and report log access lists (in Log&Report > Log Access)
- Endpoint monitor list (in Endpoint > Monitor > Endpoint Monitor)

Figure 2: Page controls

![Page controls diagram]
Using column settings to control the columns displayed

Using column settings, you can format some web-based manager lists so that information that is important to you is easy to find and less important information is hidden or less distracting.

On web-based manager pages that contain complex lists, you can change column settings to control the information columns that are displayed for the list and to control the order in which they are displayed. Web-based manager pages with column settings controls include:

- Network interface list
- Firewall policy and IPv6 policy
- Intrusion protection predefined signatures list
- Firewall user monitor list
- IPSec VPN Monitor
- Endpoint NAC list of known endpoints
- Log and report log access lists.

**Note:** Any changes that you make to the column settings of a list are stored in the unit’s configuration and will display the next time that you access the list.

The following procedure assumes that you are already at the page where you want to change column settings to control how the columns display on the page.

To change column settings

1. From within the page, select Column Settings.
2. From Available Fields, select the column heading to be displayed.
3. Select the right arrow to move the heading to Show these fields in this order.
4. Repeat steps 2 and 3 until all column headings are in Show these fields in this order.
5. To remove a column, select a column heading in Show these fields in this order and use the left arrow to move the column to Available Fields.
6. To change the order of the columns, select the column heading and then select the Move Up or Move Down arrows.

For example, you can change interface list column headings to display only the IP/Netmask, MAC address, MTU, and interface Type for each interface.
Using filters with column settings

On most web-based manager pages that contain lists, you can combine filters with column settings to provide even more control of the information displayed by the list.

For example, you can go to Intrusion Protection > Predefined and configure the Intrusion Protection predefined signatures list to show only the names of signatures that protect against vulnerabilities for a selected application. To do this, set Column Settings to only display Applications and Name. Then apply a filter to the Applications column so that only selected applications are listed. In the pre-defined signatures list you can also sort the list by different columns; you might want to sort the list by application so that all signatures for each application are grouped together.

Common web-based manager tasks

This topic describes how to do common web-based manager tasks that occur when first setting up the unit, as well as afterward. A common web-based manager task that an administrator may do on a regular basis is switch VDOMs, log out, or change another administrator’s password. You should change administrator passwords on a regular basis for improved security.

This topic describes the following common web-based manager tasks:

- Connecting to the web-based manager
- Modifying current settings
- Changing your administrator password
- Changing the web-based manager language
- Changing administrative access to the unit
- Changing the web-based manager idle timeout
- Switching VDOMs
- Connecting to the CLI from the web-based manager
- Contacting Customer Support
- Logging out

Connecting to the web-based manager

When first connecting to the web-based manager, you require the following:

- a unit connected to your network according to the instructions in the QuickStart Guide and Install Guide for that unit
- the IP address of a FortiGate interface that you can connect to
- a computer with an Ethernet connection to a network that can connect to the unit
- a supported web browser. See the Knowledge Base articles Microsoft Windows WEB browsers supported by Fortinet products web-based manager (GUI) web browsers and Mac OS browsers for use with Fortinet hardware web-based manager (GUI).
To connect to the web-based manager

1. Start your web browser and browse to https:// followed by the IP address of the unit’s interface that you can connect to.

For example, if the IP address is 192.168.1.99, browse to https://192.168.1.99. (remember to include the “s” in https://).

To support a secure HTTPS authentication method, the unit ships with a self-signed security certificate, which is offered to remote clients whenever they initiate a HTTPS connection to the unit. When you connect, the unit displays two security warnings in a browser.

The first warning prompts you to accept and optionally install the unit’s self-signed security certificate. If you do not accept the certificate, the unit refuses the connection.

If you accept the certificate, the login page appears. The credentials entered are encrypted before they are sent to the unit. If you choose to accept the certificate permanently, the warning is not displayed again.

Just before the login page is displayed, a second warning informs you that the FortiGate certificate distinguished name differs from the original request. This warning occurs because the unit redirects the connection. This is an informational message. Select OK to continue logging in.

2. Type admin or the name of a configured administrator in the Name field.

3. Type the password for the administrator account in the Password field.

4. Select Login.

Modifying current settings

When you are modifying current settings, such as changing an administrator’s password, you must highlight the item and then select the icon because all available icons are not accessible otherwise. This way of accessing icons is explained in the following procedure.

Use the following procedure whenever you are modifying current settings.

To access icons for modifying items within a list

1. In the Check box column, within the row of the setting you want to change, select the check box to highlight the row.

   The grayed icons are now accessible. On some pages, all icons may not be accessible when you highlight the row.

2. With the icon or icons now accessible, select the icon that you want to use to make modifications with (such as the Edit icon).

   After the modifications are made, and you are back to the list on the page, the check box is unselected and the row unhighlighted.

Changing your administrator password

By default, you can log in to the web-based manager by using the admin administrator account and no password. You should add a password to the admin administrator account to prevent anybody from logging in to the unit and changing configuration options. For improved security, you should regularly change the admin administrator account password and the passwords for any other administrator accounts that you add.

To change an administrator’s password, go to System > Admin > Administrators, edit the administrator account, and then change the password. Select OK to save the new password.
You can also add new administrator accounts by selecting Create New. For more information about adding administrators, changing administrator account passwords and related configuration settings, see “Admin” on page 114.

**Note:** If you forget or lose an administrator account password and cannot log in to the unit, see the Fortinet Knowledge Base article Recovering a lost FortiGate administrator account password.

### Changing the web-based manager language

You can change the web-based manager to display language in English, Simplified Chinese, Japanese, Korean, Spanish, Traditional Chinese, or French. For best results, you should select the language that the management computer operating system uses.

To change the language, go to System > Admin > Settings, and under Display Settings, select the language you want from the Language drop-down list, and select Apply. The web-based manager pages display the chosen language.

### Changing administrative access to the unit

Through administrative access, an administrator can connect to the unit to view and change configuration settings. The default configuration allows administrative access to one or more of the unit’s interfaces as described in your unit’s QuickStart Guide and Install Guide.

You can change administrative access by:

- enabling or disabling administrative access from any FortiGate interface
- enabling or disabling securing HTTPS administrative access to the web-based manager (recommended)
- enabling or disabling HTTP administrative access to the web-based manager (not recommended)
- enabling or disabling secure SSH administrative access to the CLI (recommended)
- enabling or disabling SSH or Telnet administrative access to the CLI (not recommended).

To change administrative access, go to System > Network > Interface, edit the administrator, and select the administrative access type or types for that interface. Select OK to save the changes.

### Changing the web-based manager idle timeout

By default, the web-based manager disconnects administrative sessions if no activity takes place for five minutes. This idle timeout is recommended to prevent someone from using the web-based manager from a PC that is logged in to the web-based manager and then left unattended.

To change the idle timeout, go to System > Admin > Settings, and under Idle Timeout enter the time in minutes, and then select Apply to save the changes.

### Switching VDOMs

When VDOMs are enabled, a menu appears in the left column called Current VDOM. This menu displays a drop-down list beside it. The drop-down list contains all the configured VDOMs on that unit. This provides an easy, quick way to access a VDOM.

To switch to a VDOM using the Current VDOM menu, select the VDOM that you want to switch to from the drop-down list beside Current VDOM. You are automatically redirected to that VDOM.
Connecting to the CLI from the web-based manager

You can connect to the CLI from the web-based manager dashboard by using the CLI console widget. You can use the CLI to configure all configuration options available from the web-based manager. Some configuration options are available only from the CLI. As well, you can use the CLI to enter diagnose commands and perform other advanced operations that are not available from the web-based manager. For more information about the CLI, see the FortiGate CLI Reference.

To connect to the CLI console, go to System > Dashboard > Status, and in the CLI Console widget select inside the window. You are automatically logged in to the CLI. For more information, see “CLI Console widget” on page 48.

Contacting Customer Support

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

- visit the Fortinet Knowledge Base
- log into Customer Support (Support Login)
- register your Fortinet product (Product Registration)
- view Fortinet Product End of Life information
- find out about Fortinet Training and Certification
- visit the FortiGuard Center.

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

Logging out

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. To change the timeout, see “Changing the web-based manager idle timeout” on page 29.

Using online help

The Online Help button displays context-sensitive online help for the current web-based manager page. The online help page that is displayed is called a content pane and contains information and procedures related to the current web-based manager page. Most help pages also contain hyperlinks to related topics. The online help system also includes a number of links that you can use to find additional information.
To view the online help table of contents or index, and to use the search feature, select Online Help in the button bar in the upper right corner of the web-based manager. From the online help, select Show Navigation.
Searching the online help

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

- If you search for multiple words, the search finds only those 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 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 finds only 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 online help system

1. From any web-based manager page, select the online help button.
2. Select Show Navigation.
3. Select Search.
4. In the search field, enter one or more words to search for and then press the Enter key on your keyboard or select Go.

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

Figure 5: Searching the online help system

Using the keyboard to navigate in the online help

You can use the keyboard shortcuts listed in Table 3 to display and find information in the online help.

Table 3: Online help navigation keys

<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> if you have comments on or corrections 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, to make it easier to find useful online help pages.</td>
</tr>
</tbody>
</table>
System

This section introduces you to the System menu. If you require more information about the features within the System menu, see the FortiOS Handbook.

This section contains the following topics:

- Dashboard
- Network
- DHCP Server
- Config
- Admin
- Certificates
- Maintenance
- FortiGuard

Dashboard

The Dashboard menu provides a way to view network activity and events, as well as configure system settings, such as the unit’s system time or enabling VDOMs. The Dashboard menu contains submenus that are referred to as dashboards. There are two default dashboards, Status and Usage, and you can customize these default dashboards to your requirements including renaming them. The dashboards that you create are automatically added to the Dashboard menu, under the default dashboards.

Network activity and events are viewed on dashboards using widgets. Widgets provide an easy and quick way to view a variety of information, such as statistical or log information. Widgets are added to dashboards after you have created a dashboard. The two default dashboards contain certain widgets already; however, you can remove these widgets, add widgets, or modify the widgets.

Dashboards can be used to view specific information, such as log information. For example, the Archives dashboard (System > Dashboard > Archives) contains the DLP Archive Usage and Log and Archive Statistics widgets, allowing users to view only log archive information.

Administrators must have read and write privileges for configuring dashboards as well as adding widgets to dashboards.

This topic includes the following:

- Adding dashboards
- Adding widgets to a dashboard
- System Information widget
- License Information widget
- Unit Operation widget
- System Resources widget
- Alert Message Console widget
- Log and Archive Statistics widget
• CLI Console widget
• Top Sessions widget
• Top Viruses widget
• Top Attacks widget
• Traffic History widget
• Top Policy Usage widget
• DLP Archive Usage widget
• RAID monitor
• Top Application Usage widget
• Storage widget
• P2P Usage widget
• Per-IP Bandwidth Usage widget
• VoIP Usage widget
• IM Usage widget
• FortiGuard widget

Note: Your browser must support Java script to view the System Dashboard page.

The Topology Viewer is not included in FortiOS 4.0 MR2. If upgrading to FortiOS 4.0 MR2, all Topology Viewer configuration settings will be lost.

Adding dashboards

Dashboards that you create are automatically added under the default status and usage dashboards. You can add, remove or rename a dashboard, regardless of whether it is default. You can also reset the Dashboard menu to its default settings by selecting Reset Dashboards.

Note: If VDOMs are enabled, only the dashboards within Global are available for configuration.

To add a dashboard to the dashboard menu

1. Go to System > Dashboard > Status.
2. Select Dashboard, located at the top of the page.
3. A drop-down list appears with the following options:
   - Add Dashboard: Add a new dashboard to the Dashboard menu.
   - Rename Dashboard: Rename the current dashboard. You can rename the existing default menus Status and Usage.
   - Delete Dashboard: Removes the current dashboard that you are viewing.
   - Reset Dashboards: Resets the entire Dashboard menu back to its default settings.
4. Select Add Dashboard.
5. Enter a name for the dashboard in the Name field in the Add Dashboard window.
6 Select OK.
   You are automatically redirected to the new dashboard. You can start adding widgets to
   the dashboard.

Adding widgets to a dashboard

After adding a dashboard to the Dashboard menu, you can add multiple widgets to that
dashboard. You can customize most widgets to display specific information, and with
some widgets, you can view more detailed information.

To add a widget to a dashboard, select Widget (located at the top of the dashboard page),
and then select a widget in the Click active module name to add module to the page
window.

Figure 6: A minimized display

Explanation of a widget's title bar area

<table>
<thead>
<tr>
<th>Widget Title</th>
<th>History</th>
<th>Open/Close arrow</th>
<th>Refresh</th>
<th>Close</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shows the name of the display</td>
<td>Select to open or close the display.</td>
<td>Select to show an expanded set of data. Not available for all widgets.</td>
<td>Select to update the displayed information.</td>
<td>Select to close the display. You will be prompted to confirm the action.</td>
</tr>
</tbody>
</table>

Note: The information that appears on the Status page applies to the whole HA cluster, not
just the primary unit. This includes information such as URLs visited, emails sent and
received, as well as viruses caught.

System Information widget

The System Information widget contains general system information, such as the unit’s
serial number, as well as the firmware version that is currently running. This widget also
provides settings for backing up or restoring configuration settings, changing the operation
mode, enabling or disabling virtual domains, and changing the currently logged in
administrator’s password.

By default, the System Information widget is found on the Status page (System >
Dashboard > Status).

System Information widget

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Uptime</th>
</tr>
</thead>
</table>
| The serial number of the unit. The serial number is specific to that unit and
does not change with firmware upgrades. | The time in days, hours, and minutes since the unit was started. |
System Time
The current date and time according to the unit’s internal clock. When you select Change, you are automatically redirected to the Time Settings page where you can change the unit’s system time. See “Configuring system time” on page 39.

HA Status
The status of high availability for this unit.
Standalone indicates the unit is not operating in HA mode.
Active-Passive or Active-Active indicate the unit is operating in HA mode.
When you select Configure, you are automatically redirected to the High Availability page. See “HA” on page 92.

Cluster Name
The name of the HA cluster for this unit.
The unit must be operating in HA mode to display this field.

Cluster Members
The units in the HA cluster. Information displayed about each member includes host name, serial number, and whether the unit is a primary (master) or subordinate (slave) unit in the cluster.
The unit must be operating in HA mode with virtual domains disabled to display this field.

Virtual Cluster 1
The role of each unit in virtual cluster 1.

Virtual Cluster 2
The role of each unit in virtual cluster 2.

Host Name
The host name of the current FortiGate unit. When you select Change, you are automatically redirected to the Edit Host Name page. See “Changing the unit’s host name” on page 39.
If the unit is in HA mode, this field is not displayed.

Firmware Version
The version of the current firmware installed on the unit. When you select Update, you are automatically redirected to the Firmware Update/Downgrade page. See “Changing the firmware” on page 40.

System Configuration
The time period of when the configuration file was backed up. You can select Backup to back up the current configuration; when you select Backup, you are automatically redirected to the Backup page. If you want to restore a configuration file, select Restore; when you select Restore, you are automatically redirected to the Restore page.

FortiClient Version
The currently version of FortiClient uploaded to your unit used for endpoint control. For more information, see “Configuring FortiClient installer download and version enforcement” on page 349.

Operation Mode
The operating mode of the current unit. A unit can operate in NAT mode or Transparent mode. Use to switch between NAT and Transparent mode. When you select Change, you are automatically redirected to the Mode page. See “Changing the operation mode” on page 112.
If virtual domains are enabled, this field shows the operating mode of the current virtual domain. Each virtual domain can be operating in either NAT mode or Transparent mode.
If virtual domains are enabled, the Global System Status dashboard does not include this field.

Virtual Domain
Status of virtual domains on your FortiGate unit. Select Enable or Disable to change the status of virtual domains feature.
If you enable or disable virtual domains, your session will be terminated and you will need to log in again.

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

Current User
The name of the admin account that you have used to log into the FortiGate unit. If you are authenticated locally by password, not by PKI or remote authentication, you can select Change Password to change the password for this account. When you change the password, you are logged out and must log back in with the new password.
### Configuring system time

The unit’s system time can be changed in the System Information widget. You can also view what time it is in the System Time row of the System Information widget.

Use the following table to change the unit’s current time and zone, or to synchronize the unit’s internal clock with an NTP server.

#### Time Settings page

<table>
<thead>
<tr>
<th><strong>System Time</strong></th>
<th>The current system date and time on the unit.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Refresh</strong></td>
<td>Update the display of the unit’s current system date and time.</td>
</tr>
<tr>
<td><strong>Time Zone</strong></td>
<td>Select the current system time zone for the unit.</td>
</tr>
<tr>
<td><strong>Automatically adjust clock for daylight saving changes</strong></td>
<td>Select to automatically adjust the system clock when your time zone changes between daylight saving time and standard time.</td>
</tr>
<tr>
<td><strong>Set Time</strong></td>
<td>Select to set the system date and time to the values you set in the Hour, Minute, Second, Year, Month and Day fields.</td>
</tr>
<tr>
<td><strong>Synchronize with NTP Server</strong></td>
<td>Select to use a Network Time Protocol (NTP) server to automatically set the system date and time. You must specify the server and synchronization interval.</td>
</tr>
</tbody>
</table>


| **Server** | Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, see [http://www.ntp.org](http://www.ntp.org). |
| **Sync Interval** | Specify how often the unit should synchronize its time with the NTP server. For example, a setting of 1440 minutes causes the unit to synchronize its time once a day. |

### Changing the unit’s host name

The host name appears in the Host Name row, in the System Information widget. The host name also appears at the CLI prompt when you are logged in to the CLI. The host name is also used as the SNMP system name.

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

Administrators whose admin profiles permit system configuration write access can change the unit’s host name.

If the host name is longer than 16 characters, it will be displayed as being truncated and end with a “~”. The full host name will be displayed under System > Status > Dashboard, but the truncated host name will be displayed on the CLI and other places it is used. If the unit is part of an HA cluster, you should use a unique host name to distinguish the unit from others in the cluster.

To change the host name on the unit, within the System Information widget, select Change in the Host Name row. When you select Change, you are automatically redirected to the Edit Host Name page. In the New Name field, enter the new host name for the unit and then select OK.

The new host name is displayed in the Host Name field and the CLI prompt. It is also added to the SNMP System Name.
Changing the firmware

**Caution:** By installing an older firmware image, some system settings may be lost. You should always back up your configuration before changing the firmware image.

Administrators whose admin profiles permit maintenance read and write access can change the unit’s firmware. Firmware images can be installed from a number of sources including a local hard disk, a local USB disk, or the FortiGuard Network. Firmware changes either upgrade to a newer version or revert to an earlier version. Follow the appropriate procedure to change your firmware.

When you select *Upgrade* (or *Downgrade*, if downgrading the firmware), you are automatically redirected to the Firmware Upgrade/Downgrade page.

**Firmware Upgrade/Downgrade page**
Provides settings for upgrading or downgrading the current firmware image on your unit.

- **Upgrade From**
  Select the firmware source from the drop down list of available sources. Possible sources include *Local Hard Disk*, *USB*, and *FortiGuard Network*. This field does not appear on all models.

- **Upgrade File**
  Browse to the location of the firmware image on your local hard disk. This field is available for local hard disk and USB only.

- **Allow Firmware Downgrade**
  Select to confirm the installation of an older firmware image (downgrade). This field only displayed when attempting to downgrade firmware.

- **Upgrade Partition**
  The number of the partition being updated. This field is available only if your unit has more than one firmware partition.

- **More Info**
  Go to the FortiGuard Center to learn more about firmware updates through the FortiGuard network.

**Note:** You need to register your unit with Customer Support to access firmware updates for your model. For more information, go to [http://support.fortinet.com](http://support.fortinet.com) or contact Customer Support.

Monitoring administrators

You can view detailed information about each administrator that is logged into the unit from the System Information widget.

To view logged in administrators, in the System Information widget, select *Details*. When you select *Details*, the Administrators logged in window appears, and details about each administrator are shown. You can also disconnect an administrator or refresh the list from this window.

**Current Administrators information page (System Information widget)**
Lists the administrators that are currently logged into the web-based manager and CLI. You can disconnect administrators from this page as well as refresh the information on the page.

- **Disconnect**
  Select to disconnect the selected administrators. This is available only if your admin profile gives you system configuration read and write permission.

- **Refresh**
  Select to update the list.

- **Close**
  Select to close the window.

- **User Name**
  The administrator account name.
License Information widget

License Information displays the status of your technical support contract and FortiGuard subscriptions. The unit updates the license information status indicators automatically when attempting to connect to the FortiGuard Distribution Network (FDN). FortiGuard Subscriptions status indicators are green if the FDN was reachable and the license was valid during the last connection attempt, grey if the FortiGate unit cannot connect to the FDN, and orange if the FDN is reachable but the license has expired.

When a new unit is powered on, it automatically searches for FortiGuard services. If the unit is configured for central management, it will look for FortiGuard services on the configured FortiManager system. The unit sends its serial number to the FortiGuard service provider, which then determines whether the unit is registered and has valid contracts for FortiGuard subscriptions and FortiCare support services. If the unit is registered and has a valid contract, the License Information is updated.

If the unit is not registered, any administrator with the super_admin profile sees a reminder message that provides access to a registration form.

When a contract is due to expire within 30 days, any administrator with the super_admin profile sees a notification message that provides access to an Add Contract form. Simply enter the new contract number and select Add. Fortinet Support also sends contract expiry reminders.

You can optionally disable notification for registration or contract inquiry using the config system global command in the CLI. Selecting any of the Configure options will take you to the Maintenance page. For more information, see “Maintenance” on page 136.

**License Information widget**

**Support Contract**

Displays details about your current Fortinet Support contract including expiry dates and registration status.

- If Not Registered appears, select Register to register the unit.
- If Expired appears, select Renew for information on renewing your technical support contract. Contact your local reseller.
- If Registered appears the name of the support that registered this unit is also displayed.
- You can select Login Now to log into the Fortinet Support account that registered this unit.

**FortiGuard Services**

**AntiVirus**

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

**AV Definitions**

The currently installed version of the FortiGuard Antivirus definitions. To update the definitions manually, select Update.

**Extended set**

The currently installed version of the extended FortiGuard Antivirus definitions. The extended antivirus database is available only on certain models.

To update the definitions manually, select Update.

**Intrusion Protection**

The FortiGuard Intrusion Prevention System (IPS) license version, license issue date and service status. If your license has expired, you can select Renew to renew the license.

**IPS Definitions**

The currently installed version of the IPS attack definitions. To update the definitions manually, select Update.
**Manual updating FortiGuard definitions**

You can manually update several FortiGuard services from the License Information widget. The services that you can manually update are antivirus definitions, intrusion protection definitions, as well as VCM plugin.

For information about configuring automatic FortiGuard updates, see "Configuring the FortiGate unit for FDN and FortiGuard subscription services" on page 141.

**To update FortiGuard definitions manually**

1. Download the latest update files from Fortinet support site and copy it to the computer that you use to connect to the web-based manager.

2. Log in to the web-based manager and locate the License Information widget.

---

| **Vulnerability Compliance and Management** | The currently installed version of the vulnerability compliance and management services. |
| **VCM Plugin** | The currently installed vulnerability compliance and management plugin. To update the plugin, select *Update*. |
| **Web Filtering** | The FortiGuard Web Filtering license status, expiry date and service status. If your license has expired, you can select *Renew* to renew the license. |
| **Email Filtering** | The FortiGuard Email Filtering or Antispam license status, license expiry date and service status. If your license has expired, you can select *Renew* to renew the license. |
| **Email Filtering Rule Set** | The currently installed version of the FortiGuard Email Filtering rule set. To update the rule set manually, select *Update*. |
| **Analysis & Management Service** | The FortiGuard Analysis Service and Management Service license, license expiry date, and leachability status. |
| **Services Account ID** | Displays the FortiGuard Analysis and Management Services account ID. This ID is used to validate your license for this particular FortiGuard subscription service. |
| **Virtual Domain** | The maximum number of virtual domains the unit supports with the current license. For high-end models, you can select the *Purchase More* link to purchase a license key through Fortinet technical support to increase the maximum number of VDOMs. For more information, see "Adding VDOM Licenses" on page 152. |
| **Endpoint Security** | View information about the latest version of the FortiClient application available from FortiGuard for EndPoint NAC. For more information, see "Configuring FortiClient installer download and version enforcement" on page 349. |
| **FortiClient Software** | To download the installer on a PC, select *Download* in the *Windows Installer* row. To download the installer on a MAC, select *Download* in the *Mac Installer* row. |
| **Application Signature package** | The version number of the current endpoint NAC application detection predefined signature package. |
3 In the License Information widget, in the AV Definitions row, select Update.
   You are automatically redirected to the Anti-Virus Definitions Update page. A similar
   page opens for each of the services. For example, selecting Update in the IPS
   Definitions row automatically redirects you to the Intrusion Prevention System
   Definitions Update page.

4 Select Browse and locate the update file, or type the path and filename.

5 Select OK to copy the update file to the unit.
   The unit updates the AV definitions. This takes about one minute.

6 Verify the update was successful by locating the License Information widget and
   viewing the date given in the row.

7 Repeat steps 3 to 6 for IPS definitions and VCM Plugin.

8 Go to System > Dashboard > Status to confirm that the version information for the
   selected definition or rule set has updated.
   Date When the MM4 message was sent or received.
   From The IP address the MM4 message was from.
   To The IP address where the MM4 message was going.
   Subject The subject of the MM4 message.

**Unit Operation widget**

![Caution: Abruptly powering off the unit may corrupt its configuration. Using the reboot and
shutdown options here or in the CLI ensures proper shutdown procedures are followed to
prevent any loss of configuration.]

In the Unit Operation widget, an illustration of the unit’s front panel shows the status of the
unit’s Ethernet network interfaces. If a network interface is 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 pop-up window opens allowing you to enter the
reason for the system event. Your reason will be added to the Disk Event Log if disk
logging, event logging, and admin events are enabled.

You can only have one management and one logging/analyzing method displayed for your
unit. The graphic for each will change based on which method you choose. If none are
selected, no graphic is shown.

**Unit Operation widget**

<table>
<thead>
<tr>
<th>INT / EXT / DMZ / HA / WAN1 / WAN2 / 1 / 2 / 3 / 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>The network interfaces on the unit. The names and number of these interfaces vary by model.</td>
</tr>
<tr>
<td>The icon below the interface name indicates its up/down status by 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. A tooltip displays the full name of the interface, its 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.</td>
</tr>
</tbody>
</table>
The System Resources widget displays basic unit resource usage, such as CPU and memory (RAM) usage. Any System Resources that are not displayed on the status page can be viewed as a graph by selecting the History icon.

To see the most recent CPU and memory usage, select the Refresh icon.

**System Resources widget**

**History**

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. See “Viewing operational history” on page 45.

**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.

The displayed CPU usage is equivalent to using the CLI command `get system performance status and adding user, system, and nice percentages. Both the web-based CPU Usage and the CLI command access the same CPU information.`
Memory Usage

The current memory (RAM) 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 Usage

The current status of the FortiAnalyzer disk space used by this unit’s quota, displayed as a pie chart and a percentage.
You can use the System Resources edit menu to select not to display this information.
This is available only if you have configured logging to a FortiAnalyzer unit.

Viewing operational history

The System Resource History page displays six line graphs representing different system resources and protection activity over time.

By default, the refresh rate is every 30 seconds and the time interval is every 10 minutes.
When you change the time interval, you The refresh rate is every 30 seconds for the graphs.
To view the operational history, on the System Resources widget, select History in the title bar area.

Operational History window

This window allows you to see the detailed information about the operational history of your unit.

Time Interval
Select the time interval to display along the bottom axis of the graphs.

CPU Usage History
Percentage CPU usage for the preceding interval.

Memory Usage History
Percentage memory usage for the preceding interval.

Session History
Number of sessions over the preceding interval.

Network Utilization History
Network utilization for the preceding interval.

Virus History
Number of Viruses detected over the preceding interval.

Intrusion History
Number of intrusion attempts detected over the preceding interval.

Alert Message Console widget

Alert messages help you track system events on your unit such as firmware changes, network security events, or virus detection events.
Each message shows the date and time that the event occurred.
The following types of messages can appear in the Alert Message Console:

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

System shutdown
An administrator shut down the unit from the web-based manager or CLI.

Firmware upgraded by <admin_name>
The named administrator upgraded the firmware to a more recent version on either the active or non-active partition.

Firmware downgraded by <admin_name>
The named administrator downgraded the firmware to an older version on either the active or non-active partition.

FortiGate has reached connection limit for <n> seconds
The antivirus engine was low on memory for the duration of time shown and entered conserve mode. Depending on model and configuration, content can be blocked or can pass unscanned under these conditions.
You can configure the alert message console settings to control what types of messages are displayed on the console.

To configure the Alert Message Console

1. Go to System > Dashboard > Status.
2. Select the Edit icon in the Alert Message Console title bar.
3. Select the types of alerts that the Alert Message Console should display.
4. By default, all alert types are enabled. Select OK.

Log and Archive Statistics widget

The Log and Archive Statistics widget allows you to see at a glance the activity of what is DLP archiving, network traffic, and security problems including attack attempts, viruses caught, and spam emails caught.

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

The information displayed in the Log and Archive Statistics widget is derived from log messages. You can use the information gathered by log messages to see trends in network activity or attacks over time. Various configuration settings are required to actually collect data for the Log and Archive Statistics widget as described below.

**Log and Archive Statistics widget**

<table>
<thead>
<tr>
<th>Since</th>
<th>The date and time when the counts were last reset. Counts are reset when the unit reboots, or when you select Reset in the title bar area.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Archive</td>
<td>A summary of the HTTP, HTTPS, email, FTP IM, and VoIP (also called session control) traffic that has passed through the unit, and has been archived by DLP. This widget also Indicating the average DLP archive bytes per day since the last time it was reset. The Details pages list the last items of the selected type—up to 64 items—and provides 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 Log &amp; Report &gt; Log Config &gt; Log Settings. You configure the unit to collect DLP archive data for the widget by configuring a DLP sensor to archive its log data. For more information, see &quot;DLP archiving&quot; on page 291. You must also add the profile to a firewall policy. When the firewall policy receives sessions for the selected protocols, meta-data is added to the statistics widget. The Email statistics are based on email protocols. POP3 and IMAP traffic is registered as email received, and SMTP is email sent. If your unit supports SSL content scanning and inspection, incoming email also includes POP3S and IMAPS and outgoing email also includes SMTPS. If incoming or outgoing email does not use these protocols, these statistics will not be accurate. The IM statistics are based on the AIM, ICQ, MSN, and Yahoo! protocols and configured by selecting Archive in DLP Sensors for IM DLP rules.</td>
</tr>
</tbody>
</table>

You must also add the profile to a firewall policy. When the firewall policy receives sessions for the selected protocols, meta-data is added to the statistics widget.

The Email statistics are based on email protocols. POP3 and IMAP traffic is registered as email received, and SMTP is email sent. If your unit supports SSL content scanning and inspection, incoming email also includes POP3S and IMAPS and outgoing email also includes SMTPS. If incoming or outgoing email does not use these protocols, these statistics will not be accurate.

The IM statistics are based on the AIM, ICQ, MSN, and Yahoo! protocols and configured by selecting Archive in DLP Sensors for IM DLP rules.
The VoIP statistics are based on the SIP, SIMPLE and SCCP session control protocols and configured by selecting Archive in DLP Sensors for Session Control DLP rules.

Log

A summary of traffic, viruses, attacks, spam email messages, and blocked URLs that the unit has logged. Also displays the number of sessions matched by DLP and event log messages. The Details pages list the 20 most recent items, providing the time, source, destination and other information.

DLP data loss detected actually displays the number of sessions that have matched DLP sensor profiles. DLP collects meta-data about all sessions matched by DLP sensors and records this meta-data in the DLP log. Every time a DLP log message is recorded, the DLP data loss detected number increases. If you are using DLP for summary or full archiving the DLP data loss detected number can get very large. This number may not indicate that data has been lost or leaked.

Viewing DLP archive section of the Log and Archive Statistics widget

From the Log and Archive Statistics widget, you can view statistics about HTTP, HTTPS, FTP and IM traffic coming through the 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 DLP archive and attack log information, and reset the counts to zero.

DLP archive information is viewed from the DLP Archive section of the Log and Archive Statistics widget. You must select Details to view the available archive information.

Table 4: Viewing DLP archive information

<table>
<thead>
<tr>
<th>HTTP</th>
<th>Date and Time – The time when the URL was accessed. From – The IP address from which the URL was accessed. URL – The URL that was accessed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Date and Time – The time that the email passed through the FortiGate unit. From – The sender’s email address. To – The recipient’s email address. Subject – The subject line of the email.</td>
</tr>
<tr>
<td>FTP</td>
<td>Date and Time – The time of access. Destination – The IP address of the FTP server that was accessed. User – The User ID that logged into the FTP server. Downloads – The names of files that were downloaded. Uploads – The names of files that were uploaded.</td>
</tr>
<tr>
<td>IM</td>
<td>Date / Time – The time of access. Protocol – The protocol used in this IM session. Kind – The kind of IM traffic this transaction is. Local – The local address for this transaction. Remote – The remote address for this transaction Direction – If the file was sent or received.</td>
</tr>
</tbody>
</table>

Viewing the Log section of the Log and Archive Statistics widget

From the Log and Archive Statistics widget, you can view statistics about the network attacks that the FortiGate unit has stopped. You can view statistics about viruses caught, attacks detected, spam email detected, and URLs blocked. You can also view information about sessions matched by DLP rules. 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 DLP archive and attack log information and reset the counts to zero.

Log information about network traffic, attacks, as well as other valuable is viewed from the Log section of the Log and Archive Statistics widget. You must select Details to view the available attack information.
Table 5: Viewing Attack Log information

<table>
<thead>
<tr>
<th>AV</th>
<th>Date and Time – The time when the virus was detected.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From – The sender’s email address or IP address.</td>
</tr>
<tr>
<td></td>
<td>To – The intended recipient’s email address or IP address.</td>
</tr>
<tr>
<td></td>
<td>Service – The service type, such as POP or HTTP.</td>
</tr>
<tr>
<td></td>
<td>Virus – The name of the virus that was detected.</td>
</tr>
<tr>
<td>IPS</td>
<td>Date and Time – The time that the attack was detected.</td>
</tr>
<tr>
<td></td>
<td>From – The source of the attack.</td>
</tr>
<tr>
<td></td>
<td>To – The target host of the attack.</td>
</tr>
<tr>
<td></td>
<td>Service – The service type.</td>
</tr>
<tr>
<td></td>
<td>Attack – The type of attack that was detected and prevented.</td>
</tr>
<tr>
<td>Email</td>
<td>Date and Time – The time that the spam was detected.</td>
</tr>
<tr>
<td></td>
<td>From -&gt; To IP – The sender and intended recipient IP addresses.</td>
</tr>
<tr>
<td></td>
<td>From -&gt; To Email Accounts – The sender and intended recipient email addresses.</td>
</tr>
<tr>
<td></td>
<td>Service – The service type, such as SMTP, POP or IMAP.</td>
</tr>
<tr>
<td></td>
<td>SPAM Type – The type of spam that was detected.</td>
</tr>
<tr>
<td>URLs</td>
<td>Date and Time – The time that the attempt to access the URL was detected.</td>
</tr>
<tr>
<td></td>
<td>From – The host that attempted to view the URL.</td>
</tr>
<tr>
<td></td>
<td>URL Blocked – The URL that was blocked.</td>
</tr>
<tr>
<td>DLP</td>
<td>Date and Time – The time that the attempt to access the URL was detected.</td>
</tr>
<tr>
<td></td>
<td>Service – The service type, such as HTTP, SMTP, POP or IMAP.</td>
</tr>
<tr>
<td></td>
<td>Source – The source address of the session.</td>
</tr>
<tr>
<td></td>
<td>From – The host that attempted to view the URL.</td>
</tr>
<tr>
<td></td>
<td>URL Blocked – The URL that was blocked.</td>
</tr>
<tr>
<td></td>
<td>From – The sender’s email address or IP address.</td>
</tr>
<tr>
<td></td>
<td>To – The intended recipient’s email address or IP address.</td>
</tr>
</tbody>
</table>

**CLI Console widget**

The CLI Console widget allows you to access the CLI without exiting from the web-based manager. This widget can also be customized, providing greater flexibility about how the CLI Console appears to administrators.

The two controls located on the CLI Console widget title bar are Customize, and Detach.

- **Detach** moves the CLI Console widget into a pop-up window that you can resize and reposition. The two controls on the detached CLI Console are Customize and Attach. Attach moves the CLI console widget back to the dashboard’s page.

- **Customize** allows you to change the appearance of the console by defining fonts and colors for the text and background.

Use the following table to customize the CLI Console widget.

**Console Preferences window**

This window provides settings for modifying the CLI console widget’s appearance, font, and to include an external command box.

- **Preview**
  A preview of your changes to the CLI Console’s appearance.

- **Text**
  Select the current color swatch next to this label, then select a color from the color palette to the right to change the color of the text in the CLI Console.

- **Background**
  Select the current color swatch next to this label, then select a color from the color palette to the right to change the color of the background in the CLI Console.
Top Sessions widget

Top Sessions displays either a bar graph or a table showing the IP addresses that have the most sessions currently open on the unit. The sessions are sorted by their source or destination IP address, or the port address. The sort criteria being used is displayed in the top right corner.

The Top Sessions widget polls the unit for session information.

Note: Rebooting the unit will reset the Top Session statistics to zero.

When you select Details to view the current sessions list, a list of all sessions currently processed by the unit. For more information, see “Viewing the current sessions list” on page 50.

Detailed information is available when you select the bar within the widget. Use the following table to modify the default settings of the Top Sessions widget.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use external command input box</td>
<td>Select to display a command input field below the normal console emulation area. When this option is enabled, you can enter commands by typing them into either the console emulation area or the external command input field.</td>
</tr>
<tr>
<td>Console buffer length</td>
<td>Enter the number of lines the console buffer keeps in memory. Valid numbers range from 20 to 9999.</td>
</tr>
<tr>
<td>Font</td>
<td>Select a font from the list to change the display font of the CLI Console. Select the size of the font. The default size is 10 points.</td>
</tr>
<tr>
<td>Size</td>
<td></td>
</tr>
</tbody>
</table>

Custom Top Sessions Display

Provides settings for modifying the default settings of the Top Sessions widget.

Report By

Select the method used to sort the Top Sessions on the System Status display. Choose one of:

- Source Address
- Destination Address
- Port Address

Display User Name

Select to include the username associated with this source IP address, if available. In the table display format this will be a separate column. Display UserName is available only when the sort criteria is Source Address.

Resolve Host Name

Select to resolve the IP address to the host name. Resolve Host Name is not available when the sort criteria is Destination Port.

Resolve Service

Select to resolve a port addresses into their commonly associated service names. Any port address without a service, will continue to be displayed as the port address. For example, port 443 would resolve to HTTPS. Resolve Service is only available when the sort criteria is Destination Port.

Display Format

Select how the Top Session information is displayed. Choose one of:

- Chart
- Table
Viewing the current sessions list

The current sessions list displays all sessions currently processed by the unit. For each session the current session list displays:

- the session protocol such as tcp or udp
- source address and port
- destination address and port
- the ID of the policy, if any, that applies to the session
- how long until the session expires
- which virtual domain the session belongs to

When you want to view the current session list, select **Detach** in the title bar area to properly view the entire list and to filter information. You can select **Return** to return you to the Top Sessions widget.

**Current session list**

The following appears when you select **Details** within the Top Sessions widget. You can detach this widget to expand and view the information better.

- **Refresh** Update the session list.
- **Page Controls** Enter the page number of the session to start the displayed session list. For example if there are five pages of sessions and you enter 3, page 3 of the sessions will be displayed.
  - The number following the '/' is the number of pages of sessions.
- **Total** The total number sessions.
- **Clear All Filters** Select to reset any display filters that may have been set.
- **Return** Return to the Top Sessions display.
- **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.
- **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.
- **Duration** The age of each session in seconds. The age is the amount of time the session has been active.
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 virtual domains are enabled.

Delete
Stop an active communication session. Your admin profile must include read and write access to system configuration.

Top Viruses widget
The Top Viruses widget displays a bar graph that represent the most frequent virus threats as detected by the unit.

If you select the History icon, located in the title bar area, a window opens that displays up to the 20 most recent viruses that have been detected with information including the virus name, when it was last detected, and how many times it was detected. The system stores up to 1024 entries, but only displays up to 20 in the web-based manager.

You can modify several settings for this widget when you select the Edit icon in this widget's title bar area. You must select OK to save the settings.

Use the following table to modify the default settings for the Top Viruses widget.

| Custom Top Viruses Display | Provides settings for modifying the default settings of the Top Viruses widget. |
| Custom Widget Name | Enter a new name for the widget. This is optional. |
| Refresh Interval | Select display update interval in seconds. Range 10 to 240 seconds. Select 0 to disable updating. You can also update using the Refresh icon in the module header. |
| Top Viruses To Show | Select whether to display top 5, 10, 15, or 20 viruses. |

Top Attacks widget
Top Attacks displays a bar graph representing the most numerous attacks detected by the unit.

If you select the History icon, opens a window that displays up to the 20 most recent attacks that have been detected with information including the attack name, when it was last detected, and how many times it was detected. The unit stores up to 1024 entries, but only displays up to 20 in the web-based manager.

You can configure several settings for this widget when you select the Edit icon in this widget's title bar area. You must select OK to save the settings.

Use the following table to modify the default settings of the Top Attacks widget.

| Custom Top Attacks Display | Provides settings for modifying the default settings of the Top Attacks widget. |
| Custom Widget Name | Enter a new name for the widget. This is optional. |
| Refresh Interval | Select display update interval in seconds. Range 10 to 240 seconds. Select 0 to disable updating. You can also update using the Refresh icon in the module header. |
| Top Attacks To Show | Select whether to display top 5, 10, 15, or 20 attacks. |

Traffic History widget
The Traffic History widget shows the traffic on one selected interface over the last hour, day, and month. This feature can help you locate peaks in traffic that you need to address as well as their frequency, duration, and other information.
Only one interface at a time can be monitored. By default, no interface is monitored. You can change the interface being monitored by selecting Edit, choosing the interface from the drop down menu, and selecting Apply. All traffic history data is cleared when you select Apply.

If you want to expand your view of the information within the widget, selectEnlarge in the title bar area.

**Traffic History widget**

<table>
<thead>
<tr>
<th>Interface: &lt;interface_name&gt;</th>
<th>The interface that is being monitored.</th>
</tr>
</thead>
<tbody>
<tr>
<td>bit/s</td>
<td>The units of the traffic graph. The scale varies based on traffic levels to allow it to show traffic levels no matter how little or how much traffic there is.</td>
</tr>
<tr>
<td>Last 60 Minutes</td>
<td>Three graphs showing the traffic monitored on this interface of the unit over different periods of time.</td>
</tr>
<tr>
<td>Last 24 Hours</td>
<td>Certain trends may be easier to spot in one graph over the others.</td>
</tr>
<tr>
<td>Last 30 Days</td>
<td></td>
</tr>
<tr>
<td>Traffic In</td>
<td>The traffic entering the unit on this interface is indicated with a thin red line.</td>
</tr>
<tr>
<td>Traffic Out</td>
<td>The traffic leaving the unit on this interface is indicated with a dark green line, filled in with light green.</td>
</tr>
</tbody>
</table>

You can modify several default settings for this widget when you select the Edit icon in this widget’s title bar area. You must select OK to save the settings. Use the following table for modifying the default settings for the Traffic History widget.

**Custom Traffic History Display**

Provides settings for modifying the default settings of the Traffic History widget.

<table>
<thead>
<tr>
<th>Custom Widget Name</th>
<th>Enter a new name for the widget. This is optional.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Network Interface</td>
<td>Select an interface (FortiGate unit's interfaces) from the drop-down list. The interface you choose displays the traffic occurring on it.</td>
</tr>
<tr>
<td>Enable Refresh</td>
<td>Select to enable the information to refresh.</td>
</tr>
</tbody>
</table>

**Top Policy Usage widget**

The Top Policy Usage widget shows the volume of traffic passing through the unit classified by firewall policy as either a chart or a table.

From the chart or table display you can:

- View details about firewall policies by pausing the mouse pointer over each bar in the chart.
- Select a firewall policy on the graph to view and optionally change the firewall policy.

Top Policy Usage data is collected by all firewall policies. You can configure Top Policy Usage to show data for up to 20 firewall policies. Only firewall policies that have accepted sessions appear on the chart or table.

Use the following table to modify the default settings of the Top Policy Usage widget.

**Dashboard - Custom Top Policy Usage Display**

Provides settings for modifying the default settings of the Top Policy Usage widget.

<table>
<thead>
<tr>
<th>Custom Widget Name</th>
<th>Enter a new name for the widget. This is optional.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort Criteria</td>
<td>Select whether to sort the policies by number of Bytes or number of Packets.</td>
</tr>
<tr>
<td>VDOM</td>
<td>Select the VDOM to monitor or select Global. This is available for global administrators only. VDOM administrators see only their only VDOM.</td>
</tr>
</tbody>
</table>
DLP Archive Usage widget

The DLP Archive Usage widget shows the volume of log data that the unit has sent for archival storage (DLP Archive). You can categorize the information by DLP Rule, firewall policy, DLP sensor applied to a firewall policy, or protocol.

From the table display you can:

- View details about the data by pausing the mouse pointer over each bar in the chart.
- Select a bar on the graph to view more information about the data.

The data for this widget is collected by adding a DLP sensor profile to a firewall policy. Only information about sessions matched by DLP sensors is added to the chart or table. Sessions accepted by firewall policies (with no DLP sensor applied to that firewall policy) do not contribute to the data displayed.

You can modify several settings within this widget. You must select OK to save the settings.

Use the following table to modify the default settings of the DLP Archive Usage widget.

<table>
<thead>
<tr>
<th>Custom DLP Archive Display</th>
<th>Provides settings for modifying the default settings of the DLP Archive Usage widget.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Widget Name</td>
<td>Enter a new name for the widget. This is optional.</td>
</tr>
<tr>
<td>Report By</td>
<td>Select one of: DLP Rule, Profile, Policy, or Protocol.</td>
</tr>
<tr>
<td>Sort Criteria</td>
<td>Select whether to sort the results by number of Bytes or number of Messages.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocols to include.</td>
</tr>
<tr>
<td>VDOM</td>
<td>Select the VDOM to monitor or select Global. This is available for global</td>
</tr>
<tr>
<td></td>
<td>administrators only. VDOM administrators see only their only VDOM. This field is</td>
</tr>
<tr>
<td></td>
<td>not available if Report By is Protocol.</td>
</tr>
<tr>
<td>Top Entries To Show</td>
<td>Select whether to display top 5, 10, 15, or 20 items.</td>
</tr>
<tr>
<td>Refresh Interval</td>
<td>Select display update interval in seconds. Range 10 to 240 seconds. Select 0 to</td>
</tr>
<tr>
<td></td>
<td>disable updating. You can also update using the Refresh icon in the module header.</td>
</tr>
</tbody>
</table>

RAID monitor

The RAID monitor widget shows the current state of the RAID array and each RAID disk. For information on configuring the RAID array, see “Configuring the RAID array” on page 177.

The RAID monitor widget does not display unless the unit has more than one disk installed.

<table>
<thead>
<tr>
<th>RAID monitor widget</th>
<th>Select to configure the RAID array, or rebuild a degraded array.</th>
</tr>
</thead>
</table>
The RAID disk is configured from the Disk Configuration page. When you select Configure on the RAID Monitor widget, you are automatically redirected to the Disk Configuration page where you can configure the settings of the current RAID array.

For information on configuring the RAID array, see “Configuring the RAID array” on page 177.

Use the following table to configure the RAID disk.
Disk Configuration page
Provides settings for configuring the RAID array. When you select [Configure] in the title bar area, you are automatically redirected to the Disk Configuration page.

RAID level
Select the level of RAID. Options include:
- **RAID-0** — (striping) better performance, no redundancy
- **RAID-1** — (mirroring) half the storage capacity, but totally redundant
- **RAID-5** — striping with parity checking, and redundancy

Available RAID level options depend on the available number of hard disks. Two or more disks are required for RAID 0 or RAID 1. Three or more disks are required for RAID 5.

Changing the RAID level will take effect when Apply is selected.
Changing the RAID level will erase any stored log information on the array, and reboot the unit. The unit will remain offline while it reconfigures the RAID array. When it reboots, the array will need to synchronize before being fully operational.

Status
The status, or health, of RAID array. This status can be one of:
- **OK** — standard status, everything is normal
- **OK (Background-Synchronizing) (%)** — synchronizing the disks after changing RAID level. Synchronizing progress bar shows percent complete
- **Degraded** — One or more of the disks in the array has failed, been removed, or is not working properly. A warning is displayed about the lack of redundancy in this state. Also, a degraded array is slower than a healthy array. Select **Rebuild RAID** to fix the array.
- **Degraded (Background-Rebuilding) (%)** — The same as degraded, but the RAID array is being rebuilt in the background. The array continues to be in a fragile state until the rebuilding is completed.

Size
The size of the RAID array in gigabytes (GB). The size of the array depends on the RAID level selected, and the number of disks in the array.

Rebuild RAID
Select to rebuild the array after a new disk has been added to the array, or after a disk has been swapped in for a failed disk.
If you try to rebuild a RAID array with too few disks you will get a rebuild error. After inserting a functioning disk, the rebuild will start.
This button is only available when the RAID array is in a degraded state and has enough disks to be rebuilt.
You cannot restart a rebuild once a rebuild is already in progress.

**Note:** If a disk has failed, the number of working disks may not be enough for the RAID level to function. In this case, replace the failed disk with a working disk to rebuild the RAID array.

Disk#
The disk’s position in the array. This corresponds to the physical slot of the disk.
If a disk is removed from the unit, the disk is marked as not a member of the array and its position is retained until a new disk is inserted in that drive bay.

Status
The status of this disk. Options include OK, and unavailable.
A disk is unavailable if it is removed or has failed.

Member
Display if the selected disk is part of the RAID array.
A green icon with a check mark indicates the disk is part of the array.
A grey icon with an X indicates the disk is not part of the RAID array.
A disk may be displayed as healthy on the dashboard display even when it is not a member in the RAID array.
A disk may be available but not used in the RAID array. For example three disks in a RAID 1 array, only two are used.

Capacity
The storage capacity that this drive contributes to the RAID array.
The full storage capacity of the disk is used for the RAID array automatically.
The total storage capacity of the RAID array depends on the capacity and numbers of the disks, and the RAID level of the array.
**Top Application Usage widget**

The Top Application Usage widget shows the volume of traffic passing through the unit classified by application type as either a chart or a table. The chart displays applications in order of use.

From the chart or table display you can:

- View traffic volumes by pausing the mouse pointer over each bar.
- Select an application type on the graph to view information about the source addresses that used the application and the amount of data transferred by sessions from each source address.

Top Application Usage data collection is started by adding application control lists to firewall policies. Only information about applications matched by application control is added to the chart or table. Sessions accepted by firewall policies (with no application control list applied to that firewall policy) do not contribute to the data displayed.

Use the following table to modify the default settings for the Top Application Usage widget.

<table>
<thead>
<tr>
<th>Custom Top Application Usage Display</th>
<th>Provides settings for modifying the default settings of the Top Applications Usage widget.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Custom Widget Name</strong></td>
<td>Enter a new name for the widget. This is optional.</td>
</tr>
<tr>
<td><strong>Sort Criteria</strong></td>
<td>Select whether to sort the applications by number of Bytes or number of Messages.</td>
</tr>
<tr>
<td><strong>Application Details</strong></td>
<td>The detail information about the application information that will be displayed in the widget.</td>
</tr>
<tr>
<td><strong>Report By</strong></td>
<td>Select Source Address or Destination Address.</td>
</tr>
<tr>
<td><strong>Display User Name</strong></td>
<td>Select the check box to show the user name (when known) instead of the IP address.</td>
</tr>
<tr>
<td><strong>Resolve Host Name</strong></td>
<td>Select to use reverse-DNS lookup to determine the host name instead of displaying the IP address.</td>
</tr>
<tr>
<td><strong>VDOM</strong></td>
<td>Select the VDOM to monitor or select Global. This is available for global administrators only. VDOM administrators see only their only VDOM.</td>
</tr>
<tr>
<td><strong>Display Format</strong></td>
<td>Select Chart or Table display.</td>
</tr>
<tr>
<td><strong>Top Entries To Show</strong></td>
<td>Select whether to display top 5, 10, 15, or 20 applications.</td>
</tr>
<tr>
<td><strong>Refresh Interval</strong></td>
<td>Select display update interval in seconds. Range 10 to 240 seconds. Select 0 to disable updating. You can also update using the Refresh icon in the module header.</td>
</tr>
</tbody>
</table>

**Storage widget**

The Storage widget allows you to view the status of each disk currently installed on your unit. The status includes how much space is used and how much free space is available. You can find out more detailed information about a disk’s status by going to System > Maintenance > Disk. The Storage page displays information regarding the disk’s health, RAID events, visual representation of the disk, and configuration of the management of the disk. The management configuration could be that three partitions have been configured, with one for firmware, another for logs, and the last for WAN Opt storage. For more information about disk management, see “Disk” on page 152.

**P2P Usage widget**

The P2P Usage widget displays the total bytes and total bandwidth for each supported instant messaging client. These clients are WinNY, BitTorrent, eDonkey, Guntella, and KaZaa. With P2P Usage, you can only modify the default name of the widget.
You can only change the name of the P2P Usage widget. To change the name, select the Edit icon in the title bar and then enter a name in the Custom Widget Name field. Select OK to save the change.

**Per-IP Bandwidth Usage widget**

The Per-IP Bandwidth Usage widget allows you to view per-IP address session data. The data, which displays each IP address that initiated the traffic (and its current bandwidth consumption), is similar to the top session widget. Instead of viewing the IP address of the person who initiated the traffic, you can choose to view their name by selecting Resolve Host Name in the editing window.

You can configure several settings for this widget when you select the Edit icon in this widget's title bar area. You must select OK to save the settings.

Use the following table to modify the settings for the Per-IP Bandwidth Usage widget.

<table>
<thead>
<tr>
<th>Custom Per-IP Bandwidth Usage Display</th>
<th>Provides settings for modifying the default settings of the Per-IP Bandwidth Usage widget.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Widget Name</td>
<td>Enter a new name for the widget. This is optional.</td>
</tr>
<tr>
<td>Resolve Host Name</td>
<td>Select to display a name instead of the IP address.</td>
</tr>
<tr>
<td>Display Format</td>
<td>Select either Chart or Table. If you select Chart, the information displays as a bar chart. If you select Table, the information displays within a table.</td>
</tr>
<tr>
<td>Top Entries to Show</td>
<td>Select the top entries that will appear within the table or chart.</td>
</tr>
<tr>
<td>Refresh Interval</td>
<td>Select display update interval in seconds. Range 10 to 240 seconds. Select 0 to disable updating. You can also update using the Refresh icon in the module header.</td>
</tr>
</tbody>
</table>

**VoIP Usage widget**

In the VoIP Usage widget, you can view current active VoIP calls (using over SIP and SCCP protocols), as well as calls that have been dropped, failed or went unanswered. You can easily see how many calls actual succeeded, and how many calls there were in total from when you last cleared the information in the widget.

You can only change the name of the VoIP Usage widget. To change the name, select the Edit icon in the title bar and then enter a name in the Custom Widget Name field. Select OK to save the change.

**IM Usage widget**

The IM Usage widget provides details about instant messaging clients and their activity that is occurring on your network. From within this widget, you can view information regarding users, chats, messages, file transfer between clients, and any voice chats that occurred as well. IM Usage provides this information for IM, Yahoo!, AIM, and ICQ.

You can only change the name of the IM Usage widget. To change the name, select the Edit icon in the title bar and then enter a name in the Custom Widget Name field. Select OK to save the change.

**FortiGuard widget**

You can configure a separate Alert Message Console widget that displays only FortiGuard alert information that is received from the FortiGuard Center. You can rename the newly created Alert Message Console widget and select the option FortiGuard security alerts to enable alerts are received and display on the widget.
FortiGuard provides you with information regarding the FortiGuard Center’s current news and RSS feeds. This version of the Alert Message Console widget displays the RSS feeds from the FortiGuard Center, notifying FortiGuard subscribers about the latest news and threats.

To configure the FortiGuard widget
1. On the dashboard page, select Widget and add the Alert Message Console widget.
2. Select the Edit icon in the widget’s title bar area.
3. Enter FortiGuard in the Custom Widget Name field.
4. Select the check box beside each option except for the check box beside FortiGuard security alerts.
   By default, all of the options are enabled.
5. To change the number of alerts that display, select a number from the drop-down list beside Number of alerts to display on the dashboard.
6. Select OK.

Network

The Network menu allows you to configure the unit to operate on the network. This menu provides features for configuring and viewing basic network settings, such as FortiGate interfaces and DNS options. There are also advanced options that include adding zones and VLAN subinterfaces.

This topic contains the following:
- Interface configuration and settings
- Configuring zones
- Configuring the modem interface
- FortiGate DNS services
- Configuring the explicit web proxy
- Configuring WCCP
- Routing table (Transparent Mode)

Note: Unless stated otherwise, the term interface can refer to either a physical FortiGate interface or to a virtual FortiGate VLAN subinterface.

If 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 configuration and settings

In System > Network > Interface, you can configure the interfaces that handle incoming and outgoing traffic. For example, on internal, this interface handles traffic that is coming into the unit; wan1 interface handles traffic that is going outside of the internal network or Intranet of the organization.

There are different options for configuring interfaces when the unit is in NAT/Route mode or Transparent mode. Some of these options include adding VLAN subinterfaces, modifying the configuration of a physical interface, or adding VDOM links on units with multiple VDOMs enabled.
Interface page
Lists all the interfaces that are default and those that you have created. On this page you can view the status of each interface, create a new interface, edit an existing interface, or remove an interface.

Create New
Select Create New to add a new interface. When you select Create New, you are automatically redirected to the New Interface page. Depending on the model you can add a VLAN interface, a loopback interface, a IEEE 802.3ad aggregated interface, or a redundant interface.
- “Adding VLAN interfaces” on page 64
- “Adding loopback interfaces” on page 64
- “Adding 802.3ad aggregate interfaces” on page 64
- “Adding redundant interfaces” on page 65
When VDOMs are enabled, you can also select Create New to add Inter-VDOM links.

Switch Mode
On supported models, select Switch Mode to change between switch mode and interface mode. Switch mode combines some FortiGate interfaces into one switch with one IP address. Interface mode allows you to configure them as separate interfaces.

On some FortiGate models you can also select Hub Mode. Hub mode is similar to switch mode except that in hub mode the interfaces do not learn the MAC addresses of the devices on the network they are connected to and may also respond quicker to network changes. Normally, you would only select Hub Mode if you are having network performance issues when operating with switch mode. The configuration of the FortiGate unit is the same whether in switch mode or hub mode.

Before switching modes, all configuration settings for the interfaces affected by the change must be set to defaults. When you select Switch Mode the web-based manager displays the list of affected interfaces.

Show backplane interfaces
Select to make FortiGate-5000 series backplane interfaces visible. Once visible, these interfaces can be configured as regular physical interfaces.

Column Settings
Select to change the columns of information that are displayed on the interface list.

Description
Display a description for the interface is one has been added.

Name
The names of the physical interfaces on your FortiGate unit. This includes any alias names that have been configured.

The names of the physical interfaces depend on the model. Some names indicate the default function of the interface such as internal, external, wan1 (wide are network), wlan (wireless LAN) and dmz. Other names are more generic such as port1, port20, and so on. Some models also include a modem interface named modem.

When you combine several interfaces into an aggregate or redundant interface, only the aggregate or redundant interface is listed, not the component interfaces.

On FortiGate models that support switch mode, the individual interfaces in the switch are not displayed when in switch mode. For more information, see “Switch Mode” on page 63.

If you have added VLAN interfaces, they also appear in the name list, below the physical or aggregated interface to which they have been added.

If you have added loopback interfaces, they also appear in the interface list, below the physical interface to which they have been added. If you have software switch interfaces configured, you will be able to view them. For more information, see “Adding software switch interfaces” on page 72.

If you have interface mode enabled on a model with a switch interface, you will see multiple internal interfaces. If switch mode is enabled, there will only be one internal interface.
After going to System > Network > Interface and selecting Create New, the New Interface page appears and you can then configure the settings of an interface. You can also edit an interface to modify its settings.

Use the following table to configure interface settings for an interface.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/Netmask</td>
<td>The current IP address/netmask of the interface. In VDOM mode, when VDOMs are not all in NAT or Transparent mode some values may not be available for display and will be displayed as &quot;-&quot; instead. When IPv6 Support is enabled on the web-based manager, IPv6 addresses may be displayed in this column.</td>
</tr>
<tr>
<td>Access</td>
<td>The administrative access configuration for the interface.</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>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 of an interface, select the Edit icon to edit the interface and change the Administrative Status setting for the interface.</td>
</tr>
<tr>
<td>Link Status</td>
<td>The status of the interface physical connection. Link status can be either up or down. If link status is up there is an active physical connection between the physical interface and a network switch. If link status is down the interface is not connected to the network or there is a problem with the connection. You cannot change link status from the web-based manager. Link status is only displayed for physical interfaces.</td>
</tr>
<tr>
<td>MAC</td>
<td>The MAC address of the interface.</td>
</tr>
<tr>
<td>Mode</td>
<td>Shows the addressing mode of the interface. The addressing mode can be manual, DHCP, or PPPoE.</td>
</tr>
<tr>
<td>MTU</td>
<td>The maximum number of bytes per transmission unit (MTU) for the interface.</td>
</tr>
<tr>
<td>Secondary IP</td>
<td>Displays the secondary IP addresses added to the interface.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the interface. Valid types include:</td>
</tr>
<tr>
<td></td>
<td>• Physical - a physical network interface, including the modem interface</td>
</tr>
<tr>
<td></td>
<td>• VLAN - a VLAN interface</td>
</tr>
<tr>
<td></td>
<td>• Aggregate - a group of 802.3ad aggregated interfaces</td>
</tr>
<tr>
<td></td>
<td>• Redundant - a group of redundant interfaces</td>
</tr>
<tr>
<td></td>
<td>• VDOM Link - a pair of virtual interfaces that link two VDOMs</td>
</tr>
<tr>
<td></td>
<td>• Pair - one two interfaces that are joined together, such as 2 VDOM links</td>
</tr>
<tr>
<td></td>
<td>• Switch - two or more interfaces joined together to create a software switch interface</td>
</tr>
<tr>
<td></td>
<td>• Tunnel - a virtual IPSec VPN interface</td>
</tr>
<tr>
<td></td>
<td>• VAP - a wireless controller virtual access point (VAP or virtual AP)</td>
</tr>
<tr>
<td>Virtual Domain</td>
<td>The virtual domain to which the interface belongs. This column is visible when VDOM configuration is enabled.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The configured VLAN ID for VLAN subinterfaces.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes an interface from the list on the Interface page. Available for interfaces added by selecting Create New. For example, you can remove VLAN, loopback, aggregate, and redundant interfaces. You can only remove an interface if it is not used in another configuration.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies settings within the configuration of an interface.</td>
</tr>
<tr>
<td>View</td>
<td>View the interface’s configuration.</td>
</tr>
</tbody>
</table>
New Interface page

Provides settings for configuring a new interface. When you select Create New on the Interface page, you are automatically redirected to this page. If you are editing an existing interface, you are automatically redirected to the Edit Interface page.

Name

The name of the interface. You can specify and change the names of VLAN, loopback, IEEE 802.3ad aggregated, and redundant interfaces.

You cannot change the name of an existing interface.

The interface display also includes the MAC address of the physical interface.

Alias

Enter another name for the interface that will easily distinguish this interface from another. This is available only for physical interfaces where you cannot configure the name. The alias can be a maximum of 15 characters.

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.

Link Status

Indicates whether the interface is connected to a network (link status is Up) or not (link status is Down).

Type

When adding a new interface, set Type to the type of interface that you want to add:

- Set Type to VLAN to add a VLAN interface.
- Set Type to Loopback Interface to add a loopback interface.
- On some models you can set Type to 802.3ad Aggregate to add an aggregate interface.
- On some models you can set Type to Redundant Interface to add a redundant interface.

Other types include:

- Software Switch - a software switch interface.
- Tunnel - a virtual IPSec VPN interface.
- VAP Interface - a wireless controller virtual access point (VAP or virtual AP) interface.

You cannot change the Type except when adding a new interface.

Interface

Select the name of the physical interface to which to add a VLAN interface.

Once created, the VLAN interface is listed below its physical interface in the Interface list.

You cannot change the physical interface of a VLAN interface except when adding a new VLAN interface.

Displayed when Type is set to VLAN.

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 except when add a new VLAN interface.

The VLAN ID can be any number between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch connected to the VLAN subinterface. For more information, see “Adding VLAN interfaces” on page 64.

Displayed when Type is set to VLAN.

Virtual Domain

Select the virtual domain to add the interface to.

Admin accounts with super_admin profile can change the Virtual Domain.

Physical Interface Members

- Software switch interface - this section is a display-only field showing the interfaces that belong to the software switch virtual interface.
- 802.3ad aggregate or Redundant interface - this section includes available interface and selected interface lists to enable adding or removing interfaces from the interface. For more information, see “Adding 802.3ad aggregate interfaces” on page 64 and “Adding redundant interfaces” on page 65.

Available Interfaces

Select interfaces from this list to include in the grouped interface - either redundant or aggregate interface. Select the right arrow to add an interface to the grouped interface.
Selected interfaces
These interfaces are included in the aggregate or redundant interface. Select the left arrow to remove an interface from the grouped interface. For redundant interfaces, the interfaces will be activated during failover from the top of the list to the bottom.

Addressing mode
Select the addressing mode for the interface.
- Select Manual and add an IP/Netmask for the interface. If IPv6 configuration is enabled you can add both a IPv4 and an IPv6 IP address.
- Select DHCP to get the interface IP address and other network settings from a DHCP server. See “Configuring DHCP on an interface” on page 65
- Select PPPoE to get the interface IP address and other network settings from a PPPoE server. See “Configuring PPPoE on an interface” on page 66.

IP/Netmask
If Addressing Mode is set to Manual, enter an IPv4 address/subnet mask for the interface.
Two FortiGate interfaces cannot have IP addresses on the same subnet.

IPv6 Address
If Addressing Mode is set to Manual and IPv6 support is enabled on the web-based manager, enter an IPv6 address/subnet mask for the interface. A single interface can have both an IPv4 and IPv6 address or just one or the other.

Enable one-arm sniffer
Select to configure this interface to operate as a one-armed sniffer as part of configuring a unit to operate as an IDS appliance by sniffing packets for attacks without actually receiving and otherwise processing the packets. Once the interface is enabled for sniffing you cannot use the interface for other traffic. You must add sniffer policies for the interface to actually sniff packets.

Enable explicit Web Proxy
Select to enable explicit web proxying on this interface. When enabled, this interface will be displayed on System > Network > Web Proxy under Listen on Interfaces and web traffic on this interface will be proxied according to the Web Proxy settings.

Enable DDNS
Select Enable DDNS to configure a Dynamic DNS service for this interface. For more information, see “Configuring Dynamic DNS on an interface” on page 67.

Override Default MTU Value
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
- larger frame sizes if supported by the FortiGate model
Only available on physical interfaces. Virtual interfaces associated with a physical interface inherit the physical interface MTU size. 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.

Enable DNS Query
Select to configure the interface to accept DNS queries. Select recursive or non-recursive.
- recursive: Look up domain names in the FortiGate DNS database. If the entry is not found, relay the request to the DNS servers configured under System > Network > Options.
- non-recursive: Look up domain names in the FortiGateDNS database. Do not relay the request to the DNS servers configured under System > Network > Options.

Administrative Access
Select the types of administrative access permitted for IPv4 connections to this interface.

Ipv6 Administrative Access
Select the types of administrative access permitted for IPv6 connections to this interface.

HTTPS
Allow secure HTTPS connections to the web-based manager through this interface.
Switch mode allows you to switch a group of related FortiGate interfaces to operate as a multi-port switch with one IP address. Switch mode is available on models with switch hardware.

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

Before you are able to change between switch mode and interface mode, all configuration settings for the affected interfaces must be set to defaults. This includes firewall policies, routing, DNS forwarding, DHCP services, VDOM interface assignments, and routing. If they are not removed, you will not be able to switch modes, and you will see an error message. The web-based manager displays the list of affected interfaces.

When you select Switch Mode on the Interface page, the Switch Mode Management screen displays. From the CLI, you can also add software switch interfaces.

Use the following table when configuring switch mode on a unit.

### Interface page containing switch mode settings (FortiWiFi models only)

Provides settings for switching a group of related FortiGate interfaces to operate as a multi-port switch with one IP address.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch Mode</strong></td>
<td>Select Switch Mode. Only one internal interface is displayed. This is the default mode.</td>
</tr>
</tbody>
</table>

---

**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.

**TELNET**

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

**Detect Interface Status for Gateway Load Balancing**

- **Detect Server**: Enter the server’s IP address.
- **Detect Protocol**: Select the check box beside the protocol that will be detected for gateway load balancing.
- **Weight**: Enter the load balancing weight.
- **Spillover Threshold**: Enter the spillover threshold number in KBps.
- **Secondary IP Address**: Add additional IPv4 addresses to this interface. Select the blue arrow to expand or hide the section.
- **Description**: Enter a description up to 63 characters to describe the interface.

**Administrative Status**

Select either Up (green arrow) or Down (red arrow) as the status of this interface.

- **Up**: indicates the interface is active and can accept network traffic.
- **Down**: indicates the interface is not active and cannot accept traffic.
Adding VLAN interfaces

A VLAN interface, sometimes called a VLAN or a VLAN subinterface, is a virtual interface on a physical interface that accepts VLAN-tagged packets using that physical interface.

To add a VLAN interface, go to System > Network > Interface, select Create New, and use the New Interface page table to configure the settings.

To view VLAN interfaces, on the Interface page, expand the parent physical interface of the VLAN interface. If there is no expand arrow displayed, there are no subinterfaces configured on that physical interface. For example, a VLAN subinterface was configured on wan2, and on the Interface page, an expand arrow appears beside wan2.

Adding loopback interfaces

A loopback interface is an ‘always up’ virtual interface that is not connected to any other interfaces. Loopback interfaces connect to a unit’s interface IP address without depending on a specific external port.

Loopback interfaces were added to assist with blackhole routing which drops packets sent to a particular network address.

A loopback interface is not connected to hardware, so it is not affected by hardware problems. As long as the unit is functioning, the loopback interface is active. This ‘always up’ feature is useful in dynamic routing where the unit relies on remote routers and the local Firewall policies to access to the loopback interface.

To add a loopback interface, go to System > Network > Interface, select Create New, and use the New Interface page table to configure the settings.

Adding 802.3ad aggregate interfaces

On some models, you can aggregate (combine) two or more physical interfaces into an IEEE standard 802.3ad link aggregate interface to increase bandwidth and provide some link redundancy. An aggregate interface is similar to a redundant interface. Aggregate interfaces provides more bandwidth for the connection to a network, but also create more points of failure than redundant interfaces. Aggregate interfaces must all connect to the same next-hop routing destination.

An interface is available to be an aggregate interface if:

- it is a physical interface, not a VLAN interface
- it is not already part of an aggregate or redundant interface
- it is in the same VDOM as the aggregated interface
- it does not have a IP address and is not configured for DHCP or PPPoE
- it does not have a DHCP server or relay configured on it
- it does not have any VLAN subinterfaces
- it is not referenced in any firewall policy, VIP, or multicast policy
- it is not an HA heartbeat interface
- it is not one of the FortiGate-5000 series backplane interfaces

Interfaces included in an aggregate interface are not listed on the System > Network > Interface list. You cannot configure the interface individually and it is not available for inclusion in firewall policies, firewall virtual IPs, or routing.

**Note:** You can add an accelerated interface (FA2 interfaces) to an aggregate link, but you will lose the FA2 acceleration. For example, if you aggregate two accelerated interfaces you will get slower throughput than if the two interfaces were separate.

To add an 802.3ad Aggregate interface, go to System > Network > Interface, select Create New, and use the New Interface page table to configure the settings. The Name field must contain a different name than other interfaces, such as zone or VDOM.

### Adding redundant interfaces

On some models 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.

In a redundant interface, traffic is only going over one interface at any time. This differs from an aggregated interface where traffic is going over all interfaces for increased bandwidth. This difference means redundant interfaces can have more robust configurations with fewer possible points of failure. This is important in a fully-meshed HA configuration.

An interface is available to be in a redundant interface 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
- 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, or multicast policy
- it is not monitored by HA
- it is not one of the FortiGate-5000 series backplane interfaces

When an interface is included in a redundant interface, it is not listed on the System > Network > Interface page. You cannot configure the interface individually and it is not available for inclusion in firewall policies, VIPs, or routing.

To add a redundant interface, go to System > Network > Interface, select Create New, and use the and use the New Interface page table to configure the settings. The Name field must contain a different name than other interfaces, such as zone or VDOM.

### Configuring DHCP on an interface

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

By default, low-end models are configured to DHCP addressing mode with Override Internal DNS and Retrieve default Gateway from DHCP server both enabled. These settings allow for easy out-of-the-box configuration.
Configure DHCP for an interface in System > Network > Interface using the following table. Make sure to select DHCP in the Address Mode section of the New Interface page.

<table>
<thead>
<tr>
<th>Addressing mode section of New Interface page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Obtained IP/Netmask</strong></td>
</tr>
<tr>
<td><strong>Renew</strong></td>
</tr>
<tr>
<td><strong>Expiry Date</strong></td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
</tr>
<tr>
<td><strong>Distance</strong></td>
</tr>
<tr>
<td><strong>Retrieve default gateway from server</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Override internal DNS</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Configuring PPPoE on an interface**

If you configure the interface to use PPPoE, the unit automatically broadcasts a PPPoE request from the interface.

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

Configure PPPoE on an interface in System > Network > Interface using the following table.

<table>
<thead>
<tr>
<th>Addressing mode section of New Interface page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>initializing</strong></td>
</tr>
<tr>
<td><strong>connecting</strong></td>
</tr>
</tbody>
</table>
Configuring Dynamic DNS on an interface

When the unit has a static domain name and a dynamic public IP address, you can use a Dynamic DNS (DDNS) service to update Internet DNS servers when the IP address for the domain changes. DDNS is available only in NAT/Route mode.

If at any time your 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.

To configure DDNS on an interface

1. Get the DDNS configuration information from your DDNS service.
2. Go to System > Network > Interface.
3. Select Create New.
4. Select the check box beside Enable DDNS.
5. Enter DDNS configuration information using the following table.

The following appears after selecting Enable DDNS:

<table>
<thead>
<tr>
<th>Server</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a DDNS server to use. The client software for these services is built into the firmware. The unit can connect only to one of these services.</td>
<td>Enter the fully qualified domain name of the DDNS service.</td>
</tr>
</tbody>
</table>
Configuring virtual IPSec interfaces

You create a virtual IPSec interface by selecting **Enable IPSec Interface Mode** when configuring **Advanced** options for an IPSec VPN Phase 1.

In both cases the IPSec VPN virtual interface is added to the physical interface you select in the IPSec VPN configuration.

Virtual IPSec interfaces are listed **System > Network > Interface** list. For more about configuring IPSec VPN, see "Auto Key (IKE)" on page 300 and "Manual Key" on page 306.

For an IPSec VPN interface you can:

- 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
- enter a description for the interface

**To configure a virtual IPSec interface**

1. Go to **VPN > IPsec > Auto Key (IKE)**.
2. Select **Create New Phase 1**.
3. Expand the Advanced options.
4. Select the check box beside **Enable IPsec Interface Mode**.
5. Select the **IKE Version** that you want to use for the interface.
6. Select the type of local gateway IP:
   - **Main Interface IP** Enter the IP address of the main interface.
   - **Specify** Enter the IP address that you want to use as the local gateway IP address.
7. Configure the rest of the phase 1 settings and then select **OK**.
   If you need to create a phase 2, do so as well.
8. To verify that the interface is configured and available, go to **Firewall > Policy > Policy**, and select **Create New**. In either the **Source Interface/Zone** or **Destination Interface/Zone**, use the drop-down list to view the IPSec virtual interface that you created.

**Configuring administrative access to an interface**

Administrative access is how an administrator can connect to the unit to view and change configuration settings.

You can allow remote administration of the unit running in NAT/Route mode, but allowing remote administration from the Internet could compromise the security of the unit. You should avoid this unless it is required for your configuration.

To improve the security of a 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.

For more information on configuring administrative access in Transparent mode, see “Operation mode and VDOM management access” on page 112.

**To control administrative access to an interface**

1. Go to **System > Network > Interface**.
2. Edit the interface that you want to control administrative access on.
3. Select the **Administrative Access** methods for the interface.
4. Select **OK**.

**Configuring interface status detection for gateway load balancing**

Interface status detection consists of the unit confirming that packets sent from an interface result in a response from a server. You can use up to three different protocols to confirm that an interface can connect to the server. Usually the server is the next-hop router that leads to an external network or the Internet. Interface status detection sends a packet using the configured protocols. If a response is received from the server, the unit assumes the interface can connect to the network. If a response is not received, the unit assumes that the interface cannot connect to the network.

Interface status detection is used for ECMP route failover and load balancing. For more information, see “ECMP route failover and load balancing” on page 177.

Since it is possible that a response may not be received, even if the server and the network are operating normally, the dead gateway detection configuration controls the time interval between testing the connection to the server and the number times the test can fail before the unit assumes that the interface cannot connect to the server. For more information about configuring dead gateway detection, see “Configuring Networking Options” on page 79.

To configure gateway failover detection for an interface, go to System > Network > Interface and edit an interface using the following table, making sure to select **Detect Interface Status for Gateway Load Balancing**. If you have added secondary IP addresses to an interface you can also configure interface status detection separately for each secondary IP address.

**Note:** As long as the unit receives responses for at least one of the protocols that you select, the unit assumes the server is operating and can forward packets. Responses that are received to more than one protocol does not enhance the status of the server or interface, and receiving responses from fewer protocols does not reduce the status of the server or interface.

**The Detect Interface Status for Gateway Load Balancing section of the New Interface page**

- **Detect Server**
  - The IP address of the server to test connecting to.

- **Ping**
  - Use standard ICMP ping to confirm that the server is responding. Ping confirms that the server can respond to an ICMP ping request.

- **TCP Echo**
  - Use TCP echo to confirm that the server is responding. Select this option if the server is configured to provide TCP echo services. In some cases a server may be configured to reply to TCP echo requests but not to reply to ICMP pings. TCP echo uses TCP packets on port number 7 to send a text string to the server and expect an echo reply back from the server. The echo reply just echoes back the same text to confirm that the server can respond to TCP requests. FortiGate units do not recognize RST (reset) packets from TCP Echo servers as normal TCP echo replies. If the unit receives an RST response to a TCP echo request, the unit assumes the server is unreachable.
Changing interface MTU packet size

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

Interfaces on some models support frames larger than the traditional 1,500 bytes. Contact Fortinet Customer Support for the maximum frame sizes that your unit supports.

If you need to enable sending larger frames over a route, you need all Ethernet devices on that route to support that larger frame size, otherwise your larger frames will not be recognized and are dropped.

If you have standard size and larger size 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 larger frame traffic is routed over network devices that support that larger size. 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.

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. Below Administrative Access, select Override default MTU value (1,500).
4. Set the MTU size.

If you select an MTU size larger than your unit supports, an error message will indicate this. In this situation, try a smaller MTU size until the value is supported.

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

In Transparent mode, if you change the MTU of an interface, you must change the MTU of all interfaces on the unit to match the new MTU.
Adding secondary IP addresses to an interface

If an interface is configured with a manual or static IP address, you can also add secondary static IP addresses to the interface. Adding secondary IP addresses effectively adds multiple IP addresses to the interface. The unit, static and dynamic routing, and the network see the secondary IP addresses as additional IP addresses that terminate at the interface. Secondary IP addresses cannot be assigned using DHCP or PPPoE.

All of the IP addresses added to an interface are associated with the single MAC address of the physical interface and all secondary IP addresses are in the same VDOM as the interface that are added to. You configure interface status detection for gateway load balancing separately for each secondary IP addresses. As with all other interface IP addresses, secondary IP addresses cannot be on the same subnet as any other primary or secondary IP address assigned to a FortiGate interface unless they are in separate VDOMs.

To add secondary IP addresses to an interface

1. Go to System > Network > Interface.
2. Edit the physical interface to add secondary IP addresses to.
3. Make sure the interface Addressing Mode is set to Manual and that you have added an IP/Netmask to the interface.
4. Select the blue arrow to expand the Secondary IP Address section.
5. Configure the settings for a secondary IP address and select OK to add the address and its configuration settings to the interface.
6. Repeat to add more secondary IP addresses.
7. Select OK or Apply at the bottom of the Edit Interface dialog to add the secondary IP addresses to the interface.

Tip: After adding secondary IP addresses and selecting OK to save changes to the Edit Interface dialog, you should view the interface again to make sure the secondary IP addresses have been added as expected.

Secondary IP Address section of the New Interface page

Lists the secondary IP addresses that you created.

<table>
<thead>
<tr>
<th>Add</th>
<th>Select to create a new secondary IP address. When you select Add, you are automatically redirected to the Edit Interface page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/Netmask</td>
<td>The IP address and netmask for the secondary IP.</td>
</tr>
<tr>
<td>Detect Server Enable</td>
<td>Indicates whether interface status detection is enabled for the secondary IP address.</td>
</tr>
<tr>
<td>Detect Server</td>
<td>The IP address of the detect server for the secondary IP address. The same detect server can be shared by multiple secondary IP addresses.</td>
</tr>
<tr>
<td>Detect Protocol</td>
<td>The detect protocols configured for the secondary IP address.</td>
</tr>
<tr>
<td>Administrative Access</td>
<td>The administrative access methods for this address. They can be different from the primary IP address.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the secondary IP address from the list within the Secondary IP Address section.</td>
</tr>
</tbody>
</table>
Adding software switch interfaces

You can add software switch interfaces (also called soft switch interfaces) from the CLI. A software switch interface forms a simple bridge between two or more physical or wireless FortiGate interfaces. The interfaces added to a software switch interface are called physical interface members. The members of a software switch interface cannot be accessed as individual interfaces after being added to a software switch interface. They are removed from the system interface table.

Similar to aggregate interfaces, a software switch interface functions like a normal interface. A software switch interface has one IP address. You create firewall policies to and from software switch interfaces and software switch interfaces can be added to zones. There are some limitations; software switch interfaces cannot be monitored by HA or used as HA heartbeat interfaces.

If you want to add interfaces to a software switch interface, no configuration settings can refer to those interfaces. This includes default routes, VLANs, inter-VDOM links, and policies.

Use the following CLI command to add a software switch interface called soft_switch that includes the port1, external and dmz physical interfaces:

```
cfg  
```
Adding an sFlow agent to a FortiGate interface

sFlow is a network monitoring protocol defined in RFC 3176 and described in [http://www.sflow.org](http://www.sflow.org). You can configure one or more FortiGate interfaces as sFlow agents that monitor network traffic and send sFlow datagrams containing information about traffic flow to an sFlow collector. You can add sFlow agents to any FortiGate interface, including physical interfaces, VLAN interfaces, and aggregate interfaces.

sFlow is normally used to provide an overall traffic flow picture of your network. You would usually operate sFlow agents on switches, routers, and firewalls on your network, collect traffic data from all of them and use a collector to show traffic flows and patterns.

Using this data you can determine normal traffic flow patterns for your network and then monitor for traffic flow problems. As these problems are found you can attempt to correct them and continue to use the sFlow agents and collectors to view the results of your corrective action.

The FortiGate sFlow agent functions like any sFlow agent, combining interface counters and flow samples into sFlow datagrams that are immediately sent to an sFlow collector. Because the sFlow datagrams are sent immediately without processing the data and without collecting large amounts of data, running the sFlow agent has almost no effect on system performance.

You can only configure sFlow from the CLI. To begin using sFlow you must add the IP address of your sFlow connector to the FortiGate configuration and then configure sFlow agents on FortiGate interfaces.

To configure the unit to send sFlow datagrams to an sFlow collector

1. Enter the following command to set the IP address of your sFlow collector to 172.20.120.11:
   ```plaintext
   config system sflow
   set collector-ip 172.20.120.11
   end
   ```

2. If required you can also change the UDP port number that the sFlow agent uses. You should only change this port if required by your network configuration or sFlow collector. The default sFlow port is 6343. The following command changes the sFlow agent port to 5345:
   ```plaintext
   config system sflow
   set collector-port 5345
   end
   ```

3. Use the following command to enable sFlow for the port1 interface:
   ```plaintext
   config system interface
   edit port1
   set sflow-sample enable
   end
   ```

4. Repeat this step to add sFlow agents to the FortiGate interfaces.

5. You can also change the sampling rate, polling interval, and sample direction for each sFlow agent:
   ```plaintext
   config system interface
   edit port1
   set sample-rate <rate_number>
   ```
set polling-interval <frequency>
set sample-direction {both | rx | tx}
end

sFlow with multiple VDOMs

For a unit operating with multiple VDOMs, you can add different sFlow collector IP addresses and port numbers to each non-management VDOM. Use the following command to customize the sFlow configuration for a VDOM named VDOM_1:

```
config vdom
edit VDOM_1
  config system vdom-sflow
  set vdom-sflow enable
  set collector-ip 172.20.120.11
end
```

The management VDOM and all VDOMs that you have not configured a VDOM-specific configuration for use the global sFlow configuration.

Configuring zones

By grouping interfaces into a zone you can add one set of firewall policies for the zone instead of adding separate policies for each interface. After adding interfaces to a zone, you cannot configure policies for the interfaces, but only for the zone.

You can add all types of interfaces to a zone (physical, VLAN, switch, and so on) and a zone can consist of any combination of interface types. 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 to add to the zone.

Zones are configured from 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.

Use the following table to configure zones in System > Network > Zone.

<table>
<thead>
<tr>
<th>Zone page</th>
<th>Lists all of the zones that you created. On this page you can edit, delete and create new zones.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new zone. When you select Create New, you are automatically redirected to the Edit Zone page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies settings within a zone. When you select Edit, you are automatically redirected to the Edit Zone page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a zone from within the list on the Zone page. To remove multiple zones within the list, on the Zone page, in each of the rows of the zones you want removed, select the check box and then select Delete. To remove all zones within the list, on the Zone page, select the check box in the check box column, and then select Delete.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the zone that you created.</td>
</tr>
<tr>
<td>Block intra-zone traffic</td>
<td>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.</td>
</tr>
<tr>
<td>Interface Members</td>
<td>Names of the interfaces added to the zone. Interface names depend on the FortiGate model.</td>
</tr>
</tbody>
</table>

Edit Zone page

Provides settings for configuring zones. When editing an existing zone, you are automatically redirected to this page.

| Zone Name | Enter the name for the zone. |
Configuring the modem interface

The unit can include a modem interface if you connect a modem in one of the following ways:

- You can connect a supported USB mode to any model with a USB interface.
- You can connect a supported serial model to any model with a serial modem port.
- You can insert a supported PCMCIA modem into any model with a PCMCIA slot. Power off the unit before inserting the PCMCIA modem. After inserting the modem, when you power up the unit it should automatically find the modem and create the modem interface.

In NAT/Route mode the modem can be in one of two modes:

- 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 unit to the Internet.

In redundant or standalone mode when connecting to the ISP, you can configure the unit to automatically have the modem dial up to three dialup accounts until the modem connects to an ISP.

Other models can connect to an external modem through a USB-to-serial converter. For these models, you must configure modem operation using the CLI.

Initially, modem interfaces are disabled and must be enabled in the CLI using the **system modem** command, so that to be visible in the web-based manager.

### Note:
The modem interface is not the AUX port. While the modem and AUX port may appear similar, the AUX port has no associated interface and is used for remote console connection. The AUX port is only available on models 1000A, 1000AFA2, and 3000A. For more information, see the **config system aux** command.

Configuring modem settings

When modem settings are configured on the unit, the 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.

For FortiGate-60B and FortiWifi-60B models with modems, the modem can be a management interface. When enabled, a user can dial into the unit’s modem and perform administration actions as if logged in over one of the standard interfaces. This feature is enabled in the CLI using the **config system dialinsvr** command syntax.

If VDOMs are enabled, the modem can be assigned to one of the VDOMs just like the other interfaces.

If the modem is disabled, it will not appear in the interface list and must be enabled from the CLI using the following command syntax:

```
cfgi system modem
  set status enable
end
```
After being enabled in the CLI, you can then go to System > Network > Modem to configure the modem in the web-based manager. Use the following table when configuring the modem settings in System > Network > Modem.

To configure the modem in Redundant mode, see “Redundant mode configuration” on page 77.

To configure the modem in Standalone mode, see “Standalone mode configuration” on page 78.

Note: You cannot configure and use the modem in Transparent mode.

---

**Modem page**
Provides settings for configuring the modem and dialup accounts.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Modem</strong></td>
<td>Select to enable the modem on the unit.</td>
</tr>
<tr>
<td><strong>Modem status</strong></td>
<td>Modem status can be: not active, connecting, connected, disconnecting, or hung up.</td>
</tr>
<tr>
<td><strong>Dial Now/Hang Up</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Select Standalone or Redundant mode.</td>
</tr>
<tr>
<td><strong>Auto-dial</strong> (Standalone mode)</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Dial on demand</strong> (Standalone mode)</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Idle timeout</strong> (Standalone mode)</td>
<td>Enter the timeout duration in minutes. After this period of inactivity, the modem disconnects.</td>
</tr>
<tr>
<td><strong>Redundant for</strong> (Redundant mode)</td>
<td>Select the ethernet interface for which the modem provides backup service.</td>
</tr>
<tr>
<td><strong>Holddown</strong> (Redundant mode)</td>
<td>(Redundant mode only) Enter the time (1-60 seconds) that the 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 unit switching repeatedly between the primary interface and the modem interface.</td>
</tr>
<tr>
<td><strong>Redial Limit</strong></td>
<td>The maximum number of times (1-10) that the 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.</td>
</tr>
<tr>
<td><strong>Wireless Modem</strong></td>
<td>Display a connected wireless modem if available.</td>
</tr>
<tr>
<td><strong>Supported Modems</strong></td>
<td>Select to view a list of supported modems.</td>
</tr>
<tr>
<td><strong>Usage History</strong></td>
<td>Display connections made on the modem interface. Information displayed about connections includes:</td>
</tr>
<tr>
<td></td>
<td>• date and time</td>
</tr>
<tr>
<td></td>
<td>• duration of the connection in hours, minutes, and seconds</td>
</tr>
<tr>
<td></td>
<td>• IP address connected to</td>
</tr>
<tr>
<td></td>
<td>• traffic statistics including received, sent, and total</td>
</tr>
<tr>
<td></td>
<td>• current status of the connection</td>
</tr>
<tr>
<td><strong>Dialup Account</strong></td>
<td>Configure up to three dialup accounts. The unit tries connecting to each account in order until a connection can be established. The active dialup account is indicated with a green check mark.</td>
</tr>
</tbody>
</table>
Redundant mode configuration

In redundant mode, the modem interface 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 unit routes IP packets normally destined for the selected ethernet interface to the modem interface.

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

The modem will disconnect after a period of network inactivity set by the value in idle timeout. This saves money on dialup connection charges.

For the 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:
   - **Redundant for**
   - **Holddown timer**
   - **Redial Limit**
   - **Dialup Account 1**
   - **Dialup Account 2**
   - **Dialup Account 3**
4. Select Apply.
5. To configure interface status detection for the Ethernet interface the modem backs up, see “Configuring interface status detection for gateway load balancing” on page 69.
6. To configure firewall policies for network connectivity through the modem interface, see “Adding firewall policies for modem connections” on page 78.
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 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 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.

The modem will disconnect after a period of network inactivity set by the value in idle timeout. This saves 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 > Static Route to configure static routes to route traffic to the modem interface. For example, if the modem interface is acting as the unit’s external interface, you must set the device setting of the unit default route to modem.

To configure standalone mode

1. Go to System > Network > Modem.
2. Select Standalone mode.
3. Enter the following information:
   - Auto-dial: Select if you want the modem to dial when the 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, Dialup Account 2, Dialup Account 3: Enter the ISP phone number, user name and password for up to three dialup accounts.
4. Select Apply.
5. To configure firewall policies for network connectivity through the modem interface, go to Firewall > Policy > Policy, select Create New, and configure the policy.
6. To configure static routes to route traffic to the modem interface, go to Router > Static > Static Route and use the procedure in “Adding a static route to the routing table” on page 177.

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.

You can configure firewall policies to control the flow of packets between the modem interface and the other interfaces on the unit.

To add firewall policies for modem connections, go to Firewall > Policy > Policy and configure the policy as you would normally do for any other firewall policy. If you need more information about firewall policies, see the FortiGate Fundamentals chapter in the FortiOS Handbook.
Connecting and disconnecting the modem

The following procedure explains how to connect and disconnect from a dialup account. You should verify that the modem is in Standalone mode before disconnecting or connecting from a dialup account because the modem must be in Standalone mode.

To connect to a dialup account
1. Go to System > Network > Modem.
2. Select Enable USB Modem.
3. Verify the information in Dialup Accounts.
4. Select Apply.
5. Select Dial Now.

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

To disconnect from a dialup account
1. Go to System > Network > Modem.
2. Select Hang Up to disconnect the modem.

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 screen of the web-based manager.

Configuring Networking Options

Network options include DNS server and dead gateway detection settings. Dead gateway detection settings control how interface status detection functions. You can configure DNS and other network options settings from System > Network > Options.

Use the following table when configuring or modifying DNS settings and dead gateway detection.

**Networking Options page**

Provides settings for configuring DNS settings as well as dead gateway detection settings. You can also view DNS server settings and dead gateway detection settings from this page.
DNS Settings

- **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.

IPv6 DNS Settings

- **Primary DNS Server**: Enter the primary IPv6 DNS server IP address.
- **Secondary DNS Server**: Enter the secondary IPv6 DNS server IP address.

**Dead Gateway Detection**

Configure interface status detection for one or more interfaces and use the dead gateway detection settings to configure how interface status detection functions. For information, see “Configuring interface status detection for gateway load balancing” on page 69.

- **Detection Interval**: Enter a number in seconds to specify how often the unit detects interface status.
- **Fail-over Detection**: Enter the number of times that interface status tests fail before the unit assumes that the interface is no longer functioning.

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 unit connects. DNS server IP addresses are usually supplied by your ISP.

You can configure models numbered 100 and lower to obtain DNS server addresses automatically. At least one FortiGate interface must use the DHCP or PPPoE addressing mode to obtain these addresses automatically. For more information, see “Configuring DHCP on an interface” on page 65 or “Configuring PPPoE on an interface” on page 66.

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 unit obtained automatically.

**FortiGate DNS services**

You can configure a unit to be the DNS server for any networks that can communicate with a FortiGate interface. You set up the DNS configuration for each interface in one of the following ways:

- The interface relays DNS requests to the DNS servers configured for the unit under System > Network > Options.
- The interface resolves DNS requests using a FortiGate DNS database. DNS requests for host names not in the FortiGate DNS database are dropped.
- The interface resolves DNS requests using the FortiGate DNS database and relays DNS requests for host names not in the FortiGate DNS database to the DNS servers configured for the unit under System > Network > Options. This is called a split DNS configuration.

If virtual domains are not enabled you can create one DNS databases that can be shared by all the FortiGate interfaces.

If virtual domains are enabled, you create a DNS database in each VDOM. All of the interfaces in a VDOM share the DNS database in that VDOM.
About split DNS

In a split DNS configuration you create a DNS database on the unit, usually for host names on an internal network or for a local domain. When users on the internal network attempt to connect to these host names the IP addresses are provided by the FortiGate DNS database. Host names that are not in the FortiGate DNS database are resolved by relaying the DNS lookup to an external DNS server.

A split DNS configuration can be used to provide internal users access to resources on your private network that can also be accessed from the Internet. For example, you could have a public web server behind a unit operating in NAT/Route mode. Users on the Internet access this web server using a port forwarding virtual IP. So the web server has a public IP address for internet users. But you may want users on your internal network to access the server using its private IP address to keep traffic from internal users off of the Internet. To do this, you create a split DNS configuration on the unit and add the host name of the server to the FortiGate DNS database, but include the internal IP address of server instead of the external IP address. Because the unit checks the FortiGate DNS database first, all DNS lookups for the server host name will return the internal IP address of the server.

For an example of how to configure split DNS, see “To configure a split DNS configuration” on page 83.

Configuring FortiGate DNS services

This section provides a general procedure for configuring FortiGate DNS as well as specific procedures for configuring a FortiGate interface to provide DNS services in different ways.

General FortiGate DNS server configuration

1. Go to System > Network > Options and add the IP addresses of a Primary and Secondary DNS server.

   These should be the DNS servers provided by your ISP or other public DNS servers. The unit uses these DNS servers for its own DNS lookups and can be used to supply DNS look ups for your internal networks. See “Configuring Networking Options” on page 79.

2. Go to System > Network > Interface and edit the interface connected to a network that you want the unit to be a DNS server for.

3. Select Enable DNS Query.

   • When you select Enable DNS Query, the unit relays all DNS queries received by this interface to the DNS servers configured under System > Network > Options. Select Recursive or Non-Recursive to control how this works. Recursive – Looks up domain names in the FortiGate DNS database. If the entry is not found, the request is replayed to the DNS servers configured in System > Network > Options. This setting can be used to split DNS configuration.

   • Non-recursive – Looks up domain names in the FortiGate DNS database. This setting does not relay the request to the DNS servers that are configured in System > Network > Options.

4. Go to System > Network > DNS Database and configure the FortiGate DNS database. Add zones and entries as required. See "Configuring the FortiGate DNS database" on page 83.
5 Configure the hosts on the internal network to use the FortiGate interface as their DNS server. If you are also using a FortiGate DHCP server to configure the hosts on this network, add the IP address of the FortiGate interface to the DNS Server IP address list.

Configure a FortiGate interface to relay DNS requests to the DNS servers configured for the FortiGate unit under System > Network > Options.

**To configure a FortiGate interface to relay DNS requests to external DNS servers**

1 Go to System > Network > Options and add the IP addresses of a Primary and Secondary DNS server.

These should be the DNS servers provided by your ISP or other public DNS servers. The unit uses these DNS servers for its own DNS lookups and can be used to supply DNS look ups for your internal networks. See “Configuring Networking Options” on page 79.

2 Go to System > Network > Interface and edit the interface connected to a network that you want the unit to be a DNS server for.

3 Select Enable DNS Query and select Recursive.

The interface is configured to look up domain names in the FortiGate DNS database and relay the requests for names not in the FortiGate DNS database to the DNS servers configured under System > Network > Options. If you do not add entries to the FortiGate DNS database all DNS requests are relayed to the DNS servers configured under System > Network > Options.

4 Configure the hosts on the internal network to use the FortiGate interface as their DNS server.

If you are also using a FortiGate DHCP server to configure the hosts on this network, add the IP address of the FortiGate interface to the DNS Server IP address list.

Configure a FortiGate interface to resolve DNS requests using the FortiGate DNS database and to drop requests for host names that not in the FortiGate DNS database.

**To configure a FortiGate interface to resolve DNS requests using only the FortiGate DNS database**

1 Go to System > Network > Options and add the IP addresses of a Primary and Secondary DNS server.

These should be the DNS servers provided by your ISP or other public DNS servers. The FortiGate unit uses these DNS servers for its own DNS lookups and can be used to supply DNS look ups for your internal networks. See “Configuring Networking Options” on page 79.

2 Go to System > Network > Interface and edit the interface connected to a network that you want the FortiGate unit to be a DNS server for.

3 Select Enable DNS Query and select Non-Recursive.

When you select Non-Recursive only the entries in the FortiGate DNS database are used.

4 Go to System > Network > DNS Database and configure the FortiGate DNS database. Add zones and entries as required. See “Configuring the FortiGate DNS database” on page 83.
5 Configure the hosts on the internal network to use the FortiGate interface as their DNS server.

If you are also using a FortiGate DHCP server to configure the hosts on this network, add the IP address of the FortiGate interface to the DNS Server IP address list.

Configure an interface to resolve DNS requests using the FortiGate DNS database and relay DNS requests for host names not in the FortiGate DNS database to the DNS servers configured under System > Network > Options. This is called a split DNS configuration. See “About split DNS” on page 81.

To configure a split DNS configuration

1 Go to System > Network > Options and add the IP addresses of a Primary and Secondary DNS server.

These should be the DNS servers provided by your ISP or other public DNS servers. The unit uses these DNS servers for its own DNS lookups and can be used to supply DNS look ups for your internal networks. See “Configuring Networking Options” on page 79.

2 Go to System > Network > Interface and edit the interface connected to a network that you want the unit to be a DNS server for.

3 Select Enable DNS Query and select Recursive.

The interface is configured to look up domain names in the FortiGate DNS database and relay the requests for names not in the FortiGate DNS database to the DNS servers configured under System > Network > Options. You can add entries to the FortiGate DNS database for users on the internal network. See “Configuring the FortiGate DNS database” on page 83.

4 Go to System > Network > DNS Database and configure the FortiGate DNS database.

Add zones and entries as required for users on the internal network. See “Configuring the FortiGate DNS database” on page 83.

5 Configure the hosts on the internal network to use the FortiGate interface as their DNS server.

If you are also using a FortiGate DHCP server to configure the hosts on this network, add the IP address of the FortiGate interface to the DNS Server IP address list.

Configuring the FortiGate DNS database

The FortiGate DNS database must be configured so that DNS lookups from an internal network are resolved by the FortiGate DNS database. You also need to add zones when configuring the DNS database. Each zone has its own domain name.

You then add entries to each zone. An entry is an host name and the IP address it resolves to. You can also specify if the entry is an IPv4 address (A), an IPv6 address (AAAA), a name server (NS), a canonical name (CNAME), or a mail exchange (MX) name.

Configure the FortiGate DNS database from System > Network > DNS Server using the following table.
**DNS Server page**
Lists the DNS servers that you have created. On this page, you can edit, delete or create a new DNS server.

| Create New | Creates a new DNS zone to the DNS database list. When you select Create New, you are automatically redirected to the New DNS Zone page. After you enter the DNS zone, domain name and TTL (seconds) information, the DNS Entries section of the page appears and the page name changes to Edit DNS Zone. |
| DNS Zone | The names of the DNS zones added to the DNS database list. |
| Domain Name | The domain name of each zone. |
| TTL | The TTL value for the domain name which is the packet time to live in seconds. The range is 0 to 2 147 483 647. |
| # of Entries | The number of entries in the zone. |
| Delete | Removes a zone from the DNS database. To remove multiple DNS zones from within the list, on the DNS Server page, in each of the rows of the servers you want removed, select the check box and then select Delete. To remove all DNS zones from the list, on the DNS Server page, select the check box in the check box column and then select Delete. |
| Edit | Modifies an existing zone’s settings. When you select Edit, you are automatically redirected to the Edit DNS Zone page. |

**New DNS Zone/Edit DNS Zone page**
Provides settings for configuring DNS zones which make up a DNS server.

| DNS Zone | Enter the DNS zone. |
| Domain Name | Enter the domain name. |
| TTL (seconds) | Enter the TTL value. Enter 0 to use the Zone TTL value. |

**DNS Entries section of the Edit DNS Zone page**

| Create New | Creates a new DNS entry. When you select Create New, you are automatically redirected to the New DNS Entry page. |
| Edit | Modifies settings within a DNS entry. When you select Edit, you are automatically redirected to the Edit DNS Entry page. |
| Delete | Removes a DNS entry from list within the DNS Entries section of the page. To remove multiple DNS entries from within the list, on the Edit DNS Zone page, in each of the rows of the entries you want removed, select the check box and then select Delete. To remove all DNS entries from the list, on the Edit DNS Zone page, select the check box in the check box column and then select Delete. |

**New DNS Entry page**
Provides settings for configuring each DNS entry. When you select Create New within the DNS Entries section of the Edit DNS Zone page.

| Type | Select a type from the drop-down list. You can select Address (A), IPv6 Address (AAAA), Name Server (NS), Canonical Name (CNAME), and Mail Exchange (MX). |
| Hostname | Enter the host name in the field. |
| IP Address | Enter the IP address. |
| IPv6 Address | Enter the IPv6 address. This field appears only when Type is set to IPv6 Address (AAAA). |
| Canonical Name | Enter the canonical name. This field appears only when Type is set to Canonical Name (CNAME). |
Configuring the explicit web proxy

Caution: Enabling the explicit web proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.

You can use the explicit web proxy to enable explicit HTTP and HTTPS proxying on one or more FortiGate interfaces. The explicit web proxy also supports proxying FTP sessions sent from a web browser and proxy auto-config (PAC) to provide automatic proxy configurations for explicit web proxy users. From the CLI, you can also configure the explicit web proxy to support SOCKS sessions sent from a web browser.

Note: Web proxies are configured for each VDOM when VDOMs are enabled.

The web proxy uses FortiGate routing to route sessions through the unit to a destination interface. Before a session leaves the exiting interface, the explicit web proxy changes the source addresses of the session packets to the IP address of the exiting interface. When the unit is operating in Transparent mode, the explicit web proxy changes the source addresses to the management IP address.

Usually, to configure a web proxy server for users on a network, you would enable the explicit web proxy on the FortiGate interface connected to that network. Users on the network would configure their web browsers to use a proxy server for HTTP and HTTPS, FTP, or SOCKS and set the proxy server IP address to the IP address of the FortiGate interface connected to their network. Users could also enter the PAC URL into their web browsers to automate their web proxy configuration using a PAC file stored on the unit. The proxy tries to keep the persistent sessions alive with the clients; however, there is no limit for each user and a persistent session is removed after an idle timeout of 3600 seconds.

On units that support WAN optimization, you can also enable web caching for the explicit proxy. For more information, see “Cache exempt list” on page 344.

To enable the explicit web proxy

1 Go to System > Network > Interface and enable the explicit web proxy for one or more FortiGate interfaces.

Caution: Enabling the explicit web proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.

2 Go to System > Network > Web Proxy.

3 Select Enable Explicit Web Proxy to turn on the Explicit Web Proxy.

4 Go to Firewall > Policy > Policy and select Create New and then set the Source Interface/Zone to web-proxy.
5. Configure the firewall policy as required to accept the traffic that you want to be processed by the explicit web proxy.

   The source address of the policy should match client source IP addresses. The destination address of the policy should match the IP addresses of websites that clients are connecting to.

   Traffic sent to the explicit web proxy that is not accepted by a web-proxy firewall policy is dropped.

6. Select other firewall policy options as required.

   For example, you can apply UTM protection to web proxy sessions and log allowed web proxy traffic.

7. Select Enable Identity Based Policy to apply authentication to explicit web proxy sessions.

   A number of authentication options are available:

   • For session-based authentication, each authenticated user is counted as a single user. Since multiple users can have the same user name, the proxy attempts to identify users according to their authentication membership, which is based on whether or not they were authenticated using RADIUS, LDAP, FSAE, or local databases. If a user of one session has the same name and membership as the user of another session, the explicit proxy assumes that this is one user, not two individual users.

   • For IP-based authentication, or no authentication (or if no web-proxy firewall policy was added), the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user.

   You can add multiple identity based policies to apply different authentication for different user groups and also apply different UTM and logging settings for different user groups.

**Configuring explicit web proxy settings**

Explicit web proxy settings are configured on the Web Proxy page, in System > Network > Web Proxy. Within this page, you can configure general web proxy options, such as transparent web cache.

Configure the explicit web proxy from System > Network > Web Proxy using the following table.

<table>
<thead>
<tr>
<th>Web Proxy page</th>
<th>Provides settings for configuring either the explicit web proxy and transparent web caching.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Explicit Web Proxy Options section</th>
</tr>
</thead>
</table>

Enable Explicit Web Proxy

Enable the explicit web proxy server for HTTP/HTTPS, FTP and proxy auto-config PAC sessions. You must select this option for the explicit web proxy to accept and forward packets. FTP and PAC is only supported from a web browser and not a standalone client (for example, standalone FTP clients cannot use the explicit web proxy server.)

Listen on Interfaces

Displays the interfaces that are being monitored by the explicit web proxy. If VDOMs are enabled, only interfaces that belong to the current VDOM and have explicit web proxy enabled will be displayed. If you enable the web proxy on an interface that has VLANs on it, the VLANs will only be enabled for web proxy if you manually enable each of them.

HTTP Port

Enter the port number that HTTP traffic from client web browsers use to connect to the explicit proxy. The default port number is 8080. The range is 0 to 65535. Explicit proxy users must configure their web browser’s HTTP proxy settings to use this port.
**HTTPS Port**
Enter the port number that HTTPS traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser’s HTTPS proxy settings to use this port.
The default value of 0 means use the same port as HTTP.

**FTP Port**
Enter the port number that FTP traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser’s FTP proxy settings to use this port.
The default value of 0 means use the same port as HTTP.

**PAC Port**
Select the port that PAC traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser’s PAC settings to use this port.
The default value of 0 means use the same port as HTTP.

**PAC File Content**
Select the Edit icon beside this option to change the contents in a PAC file. You can also import a PAC file using this option.
The maximum PAC file size is 8192 bytes.
You can use any PAC file syntax that is supported by your users’s browsers. The unit does not parse the PAC file.
To use PAC, users must add an automatic proxy configuration URL (or PAC URL) to their web browser proxy configuration. The default PAC file URL is:
http://<interface_ip>:<PAC_port_int>/<pac_file_str>
For example, if the interface with the explicit web proxy has IP address 172.20.120.122, the PAC port is the same as the default HTTP explicit proxy port (8080) and the PAC file name is proxy.pac the PAC file URL would be:
http://172.20.120.122:8080/proxy.pac
From the CLI you can use the following command to display the PAC file url:
```
get web-proxy explicit
```

**Unknown HTTP version**
Select the action to take when the proxy server must handle an unknown HTTP version request or message. Choose from either Reject or Best Effort.
Best Effort attempts to handle the HTTP traffic as best as it can. Reject treats known HTTP traffic as malformed and drops it. The Reject option is more secure.

**Realm**
Enter an authentication realm to identify the explicit web proxy. The realm can be any text string of up to 63 characters. If the realm includes spaces enclose it in quotes.
When a user authenticates with the explicit proxy the HTTP authentication dialog includes the realm so you can use the realm to identify the explicitly web proxy for your users.

**Default Firewall Policy Action**
Configure the explicit web proxy to block (deny) or accept sessions if firewall policies have not been added for the explicit web proxy. To add firewall policies for the explicit web proxy add a firewall policy and set the source interface to web-proxy.
The default setting or Deny blocks access to the explicit web proxy before adding a firewall policy. If you set this option to Accept the explicit web proxy server accepts sessions even if you haven’t defined a firewall policy.

**General Options (Explicit Web Proxy and Transparent Web Cache) section**

**Proxy FQDN**
Enter the fully qualified domain name (FQDN) for the proxy server. This is the domain name to enter into browsers to access the proxy server.

**Max HTTP request length**
Enter the maximum length of an HTTP request. Larger requests will be rejected.

**Max HTTP message length**
Enter the maximum length of an HTTP message. Larger messages will be rejected.

**Add headers to Forwarded Requests**
The web proxy server will forward HTTP requests to the internal network. You can include the following headers in those requests:

**Client IP Header**
Enable to include the Client IP Header from the original HTTP request.

**Via Header**
Enable to include the Via Header from the original HTTP request.
Configuring WCCP

All WCCP settings are configured in the CLI. Configure settings for Web Cache Communication Protocol (WCCP) version 2 to optimize web traffic, thus reducing transmission costs and downloading time.

When a web client (on a computer) makes a request for web content, WCCP allows the routers on the local network to redirect the web content requests to the appropriate web cache server on the local network. If the web cache server contains the information in the web content request, the web cache server sends the content directly to the local client. If the web cache does not contain the requested information, the web cache server will download the HTTP information, cache it, and send it to the local client. The local client is not aware this caching is taking place.

For web caching to function, local network traffic must be directed through one or more routers that are able to forward the HTTP requests to the web cache servers. The unit can act as a WCCP version 2 enabled router and direct web content requests to configured web cache servers.

The web caching will speed up downloads by not accessing remote websites for each HTTP request. It will also reduce the amount of data a company network sends and receives over the Internet, reducing costs.

The following are the variables and commands that are used to configure WCCP.

For the WCCP client:
```
config system setting
  set wccp-cache-engine {enable | disable}
end
```

For WCCP services:
```
config system wccp
  edit <service_id>
    set cache-id <ip_address>
    set group-address <ip_multicast_address>
    set router-list <ip_router_address>
    set authentication {enable | disable}
    set service-type {auto | standard | dynamic}
    set assignment-weight <weight_number>
    set assignment-bucket-form {cisco-implementation | wccp-v2}
end
```

Routing table (Transparent Mode)

If the unit is operating in Transparent mode, you can go to System > Network > Routing Table to add static routes to control the flow of traffic through the unit. Use the following table to add or modify static routes.

Note: In NAT/Route mode, the static routing table is located at System > Routing > Static.
DHCP Server

The DHCP Server menu provides settings for configuring DHCP servers and relays, as well as viewing leased addresses. Multiple DHCP servers and relays can be configured on any FortiGate interface.

This topic contains the following:
- DHCP servers and relays
- Service
- Viewing address leases

DHCP servers and relays

The DHCP protocol enables hosts to automatically obtain an IP address from a DHCP server. Optionally, they can also obtain default gateway and DNS server settings. A FortiGate interface or VLAN subinterface can provide the following DHCP services:
- Basic DHCP servers for non-IPSec IP networks
- 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). However, you can configure a Regular DHCP server on an interface only if the interface is a physical interface with 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.

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 unit.

### Service

On FortiGate-50 and 60 series units, 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. However, you cannot configure DHCP in Transparent mode. In Transparent mode DHCP requests pass through the unit.

An interface must have a static IP before you configure a DHCP server on it.

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.

Configure the DHCP relay or server from **System > DHCP Server > Service** using the following table as well as “Configuring DHCP on an interface” on page 65.

<table>
<thead>
<tr>
<th>Service page</th>
<th>Lists all the DHCP servers and relays that you created. On this page, you can edit, create or delete DHCP servers and relays.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new DHCP server or relay. When you select Create New, you are automatically redirected to the New DHCP Service page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies settings within the DHCP server or relay. When you select Edit, you are automatically redirected to the Edit DHCP Service page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a DHCP server or relay from the list. To remove multiple DHCP servers or relays from within the list, on the Service page, in each of the rows of servers or relays you want removed, select the check box and then select Delete. To remove all DHCP servers or relay from the list, on the Service page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td>Interface</td>
<td>The name of the FortiGate interface that the DHCP server or relay is configured for.</td>
</tr>
<tr>
<td>Mode</td>
<td>The type of DHCP used, either a relay or server.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of interface that is used. The type can be either regular or IPsec.</td>
</tr>
<tr>
<td>Options</td>
<td>The IP address range of the DHCP server. If a DHCP relay is configured, this column contains the IP address of the DHCP server.</td>
</tr>
</tbody>
</table>
**Enable**
Indicates whether the DHCP server or relay is enabled. If there is a green check mark, the server or relay is enabled. If there is a gray x, the server or relay is disabled.

**New DHCP Service page**
Provides settings for configuring a DHCP relay agent or a DHCP server.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the DHCP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Select <em>Relay</em> to configure a DHCP relay agent. Select <em>Server</em> to configure a DHCP server.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enable the DHCP server.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Regular or IPSEC DHCP server. You cannot configure a Regular DHCP server on an interface that has a dynamic IP address.</td>
</tr>
<tr>
<td>IP Range</td>
<td>Enter the start and end for the range of IP addresses that this DHCP server assigns to DHCP clients. These fields are greyed out when <em>IP Assignment Mode</em> is set to <em>User-group defined method</em>.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Enter the netmask of the addresses that the DHCP server assigns.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.</td>
</tr>
<tr>
<td>DNS Service</td>
<td>Select to use either a specific DNS server or the system's DNS settings. You can add multiple DNS servers by selecting the plus sign (+) beside DNS Server 1.</td>
</tr>
<tr>
<td>DNS Server 0</td>
<td>Enter the DNS server.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Enter the second DNS server. If you need to add more DNS servers, select the plus sign (+).</td>
</tr>
</tbody>
</table>

**Advanced section of the New DHCP Service page**
Select to configure advanced options.

| Domain | Enter the domain that the DHCP server assigns to DHCP clients. |
| Lease Time | Select Unlimited for an unlimited lease time or enter the interval in days, hours, and minutes after which a DHCP client must ask the DHCP server for new settings. The lease time can range from 5 minutes to 100 days. |
| IP Assignment Mode | Configure how the IP addresses for an IPsec DHCP server are assigned to Dialup IPSec VPN users. Select: |
| WINS Server 1 | Add the IP addresses of one or two WINS servers that the DHCP server assigns to DHCP clients. |
| WINS Server 2 | |
| Options | Select to include options for the DHCP relay or server. When you enable this option, Code field and Options field appear. You can add multiple options (both Code and Options field appear) by selecting the plus sign beside the Options field. |
| Exclude Ranges | Add a range of IP addresses to exclude. You can add up to 16 exclude ranges of IP addresses that the DHCP server cannot assign to DHCP clients. No range can exceed 65536 IP addresses. |
| Starting IP | Enter the first IP address of the exclude range. |
| End IP | Enter the last IP address of the exclude range. |
| Delete (minus sign) | Deletes the exclude range. |
Config

Viewing address leases

Address leases are available on the Address Leases page in System > DHCP Server > Address Leases. The page also displays the MAC address of the device that the IP address is assigned to.

**Address Leases page**

Lists the IP addresses that the DHCP servers have assigned, as well as the corresponding client MAC addresses.

| Interface | Select interface for which to list leases. |
| Refresh   | Refreshes 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.   |
| Status    | Indicates the status of the IP addresses for DHCP servers. |

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 assign up to 200 IP addresses as reserved. For more information, see the [FortiGate Maximum Values Matrix](#).

Use the `config system dhcp reserved-address` command to reserve IP address for specific clients.

Config

The Config menu provides settings for configuring high availability (HA) and SNMP. This menu also provides settings for customizing replacement messages as well as changing the unit’s operational mode.

This topic contains the following:

- **HA**
- **SNMP**
- **Replacement messages**
- **Operation mode and VDOM management access**

HA

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.

**HA options**

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 units in the cluster.
You can configure HA options for a unit with virtual domains (VDOMs) enabled by logging into the web-based manager as the global admin administrator and going to System > Config > HA. If HA is enabled, you will have to select Edit for the cluster member before you see the virtual cluster configuration screen for that cluster unit. For more information, see “Cluster members list” on page 94.

Note: If your 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.

Note: FortiGate HA is not compatible with PPP protocols such as PPPoE. FortiGate HA is also not compatible with DHCP. If one or more FortiGate interfaces is dynamically configured using DHCP or PPPoE, you cannot switch to operate in HA mode. Also, you cannot switch to operate in HA mode if one or more FortiGate interfaces is configured as a PPTP or L2TP client or if the unit is configured for standalone session synchronization.

### High Availability page

Lists the existing settings for a configured HA cluster as well as allows you to configure a HA cluster if not already configured. You can also modify existing settings from this page as well.

**Mode**

Select an HA mode for the cluster or return the 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 unit in a cluster 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 different 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**

Enter a name to identify the cluster. The maximum length of the group name is 32 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, however two clusters on the same network cannot have the same group name. When the cluster is operating you can change the group name, if required.

**Password**

Enter 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 password 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**

Select to enable session pickup so that if the primary unit fails, sessions are picked up by the cluster unit that becomes the new primary unit.

You must enable session pickup for session failover protection. If you do not require session failover protection, leaving session pickup disabled may reduce HA CPU usage and reduce HA heartbeat network bandwidth usage.

Session pickup is disabled by default. You can accept the default setting for session pickup and later choose to enable session pickup after the cluster is operating.
Cluster members list

You can display the cluster members list to view the status of an operating cluster and the status of the units in the cluster. The cluster members list shows the units in the cluster and for each unit shows interface connections, the cluster unit and the device priority of the cluster unit. From the cluster members list you can disconnect a unit from the cluster, edit the HA configuration of primary unit, change the device priority and host name of subordinate units, and download a debug log for any cluster unit. You can also view HA statistics for the cluster.

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 cluster members list, log into an operating cluster and go to System > Config > HA.

To display the virtual cluster members list for an operating cluster log in as the global admin administrator and go to System > Config > HA.

**Cluster Settings section of the HA page**

**View HA Statistics** Displays the serial number, status, and monitor information for each cluster unit. See “Viewing HA statistics” on page 95.
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.

View HA Statistics page
Lists the statistical information for HA. You can select how often the information is refreshed.

Refresh every
Select to control how often the web-based manager updates the HA statistics display.

Back to HA monitor
Select to 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.
## Changing subordinate unit host name and device priority

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.

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.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>View and optionally change the subordinate unit host name.</td>
</tr>
<tr>
<td>Priority</td>
<td>View and optionally change the subordinate unit device priority.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

## Disconnecting a cluster unit from a cluster

You can disconnect a cluster unit if you need to use the disconnected unit for another purpose, such as to act as a standalone firewall. 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.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>Displays the serial number of the cluster unit to be disconnected from the cluster.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface that you want to configure. You also specify the IP address and netmask for this interface. When the FortiGate unit is disconnected, all management access options are enabled for this interface.</td>
</tr>
<tr>
<td>IP/Netmask</td>
<td>Specify an IP address and netmask for the interface. You can use this IP address to connect to this interface to configure the disconnected FortiGate unit.</td>
</tr>
</tbody>
</table>
SNMP

The Simple Network Management Protocol (SNMP) allows you to monitor hardware on your network. You can configure the hardware, such as the FortiGate SNMP agent, to report system information and traps. SNMP traps alert you to events that happen, such as a log disk is full, or a virus was detected.

These traps are sent to the SNMP managers. An SNMP manager (or host) is typically a computer running an application that can read the incoming traps and event messages from the agent and send out SNMP queries to the SNMP agents. A FortiManager unit can act as an SNMP manager to one or more FortiGate units.

When using SNMP, you must also ensure you had added the correct MIB files to the unit, regardless of whether or not your SNMP manager already includes standard and private MIBs in a compiled database, ready to use. An MIB is a text file that describes a list of SNMP data objects used by the SNMP manager. The required files are Fortinet and FortiGate Management Information Base (MIB). The Fortinet MIB contains traps, fields and information that is common to all Fortinet products. The FortiGate MIB contains traps, fields and information that is specific to FortiGate units. Each Fortinet product has its own MIB – if you use other Fortinet products, you need to download their MIB files as well.

The Fortinet and FortiGate Management Information Base (MIB) files are available for download on the Fortinet Customer Support site.

The FortiGate SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiGate system information through queries and can receive trap messages from the unit.

The FortiGate SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Authentication and encryption are configured in the CLI.

**Note:** There were major changes to the MIB files between FortiOS v3.0 and v4.0. You need to use the new MIBs for FortiOS v4.0 or you may be accessing the wrong traps and fields.

SNMP configuration

In `System > Config > SNMP v1/v2c`, you can configure an SNMP agent and an SNMP community. An SNMP agent reports on the system information and traps. The unit, once the SNMP agent is enabled and configured on the SNMP v1/v2c page, acts as an SNMP agent.

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP community and a printer SNMP community.

SNMP communities are added so that SNMP managers can connect 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 unit for a different set of events. You can also add the IP addresses of up to eight SNMP managers to each community.

**Note:** When the unit is in virtual domain mode, SNMP traps can only be sent on interfaces in the management virtual domain. Traps cannot be sent over other interfaces.
Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections. Interfaces are configured in System > Network > Interface.

The following two procedures explain how to configure SNMP access when the unit is in either NAT/Route or Transparent mode.

**To configure SNMP access (NAT/Route mode)**

1. Go to System > Network > Interface.
2. Edit an interface that the SNMP manager will be connecting to.
3. In Administrative Access, select SNMP.
4. Select OK.

**To configure SNMP access (Transparent mode)**

1. Go to System > Config > Operation.
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.

Use the following table when configuring an SNMP agent and its community from System > Config > SNMP v1/2v.

<table>
<thead>
<tr>
<th><strong>SNMP v1/v2c page</strong></th>
<th>Provides settings for configuring the SNMP agent.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMP Agent</strong></td>
<td>Enables the FortiGate SNMP agent.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter descriptive information about the unit. The description can be up to 35 characters long.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Enter the physical location of the unit. The system location description can be up to 35 characters long.</td>
</tr>
<tr>
<td><strong>Contact</strong></td>
<td>Enter the contact information for the person responsible for this unit. The contact information can be up to 35 characters.</td>
</tr>
<tr>
<td><strong>Apply</strong></td>
<td>Saves changes made to the description, location, and contact information.</td>
</tr>
</tbody>
</table>

**Communities section of the page**
The list of SNMP communities added to the FortiGate configuration. You can add up to 3 communities.

<table>
<thead>
<tr>
<th><strong>Create New</strong></th>
<th>Creates a new SNMP community. When you select <strong>Edit</strong></th>
<th>Modifies settings within an SNMP community. When you select Edit, you are automatically redirected to the Edit SNMP Community page.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delete</strong></td>
<td>Removes an SNMP community from within the list.</td>
<td>Removes multiple SNMP communities from within the list, in the Communities section of the page, in each of the rows of communities you want removed, select the check box and then select Delete. To remove all SNMP communities from the list, in the Communities section of the page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The name of the SNMP community.</td>
<td></td>
</tr>
<tr>
<td><strong>Queries</strong></td>
<td>The status of SNMP queries for each SNMP community. The query status can be enabled or disabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Traps</strong></td>
<td>The status of SNMP traps for each SNMP community. The trap status can be enabled or disabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Enable</strong></td>
<td>Enable to activate an SNMP community.</td>
<td></td>
</tr>
</tbody>
</table>
Replacement messages

The unit adds replacement messages to a variety of content streams. For example, if a virus is found in an email message attachment, 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 email filtering.

This topic contains the following:

- Viewing the replacement messages list
- Modifying replacement messages
• Replacement message tags
• Mail replacement messages
• HTTP replacement messages
• Web Proxy replacement messages
• FTP replacement messages
• NNTP replacement messages
• Alert Mail replacement messages
• Spam replacement messages
• Administration replacement message
• User authentication replacement messages
• FortiGuard Web Filtering replacement messages
• IM and P2P replacement messages
• Endpoint NAC replacement messages
• NAC quarantine replacement messages
• Traffic quota control replacement messages
• SSL VPN replacement message

Viewing the replacement messages list

You use the replacement messages list to view and customize replacement messages to
your requirements. The list organizes replacement message into an number of types (for
example, Mail, HTTP, and so on). Use the expand arrow beside each type to display the
replacement messages for that category. Select the Edit icon beside each replacement
message to customize that message for your requirements.

If you are viewing the replacement messages list in a VDOM, any messages that have
been customized for that VDOM are displayed with a Reset icon that you can use to reset
the replacement message to the global version.

To view the replacement messages list, go to System > Config > Replacement Message.

Replacement Messages page

Lists the replacement messages and are grouped by their associated FortiOS feature. For
example, virus message is placed in the Mail group.

Name
The replacement message category. Select the expand arrow to expand or collapse
the category. Each category contains several replacement messages that are used
by different FortiGate features. The replacement messages are described below.

Description
A description of the replacement message.

Edit
Modifies settings within a replacement message. By selecting Edit, you are also
able to view the settings as well.

Reset
Only displayed on the a VDOM replacement message list. Select to revert to the
global version of this replacement message.

Note: FortiOS uses HTTP to send the Authentication Disclaimer page for the user to accept
before the firewall policy is in effect. Therefore, the user must initiate HTTP traffic first in
order to trigger the Authentication Disclaimer page. Once the Disclaimer is accepted, the
user can send whatever traffic is allowed by the firewall policy.
Modifying replacement messages

You can modify the text and HTML code within a replacement message to suite your requirements. Each replacement message contains the row Allowed Formats:, which indicates what type of format the replacement message is in, Text or HTML. For example, the HTTP virus replacement message’s format is HTTP and the Email file block replacement message is Text.

Use the expand arrows to view the replacement message that you want to change. You can change the content of the replacement message by editing the text and HTML codes and by working with replacement message tags. For descriptions of the replacement message tags, see Table 6 on page 101.

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 limit of 8192 characters for each replacement message. The following fields and options are available when editing a replacement message. Different replacement messages have different sets of fields and options.

To change a replacement message list, go to System > Config > Replacement Message and expand the replacement message category to access the replacement message that you want to modify. Use the following table to help you modify replacement messages.

The Replacement Message page of a replacement message

<table>
<thead>
<tr>
<th>Message Setup</th>
<th>The name of the replacement message.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Formats</td>
<td>The type of content that can be included in the replacement message. Allowed formats can be Text or HTML. You should not use HTML code in Text messages. You can include replacement message tags in text and HTML messages.</td>
</tr>
<tr>
<td>Size</td>
<td>The number of characters allowed in the replacement message. Usually size is 8192 characters.</td>
</tr>
<tr>
<td>Message Text</td>
<td>The editable text of the replacement message. The message text can include text, HTML codes (if HTML is the allowed format) and replacement message tags.</td>
</tr>
</tbody>
</table>

Replacement message tags

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. The following table lists the replacement message tags that you can add.

Table 6: 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>
</tbody>
</table>
Mail replacement messages

The unit sends the mail replacement messages listed in the following table to email clients and servers using IMAP, POP3, or SMTP when an event occurs such as antivirus blocking a file attached to an email that contains a virus. Email replacement messages are text messages.

If the unit supports SSL content scanning and inspection these replacement messages can also be added to IMAPS, POP3S, and SMTPS email messages.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>%%LINK%%</td>
<td>The link to the FortiClient Host Security installs download for the Endpoint Control feature.</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>%%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>
<tr>
<td>%%QUARFILENAME%%</td>
<td>The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk.</td>
</tr>
<tr>
<td>%%QUOTA_INFO%%</td>
<td>Display information about the traffic shaping quota setting that is blocking the user. Used in traffic quota control replacement messages.</td>
</tr>
<tr>
<td>%%QUESTION%%</td>
<td>Authentication challenge question on auth-challenge page. Prompt to enter username and password on auth-login page.</td>
</tr>
<tr>
<td>%%SERVICE%%</td>
<td>The name of the web filtering service.</td>
</tr>
<tr>
<td>%%SOURCE_IP%%</td>
<td>The IP address of the request originator who would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed.</td>
</tr>
<tr>
<td>%%TIMEOUT%%</td>
<td>Configured number of seconds between authentication keepalive connections. Used on the auth-keepalive page.</td>
</tr>
<tr>
<td>%%URL%%</td>
<td>The URL of a web page. This can be a web page that is blocked by web filter content or URL blocking. %%URL%% can also be used in http virus and file block messages to be the URL of the web page from which a user attempted to download a file that is blocked.</td>
</tr>
<tr>
<td>%%VIRUS%%</td>
<td>The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages</td>
</tr>
</tbody>
</table>
HTTP replacement messages

The unit sends the HTTP replacement messages listed in the following table to web browsers using the HTTP protocol when an event occurs such as antivirus blocking a file that contains a virus in an HTTP session. HTTP replacement messages are HTML pages.

If the unit supports SSL content scanning and inspection, and if under HTTPS in the protocol option list has Enable Deep Scan enabled, these replacement messages can also replace web pages downloaded using the HTTPS protocol.
Table 8: HTTP replacement messages

<table>
<thead>
<tr>
<th>Replacement Message name</th>
<th>Description of how a replacement message is triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus message</td>
<td>If Virus Scan is enabled for HTTP or HTTPS in an antivirus profile, the FortiGate unit blocks a file being downloaded that uses a HTTP GET which matches an entry in the selected file filter list. It is then replaced with this web page that the client's browser displays.</td>
</tr>
<tr>
<td>Infection cache message</td>
<td>This message is triggered only after the blocked URL is attempted for a second time. A web filter profile that has client comforting enabled helps to trigger this message.</td>
</tr>
<tr>
<td>File block message</td>
<td>If File Filter is enabled for HTTP or HTTPS in an antivirus profile, the FortiGate unit blocks a file being downloaded that uses a HTTP GET which matches an entry in the selected file filter list. It is then replaced with this web page that the client's browser displays.</td>
</tr>
<tr>
<td>Oversized file message</td>
<td>If Oversized File/Email set to Block for HTTP or HTTPS in a protocol options list, the FortiGate unit blocks an oversized file that is being downloaded that uses a HTTP GET and replaces the file with this web page that is displayed by the client browser.</td>
</tr>
<tr>
<td>Data leak prevention message</td>
<td>In a DLP sensor, a rule with action set to Block loads using HTTP GET with this web page. It can also block the user sending information that uses HTTP POST.</td>
</tr>
<tr>
<td>Banned by data leak prevention message</td>
<td>In a DLP sensor, a rule with action set to Ban replaces a blocked web page or file with this web page. This web page also replaces any additional web pages or files that the banned user attempts to access until the user is removed from the banned user list.</td>
</tr>
<tr>
<td>Banned word message</td>
<td>If the banned word’s score exceeds the threshold set in the web filter profile, the page is blocked and the blocked page is replaced with this web page.</td>
</tr>
<tr>
<td>Content-type block message</td>
<td>Email headers include information about content types such as image for pictures, and so on. If a specific content-type is blocked, the blocked message is replaced with this web page.</td>
</tr>
<tr>
<td>URL block message</td>
<td>If Web URL filtering is enabled in a web filter profile, and if a match is detected, a web page with a URL is blocked. The blocked page is replaced with this web page.</td>
</tr>
<tr>
<td>Client block</td>
<td>If File Filter is enabled for HTTP or HTTPS in an antivirus profile, and if a match is detected, a file being uploaded by an HTTP POST is blocked and is replaced with this web page that is displayed by the client browser.</td>
</tr>
<tr>
<td>Client anti-virus</td>
<td>If Virus Scan is enabled for HTTP or HTTPS in an antivirus profile, the infected file that is being uploaded using FTP PUT is replaced with this a web page that is displayed by the client browser.</td>
</tr>
<tr>
<td>Client filesize</td>
<td>If Oversized File/Email is set to Block for HTTP or HTTPS in a protocol options list, and an oversized file is being uploaded using FTP PUT, the file is blocked and replaced with this web page.</td>
</tr>
<tr>
<td>Client banned word</td>
<td>If Web content filtering is enabled in a web filter profile, and if a match is detected, blocks a web page being uploaded with an HTTP PUT that contains content that matches an entry in the selected Web Content Filter list. The client browser displays this web page.</td>
</tr>
<tr>
<td>POST block</td>
<td>HTTP POST Action is set to Block in an profile and the FortiGate unit blocks an HTTP POST and displays this web page.</td>
</tr>
</tbody>
</table>

Web Proxy replacement messages

The unit sends Web Proxy replacement messages listed in the following table when a web proxy event occurs that is detected and matches the web proxy configuration. These replacement messages are web pages that appear within your web browser.
The following web proxy replacement messages require an identity-based firewall policy so that the web proxy is successful. You can also enable FTP-over-HTTP by selecting the FTP option in System > Network > Web Proxy.

Table 9: Web Proxy replacement messages

<table>
<thead>
<tr>
<th>Replacement Message name</th>
<th>Description of how a replacement message is triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web proxy access denied</td>
<td>If no web proxy policy is defined, and the default action is set to Deny, this message displays. This message also displays when both of the following are true: OR no existing policy matches the incoming request OR the user is denied by an access control list. Note: The default action is ignored when there is at least one web policy defined.</td>
</tr>
<tr>
<td>Web proxy login challenge</td>
<td>If a user name and password authentication combination is entered, and is accepted as incorrect, this replacement message appears.</td>
</tr>
<tr>
<td>Web proxy login fail</td>
<td>If a user name and password authentication combination is entered, and is accepted as incorrect, this replacement message appears.</td>
</tr>
<tr>
<td>Web proxy authorization fail</td>
<td>If a username and password is entered and is correct, this replacement message appears. However, if the following is true, this replacement message also appears: The user is not allowed to view the request resources, (for example in an FSAE setup and the authentication passes), and the username and password combo is correct, but the user group does not match a user group defined in the firewall policy.</td>
</tr>
<tr>
<td>Web proxy HTTP error</td>
<td>This replacement message is triggered whenever there is a web proxy HTTP error. This message forwards the actual servers’ error message and a web proxy internal error message, for example, error 404: web page is not found.</td>
</tr>
<tr>
<td>Web proxy user-limit (CLI only)</td>
<td>If you have enabled user-limit within config system replacemsg webproxy, this message is triggered when a web proxy user has met the threshold that is defined in global resources or vdom resources.</td>
</tr>
</tbody>
</table>

FTP replacement messages

The unit sends the FTP replacement messages listed in the following table to FTP clients when an event occurs such as antivirus blocking a file that contains a virus in an FTP session. FTP replacement messages are text messages.

Table 10: FTP replacement messages

<table>
<thead>
<tr>
<th>Replacement Message name</th>
<th>Description of how a replacement message is triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus message</td>
<td>If Virus Scan is enabled for FTP in an antivirus profile, and if a match is detected, the infected file is deleted when being downloaded using FTP and sends this message to the FTP client.</td>
</tr>
<tr>
<td>Blocked message</td>
<td>If File Filter is enabled for FTP in an antivirus profile, and if a match is detected, a file being downloaded using FTP is blocked and sends this message to the FTP client.</td>
</tr>
<tr>
<td>Oversized message</td>
<td>If Oversized File/Email is set to Block for FTP in an antivirus profile, and if a match is detected, an oversized file that is being downloaded using FTP is blocked, and sends this message to the FTP client.</td>
</tr>
<tr>
<td>DLP message</td>
<td>In a DLP sensor, a rule with action set to Block replaces a blocked FTP download with this message.</td>
</tr>
<tr>
<td>DLP ban message</td>
<td>In a DLP sensor, a rule with action set to Ban blocks an FTP session if a match is detected, that uses protocols such as FTP PUT and FTP GET, displays this message. This message is displayed whenever the banned user attempts to access until the user is removed from the banned user list.</td>
</tr>
</tbody>
</table>
NNTP replacement messages

The unit sends the NNTP replacement messages listed in the following table to NNTP clients when an event occurs such as antivirus blocking a file attached to an NNTP message that contains a virus. NNTP replacement messages are text messages.

Table 11: NNTP replacement messages

<table>
<thead>
<tr>
<th>Replacement Message name</th>
<th>Description of how a replacement message is triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus message</td>
<td>If Virus Scan is enabled for NNTP in an antivirus profile, and if a match is detected, an infected file attached to an NNTP message is deleted and sends this message to the client.</td>
</tr>
<tr>
<td>Blocked message</td>
<td>If File Filter is enabled for NNTP in an antivirus profile, and if a match is detected, a file attached to an NNTP message is blocked and sends this message to the client.</td>
</tr>
<tr>
<td>Oversized message</td>
<td>If Oversized File/Email set to Block for NNTP in a protocol options list, and if a match is detected, removes an oversized file from an NNTP message and replaces the file with this message.</td>
</tr>
<tr>
<td>Data Leak prevention message</td>
<td>In a DLP sensor, a rule with action set to Block replaces a blocked NNTP message with this message.</td>
</tr>
<tr>
<td>Subject of data leak prevention message</td>
<td>If the DLP sensor contains Block, Ban, Quarantine IP address, and Quarantine interface actions, and if a match is detected, this message is then added to the subject field of all NNTP messages.</td>
</tr>
<tr>
<td>Banned by data leak prevention message</td>
<td>In a DLP sensor, a rule with the action set to Ban, replaces a blocked NNTP message with this message when a match is detected. This message also replaces any additional NNTP messages that the banned user sends until they are removed from the banned user list.</td>
</tr>
</tbody>
</table>

Alert Mail replacement messages

The unit adds the alert mail replacement messages listed in the following table to alert email messages sent to administrators.

Table 12: Alert mail replacement messages

<table>
<thead>
<tr>
<th>Replacement Message name</th>
<th>Description of how a replacement message is triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus message</td>
<td>If Virus detected is enabled for alert email message, the Virus Scan must be enabled in an antivirus profile as well; if a match is detected with both enabled, this message displays.</td>
</tr>
<tr>
<td>Block message</td>
<td>If Virus detected is enabled for alert email message, the File Filter must be enabled in an antivirus profile as well; if a match is detected with both enabled, a file is blocked.</td>
</tr>
<tr>
<td>Intrusion message</td>
<td>If Intrusion detected is enabled for alert email message, an IPS Sensor or a DoS Sensor must also be enabled as well; if a match is detects, including an attack, this message displays.</td>
</tr>
<tr>
<td>Critical event message</td>
<td>Whenever a critical level event log message is generated, this replacement message is sent; however, unless you configure an alert email message with enable Send alert email for logs based on severity and set the Minimum log level to Alert or Emergency this is message does not appear.</td>
</tr>
<tr>
<td>Disk full message</td>
<td>If Disk usage is enabled for an alert email message, and if disk usage reaches the % configured for alert email, this message displays.</td>
</tr>
<tr>
<td></td>
<td>If you enable Send alert email for logs based on severity for alert email, whether or not replacement messages are sent by alert email depends on how you set the alert email Minimum log level.</td>
</tr>
</tbody>
</table>
Spam replacement messages

The unit adds the Spam replacement messages listed in the following table to SMTP server responses if the email message is identified as spam and the spam action is discard. If the unit supports SSL content scanning and inspection these replacement messages can also be added to SMTPS server responses.

Table 13: Spam replacement messages

<table>
<thead>
<tr>
<th>Replacement Message name</th>
<th>Description of how a replacement message is triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email IP</td>
<td>If IP address BWL check is enabled for an email protocol in an email filter profile, and if a match is detected to the last hop IP address, then this replacement message is added.</td>
</tr>
<tr>
<td>DNSBL/ORDBL</td>
<td>If spamrbl is enabled in the CLI for an email protocol in an email filter profile, and if a match is detected and identified as spam, this replacement message is added.</td>
</tr>
<tr>
<td>HELO/EHLO domain</td>
<td>If HELO DNS lookup is enabled for an email protocol within an email filter profile and if a match is detected, an email message is identified as spam and adds this replacement message. HELO DNS lookup is not available for SMTPS.</td>
</tr>
<tr>
<td>Email address</td>
<td>If E-mail Address BWL check is enabled for an email protocol in an email filter profile and if a match is detected and identifies an email message as spam and adds this replacement message.</td>
</tr>
<tr>
<td>Mime header</td>
<td>If spamhdrcheck is enabled in the CLI for an email protocol within an email filter profile, and if a match is detected and identified as spam, this replacement message is added.</td>
</tr>
<tr>
<td>Returned email domain</td>
<td>If Return e-mail DNS check is enabled for an email protocol in an email filter profile, and if a match is detected and identified as spam, this replacement message is added.</td>
</tr>
<tr>
<td>Banned word</td>
<td>If Banned word check is enabled for an email protocol in an email filter profile, and if a match is detected and identified as spam, this replacement message is added.</td>
</tr>
<tr>
<td>Spam submission message</td>
<td>Any Email Filtering option enabled for an email protocol in an email filter profile identifies an email message as spam and adds this replacement message. Email Filtering adds this message to all email tagged as spam. The message describes a button that the recipient of the message can select to submit the email signatures to the FortiGuard Antispam service if the email was incorrectly tagged as spam (a false positive).</td>
</tr>
</tbody>
</table>

Administration replacement message

If you enter the following CLI command the unit displays the Administration Login disclaimer whenever an administrator logs into the unit's web-based manager or CLI.

```
config system global
set access-banner enable
end
```

The web-based manager administrator login disclaimer contains the text of the Login Disclaimer replacement message as well as Accept and Decline buttons. The administrator must select accept to login.

User authentication replacement messages

The unit uses the text of the authentication replacement messages listed in Table 14 on page 109 for various user authentication HTML pages that are displayed when a user is required to authenticate because a firewall policy includes at least one identity-based policy that requires firewall users to authenticate.
These replacement message pages are for authentication using HTTP and HTTPS. Authentication replacement messages are HTML messages. You cannot customize the firewall authentication messages for FTP and Telnet.

The authentication login page and the authentication disclaimer include replacement tags and controls not found on other replacement messages.

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.

There are some unique requirements for these replacement messages:

- 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><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">
<TABLE ALIGN="center" BGCOLOR="#00cccc" BORDER="0" CELLPADDING="15" CELLSPACING="0" WIDTH="320"><TBODY>
<TR><TH>Username:</TH><TD><INPUT NAME="%%USERNAMEID%%" SIZE="25" TYPE="text"> </TD></TR>
<TR><TH>Password:</TH><TD><INPUT NAME="%%PASSWORDID%%" SIZE="25" TYPE="password"> </TD></TR>
<TR><TD COLSPAN="2" ALIGN="center" BGCOLOR="#00cccc"> <INPUT NAME="%%STATEID%%" VALUE="%%STATEVAL%%" TYPE="hidden"> <INPUT NAME="%%REDIRID%%" VALUE="%%PROTURI%%" TYPE="hidden"> <INPUT VALUE="Continue" TYPE="submit"> </TD></TR>
</TBODY></TABLE></FORM></BODY></HTML>
```
The FortiGate unit sends the FortiGuard Web Filtering replacement messages listed in the following table to web browsers using the HTTP protocol when FortiGuard web filtering blocks a URL, provides details about blocked HTTP 4xx and 5xx errors, and for FortiGuard overrides. FortiGuard Web Filtering replacement messages are HTTP pages.

If the FortiGate unit supports SSL content scanning and inspection and if Protocol Recognition > HTTPS Content Filtering Mode is set to Deep Scan in the antivirus profile, these replacement messages can also replace web pages downloaded using the HTTPS protocol.

### Table 14: Authentication replacement messages

<table>
<thead>
<tr>
<th>Replacement Message name</th>
<th>Description of how a replacement message is triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclaimer page</td>
<td>If Enable Disclaimer and Redirect URL to (within Enable Identity Based Policy in a firewall policy) is selected in a firewall policy, and if a match is detected, after a firewall user authenticates with the FortiGate unit using HTTP or HTTPS, this disclaimer page displays. The CLI includes auth-disclaimer-page-1, auth-disclaimer-page-2, and auth-disclaimer-page-3 that you can use to increase the size of the authentication disclaimer page replacement message.</td>
</tr>
<tr>
<td>Declined disclaimer page</td>
<td>When a firewall user selects the button on the Disclaimer page to decline access through the FortiGate unit, the Declined disclaimer page is displayed.</td>
</tr>
<tr>
<td>Login page</td>
<td>The HTML page displayed for firewall users who are required to authenticate using HTTP or HTTPS before connecting through the FortiGate unit.</td>
</tr>
<tr>
<td>Login failed page</td>
<td>The HTML page displayed if firewall users enter an incorrect user name and password combination.</td>
</tr>
<tr>
<td>Login challenge page</td>
<td>The HTML page displayed if firewall users are required to answer a question to complete authentication. The page displays the question and includes a field in which to type the answer. This feature is supported by RADIUS and uses the generic RADIUS challenge-access auth response. Usually, challenge-access responses contain a Reply-Message attribute that contains a message for the user (for example, “Please enter new PIN”). This message is displayed on the login challenge page. The user enters a response that is sent back to the RADIUS server to be verified. The Login challenge page is most often used with RSA RADIUS server for RSA SecurID authentication. The login challenge appears when the server needs the user to enter a new PIN. You can customize the replacement message to ask the user for a SecurID PIN.</td>
</tr>
</tbody>
</table>
| Keepalive page           | The HTML page displayed with firewall authentication keepalive is enabled using the following command:  
```
config system global
  set auth-keepalive enable
end
```
  
  Authentication keepalive keeps authenticated firewall sessions from ending when the authentication timeout ends. Go to User > Options to set the Authentication Timeout. |
### IM and P2P replacement messages

The FortiGate unit sends the IM and P2P replacement messages listed in Table 16 to IM and P2P clients using AIM, ICQ, MSN, or Yahoo! Messenger when an event occurs such as antivirus blocking a file attached to an email that contains a virus. IM and P2P replacement messages are text messages.

#### Table 15: FortiGuard Web Filtering replacement messages

<table>
<thead>
<tr>
<th>Replacement Message name</th>
<th>Description of how a replacement message is triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL block message</td>
<td>If FortiGuard Web Filtering is enabled in a web filter profile for HTTP or HTTPS, and if a match is detected, a web page is blocked and that blocked web page is replaced with this web page.</td>
</tr>
<tr>
<td>HTTP error message</td>
<td>If Provide details for blocked HTTP 4xx and 5xx errors is enabled in a web filter profile for HTTP or HTTPS, and if a match is detected, a web page is blocked. The blocked page is replaced with this web page.</td>
</tr>
<tr>
<td>FortiGuard Web Filtering override form</td>
<td>If Allow Override is selected for a FortiGuard Web Filtering category, and a match is detected, and FortiGuard Web Filtering blocks a web page in this category, this message displays a web page. Using this web page users can authenticate to get access to the page. Go to UTM &gt; Web Filter &gt; Override to add override rules. For more information, see “Administrative overrides” on page 268. 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.</td>
</tr>
<tr>
<td>FortiGuard Web Filtering quota expired message</td>
<td>If FortiGuard Quota is enabled within a web filter profile, and if a match is detected, this message is added.</td>
</tr>
</tbody>
</table>

#### Table 16: IM and P2P replacement messages

<table>
<thead>
<tr>
<th>Replacement Message name</th>
<th>Description of how a replacement message is triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>File block message</td>
<td>If File Filter is enabled for IM in an application control list deletes a file that matches an entry in the selected file filter list and replaces it with this message.</td>
</tr>
<tr>
<td>File name block message</td>
<td>Antivirus File Filter enabled for IM in an application control list deletes a file with a name that matches an entry in the selected file filter list and replaces it with this message.</td>
</tr>
<tr>
<td>Virus message</td>
<td>If Virus Scan is enabled for IM in an application control list deletes a infected file from and replaces the file with this message.</td>
</tr>
<tr>
<td>Oversized file message</td>
<td>If Oversized File/Email set to Block for IM in a protocol options list, and if a match is detected, an oversized file is removed and replaced with this message.</td>
</tr>
<tr>
<td>Data leak prevention message</td>
<td>In a DLP sensor, a rule with action set to Block replaces a blocked IM or P2P message with this message.</td>
</tr>
<tr>
<td>Banned by data leak prevention message</td>
<td>In a DLP sensor, a rule with action set to Ban replaces a blocked IM or P2P message with this message. This message also replaces any additional messages that the banned user sends until they are removed from the banned user list.</td>
</tr>
<tr>
<td>Voice chat block message</td>
<td>In an application control list, the Block Audio option is selected for AIM, ICQ, MSN, or Yahoo! and the application control list is applied to a firewall policy.</td>
</tr>
<tr>
<td>Photo share block message</td>
<td>In an application control list, the block-photo CLI keyword is enabled for MSN, or Yahoo and the application control list is applied to a firewall policy. You enable photo blocking from the CLI.</td>
</tr>
</tbody>
</table>
Endpoint NAC replacement messages

The FortiGate unit sends one of the following pages to non-compliant users who attempt to use a firewall policy in which Endpoint NAC is enabled:

- **Endpoint NAC Download Portal** — The FortiGate unit sends this page if the Endpoint NAC profile has the *Quarantine Hosts to User Portal (Enforce compliance)* option selected. The user can download the FortiClient Endpoint Security application installer. If you modify this replacement message, be sure to retain the `%%LINK%%` tag which provides the download URL for the FortiClient installer.

- **Endpoint NAC Recommendation Portal** — The FortiGate unit sends this page if the Endpoint NAC profile has the *Notify Hosts to Install FortiClient (Warn only)* option selected. The user can either download the FortiClient Endpoint Security application installer or select the *Continue to* link to access their desired destination. If you modify this replacement message, be sure to retain both the `%%LINK%%` tag which provides the download URL for the FortiClient installer and the `%DST_ADDR%%` link that contains the URL that the user requested.

To modify these messages, go to *System > Config > Replacement Messages*. Expand *Endpoint NAC* and edit the Endpoint NAC replacement message that you want to modify.

NAC quarantine replacement messages

The page that is displayed for the user depends on whether NAC quarantine blocked the user because a virus was found, a DoS sensor detected an attack, an IPS sensor detected an attack, or a DLP rule with action set to *Quarantine IP address* or *Quarantine Interface* matched a session from the user.

The default messages inform the user of why they are seeing this page and recommend they contact the system administrator. You can customize the pages as required, for example to include an email address or other contact information or if applicable a note about how long the user can expect to be blocked.

Table 17: NAC quarantine replacement messages

<table>
<thead>
<tr>
<th>Replacement Message name</th>
<th>Description of how a replacement message is triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus Message</td>
<td>If <em>Quarantine Virus Sender</em> is enabled in an antivirus profile adds a source IP address or FortiGate interface to the banned user list. The FortiGate unit displays this replacement message as a web page when the blocked user attempts to connect through the FortiGate unit using HTTP on port 80 or when any user attempts to connect through a FortiGate interface added to the banned user list using HTTP on port 80.</td>
</tr>
<tr>
<td>DoS Message</td>
<td>For a DoS Sensor the CLI <em>quarantine</em> option set to <em>attacker</em> or <em>interface</em> and the DoS Sensor added to a DoS firewall policy adds a source IP, a destination IP, or FortiGate interface to the banned user list. The FortiGate unit displays this replacement message as a web page when the blocked user attempts to connect through the FortiGate unit using HTTP on port 80 or when any user attempts to connect through a FortiGate interface added to the banned user list using HTTP on port 80. This replacement message is not displayed if <em>quarantine</em> is set to <em>both</em>.</td>
</tr>
</tbody>
</table>
Traffic quota control replacement messages

When user traffic is going through the FortiGate unit and it is blocked by traffic shaping quota controls, users see the Traffic shaper block message or the Per IP traffic shaper block message when they attempt to connect through the FortiGate unit using HTTP.

The traffic quota HTTP pages should contain the %%QUOTA_INFO%% tag to display information about the traffic shaping quota setting that is blocking the user.

SSL VPN replacement message

The SSL VPN login replacement message is an HTML replacement message that formats the FortiGate SSL VPN portal login page. You can customize this replacement message according to your organization’s needs. 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.

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 unit’s VDOMs.

Management access to a VDOM can be restricted based on which interfaces and protocols can be used to connect to the unit.

This topic contains the following:

- Changing the operation mode
- Management access

Changing the 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.
There are two operation modes for the unit - NAT/Route and Transparent. Each mode is well suited to different situations.

**To switch from NAT/Route to Transparent mode**

1. Go to System > Config > Operation.
   
   You can also select Change in the Operation Mode row of the System Information widget. When you select Change, you are automatically redirected to the Operation page.

2. From the Operation Mode drop-down 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 unit.
   
   - **Default Gateway**: Enter the default gateway required to reach other networks from the unit.

**To switch from Transparent to NAT/Route mode**

1. Go to System > Config > Operation.
   
   You can also select Change in the Operation Mode row of the System Information widget. When you select Change, you are automatically redirected to the Operation page.

2. From the Operation Mode drop-down 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 unit.
   
   - **Device**: Select the interface to which the Interface IP/Netmask settings apply.
   
   - **Default Gateway**: Enter the default gateway required to reach other networks from the unit.
   
   - **Gateway Device**: Select the interface to which the default gateway is connected.

**Management access**

Management access defines how administrators are able to log on to the unit to perform management tasks such as configuration and maintenance. Methods of access can include local access through the console connection, or remote access over a network or modem interface using various protocols including Telnet and HTTPS.

You can configure management access on any interface in your VDOM. 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 unit also uses this IP address to connect to the FDN for virus and attack updates.

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 unit. However, allowing remote administration from the Internet could compromise the security of the unit. You should avoid this unless it is required for your configuration. To improve the security of a 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.

Admin

The Admin menu provides settings for configuring administrators and their profiles, as well as central management, and basic administrative settings such as changing the default language.

You may want to review the User Authentication chapter of the FortiOS Handbook if you are configuring authentication for administrators because the chapter contains detailed information about remote servers, such as LDAP and RADIUS.

If you are enabling IPv6 on the unit, Fortinet recommends reviewing the FortiGate Fundamentals chapter of the FortiOS Handbook. This chapter contains detailed information about IPv6. FortiGate units support IPv6-over-IPv4 tunneling.

This topic contains the following:

- Administrators
- Admin profiles
- Central Management
- Settings

Note: Always end your FortiGate session by logging out, regardless of whether you are in the CLI or the web-based manager. If you do not log out, the session remains open.

Administrators

Administrators are configured in System > Admin > Administrators. There is already a default administrator account on the unit, the super_admin, which has read and write access. You can configure different administrators to have different access profiles, such as read-only access where the administrator can only view the configuration.

There are two levels of administrator accounts to choose from, regular administrators and system administrators. Regular administrators are administrators with any admin profile other than the default super_admin. System administrators are administrators that have assigned the super_admin profile or super_admin_readonly profile, as well as the default super_admin.

When you are configuring administrators, you are actually configuring accounts. An administrator account comprises of an administrator’s basic settings as well as their access profile. The access profile is a set of allowed and blocked access to various parts of the unit, such as only able to view the UTM features, but able to configure logging and reporting settings.
When you are configuring an administrator’s password, it is important to consider the length as well as what characters are used. By default, admin has no password. The password should be 32 characters or less. The password of users with the super_admin admin profile can be reset in the CLI. If the password of a user who is logged in is changed, the user will be automatically logged out and prompted to re-authenticate with the new password. For example, the user ITAdmin with the admin profile super_admin, to set that user’s password to 123456:

```plaintext
config sys admin
  edit ITAdmin
    set password 123456
  end
```

In another example, the user ITAdmin with the admin profile super_admin, to reset the password from 123456 to the default 'empty':

```plaintext
config sys admin
  edit ITAdmin
    unset password 123456
  end
```

You can authenticate an administrator by using a password stored on the unit, a remote authentication server (such as LDAP, RADIUS, or TACACS+), or by using PKI certificate-based authentication. To authenticate an administrator with an LDAP or TACACS+ server, you must add the server to an authentication list, include the server in a user group, and associate the administrator with the user group. The RADIUS server authenticates users and authorizes access to internal network resources based on the admin profile of the user. Users authenticated with the PKI-based certificate are permitted access to internal network resources based on the user group they belong to and the associated admin profile.

**Administrator configuration**

You need to use the default "admin" account, an account with the super_admin admin profile, or an administrator with read-write access control to add new administrator accounts and control their permission levels. If you log in with an administrator account that does not have the super_admin admin profile, the administrators list will show only the administrators for the current virtual domain.

> Note: Access to the unit depends on the VDOM associated with the administrator account.

Configure administrators in System > Admin > Administrators using the following table.

<table>
<thead>
<tr>
<th><strong>Administrators page</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lists the default super_admin administrator account and all administrator accounts that you created.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Create New</strong></td>
<td>Creates a new administrator account. When you select Create New, you are automatically redirected to the New Administrator page.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The login name for an administrator account.</td>
</tr>
<tr>
<td><strong>Trusted Hosts</strong></td>
<td>The IP address and netmask of trusted hosts from which the administrator can log in.</td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td>The admin profile for the administrator.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>The type of authentication for this administrator, one of:</td>
</tr>
<tr>
<td><strong>Local</strong></td>
<td>Authentication of an account with a local password stored on the FortiGate unit.</td>
</tr>
</tbody>
</table>
Remote Authentication of a specific account on a RADIUS, LDAP, or TACACS+ server.

Remote+Wildcard Authentication of any account on an LDAP, RADIUS, or TACACS+ server.

PKI PKI-based certificate authentication of an account.

Delete Removes an administrator account from the list on the page.

You cannot delete the original “admin” account until you create another user with the super_admin profile, log out of the “admin” account, and log in with the alternate user that has the super_admin profile.

To remove multiple administrator accounts from within the list, on the Administrator page, in each of the rows of accounts you want removed, select the check box and then select Delete.

To remove all administrator accounts from within the list, on the Administrator page, select the check box in the check box column and then select Delete.

Edit Modifies settings within an administrator’s account. When you select Edit, you are automatically redirected to the Edit Administrator page.

Change Password Changes the password for the administrator account.

New Administrator page

Provides settings for configuring an administrator account. When you are configuring an administrator account, you can enable authentication for an admin from an LDAP, RADIUS or local server.

Administrator Enter the login name for the administrator account.

The name of the administrator should not contain the characters <>()#"'. Using these characters in the administrator account name can result in a cross site scripting (XSS) vulnerability.

Type Select the type of administrator account:

Regular Select to create a Local administrator account. For more information, see “Configuring regular (password) authentication for administrators” on page 117.

Remote Select to authenticate the administrator using a RADIUS, LDAP, or TACACS+ server. Server authentication for administrators must be configured first. For more information, see “Configuring RADIUS authentication for administrators” on page 117.

PKI Select to enable certificate-based authentication for the administrator. Only one administrator can be logged in with PKI authentication enabled. For more information, see “Configuring PKI certificate authentication for administrators” on page 118.

User Group Select the administrator user group that includes the Remote server/PKI (peer) users as members of the User Group. The administrator user group cannot be deleted once the group is selected for authentication.

This is available only if Type is Remote or PKI.

Wildcard Select to allow all accounts on the RADIUS, LDAP, or TACACS+ server to be administrators.

This is available only if Type is Remote. Only one wildcard user is permitted per VDOM.

Password Enter a password for the administrator account. For improved security, the password should be at least 6 characters long.

This is not available if Wildcard is selected or when Type is PKI.

For more information see the Fortinet Knowledge Base article Recovering lost administrator account passwords if you forget or lose an administrator account password and cannot log in to your FortiGate unit.

Confirm Password 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 or when PKI authentication is selected.
Configuring regular (password) authentication for administrators

You can use a password stored on the local unit to authenticate an administrator. When you select Regular for Type, you will see Local as the entry in the Type column when you view the list of administrators.

To configure a regular password authentication for administrators, go to System > Admin > Administrators, select Create New, and use the Administrators page table to configure the settings.

Note: If you forget or lose an administrator account password and cannot log in to your unit, see the Fortinet Knowledge Base article Recovering a lost FortiGate administrator account passwords.

Configuring RADIUS authentication for administrators

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. FortiGate units use the authentication and authorization functions of the RADIUS server. To use the RADIUS server for authentication, you must configure the server before you configure the FortiGate users or user groups that will need it.

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 FortiGate unit refuses the connection.

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 the RADIUS user group
• configure an administrator to authenticate with a RADIUS server.

To configure RADIUS authentication for administrators, go to System > Admin > Administrators, select Create New, and then use the Administrators page table to configure the RADIUS authentication settings.

Configuring LDAP authentication for administrators

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, printers, etc.
If you have configured LDAP support and an administrator is required to authenticate using an LDAP server, the FortiGate unit contacts the LDAP server for authentication. If the LDAP server cannot authenticate the administrator, the FortiGate unit refuses the connection.

If you want to use an LDAP 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 an LDAP server
- create an LDAP user group
- configure an administrator to authenticate with an LDAP server.

To view the LDAP server list, go to User > Remote > LDAP.

To configure LDAP authentication for administrators, go to System > Admin > Administrators, select Create New, and then use the Administrators page table to configure the LDAP authentication settings.

### Configuring TACACS+ authentication for administrators

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers.

If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiGate unit contacts the TACACS+ server for authentication. If the TACACS+ server cannot authenticate the administrator, the connection is refused by the FortiGate unit.

If you want to use an TACACS+ 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 TACACS+ server
- create a TACACS+ user group
- configure an administrator to authenticate with a TACACS+ server.

To configure TACACS+ authentication for administrators, go to System > Admin > Administrators, select Create New, and then use the Administrators page table to configure the TACACS+ authentication settings.

### Configuring PKI certificate authentication for administrators

Public Key Infrastructure (PKI) authentication uses a certificate authentication library that takes a list of peers, peer groups, and user groups and returns authentication successful or denied notifications. Users only need a valid certificate for successful authentication; no username or password is necessary.

To use PKI authentication for an administrator, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure a PKI user
- create a PKI user group
- configure an administrator to authenticate with a PKI certificate.

To configure PKI authentication for administrators, go to System > Admin > Administrators, select Create New, and then use the Administrators page table to configure the PKI authentication settings.
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 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 0.0.0.0/0.0.0.0 for IPv4, or ::/0 for IPv6. If you set one of the zero addresses to a non-zero address, the other zero addresses will be ignored. The only way to use a wildcard entry is to leave the trusted hosts at 0.0.0.0/0.0.0.0 or ::0. However, this configuration is less secure.

Admin profiles

Each administrator account belongs to an admin profile. The admin profile separates FortiGate features into access control categories for which an administrator with read/write access can enable none (deny), read only, or read/write access.

Read-only access for a web-based manager page enables the administrator to view that page. However, the administrator needs write access to change the settings on the page. You can 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 virtual IP (VIP) configurations.

The admin 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 Only access. Access to “config” commands requires Read-Write access.

<table>
<thead>
<tr>
<th>Access Control Category</th>
<th>Command Types Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Only</td>
<td>get, show</td>
</tr>
<tr>
<td>Read-Write</td>
<td>config</td>
</tr>
</tbody>
</table>

Each administrator account belongs to an admin profile. An administrator with read/write access can create admin 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.

Admin profile configuration

You need to use the admin account or an account with read/write access to create or edit admin profiles.

Configure admin profiles in System > Admin > Admin Profile using the following table.
Central Management

The Central Management menu provides the option of remotely managing your FortiGate unit by a FortiManager unit.

From System > Admin > Central Management, you can configure your FortiGate unit to back up or restore configuration settings automatically to the specified central management server. The central management server is the type of service you enable, either a FortiManager unit or the FortiGuard Analysis and Management Service. If you have a subscription for FortiGuard Analysis and Management Service, you can also remotely upgrade the firmware on the FortiGate unit.

When configuring central management settings, you can also specify the source IP address of the self-originated traffic; however, it is available only in the CLI (set fmg-source-ip).

When you are configuring your FortiGate unit to connect to and communicate with a FortiManager unit, the following steps must be taken because of the two different deployment scenarios.

- FortiGate is directly reachable from FortiManager:
  - In the FortiManager GUI, add the FortiGate unit to the FortiManager database in the Device Manager module
  - Change the FortiManager IP address
  - Change the FortiGate IP address

Admin Profile page

Lists all administration profiles that you created as well as the default admin profiles. On this page, you can edit, delete or create a new admin profile. You can edit an existing admin profile, either a default admin profile or one that you created.

Create New: Creates a new profile. When you select Create New, you are automatically redirected to the New Admin Profile page.

Profile Name: The name of the admin profile.

Delete: Removes the admin profile from the list on the page.

You cannot delete an admin profile that has administrators assigned to it.

To remove multiple admin profiles from within the list, on the Admin Profile page, in each of the rows of profiles you want removed, select the check box and then select Delete.

To remove all admin profiles from the list, on the Admin Profile page, select the check box in the check box column and then select Delete.

Edit: Modifies settings within an admin profile. When you select Edit, you are automatically redirected to the Edit Admin Profile page.

New Admin Profile page

Provides settings for configuring an administration profile. When you are editing an existing admin profile, you are automatically redirected to the Edit Admin Profile page.

Profile Name: Enter the name of the admin profile.

Access Control: List of the items that can customize access control settings if configured.

None: Deny access to all Access Control categories.

Read Only: Enable Read access in all Access Control categories.

Read-Write: Select to allow read/write access in all Access Control categories.

Access Control (categories): Make specific control selections as required.
• FortiGate behind NAT
  • In System > Admin > Central Management, choose FortiManager
  • Add the FortiManager unit to the Trusted FortiManager List, if applicable
  • Change the FortiManager IP address
  • Change the FortiGate IP address
  • Contact the FortiManager administrator to verify the FortiGate unit displays in the Device list in the Device Manager module

Central Management page
Provides the settings for configuring central management options, as well as enabling or disabling the service on the FortiGate unit.

<table>
<thead>
<tr>
<th>Enable Central Management</th>
<th>Enables the Central Management feature on the FortiGate unit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the type of central management for this FortiGate unit. You can select FortiManager or the FortiGuard Management Service.</td>
</tr>
<tr>
<td>FortiManager</td>
<td>Select to use FortiManager as the central management service for the unit.</td>
</tr>
<tr>
<td></td>
<td>Enter the IP address or name of the FortiManager unit in the IP/Name field.</td>
</tr>
<tr>
<td></td>
<td>If your organization is operating a FortiManager cluster, add the IP address or name of the primary FortiManager unit to the IP/Name field and add the IP address or name of the backup FortiManager units to the Trusted FortiManager list.</td>
</tr>
<tr>
<td></td>
<td>Status indicates whether or not the FortiGate unit can communicate with the FortiManager unit added to the IP/Name field.</td>
</tr>
<tr>
<td></td>
<td>Select Register to include the FortiManager unit in the Trusted FortiManager List.</td>
</tr>
<tr>
<td></td>
<td>A red arrow-down indicates that there is no connection enabled. A green arrow-up indicates that there is a connection. A yellow caution symbol appears when your FortiGate unit is considered an unregistered device by the FortiManager unit.</td>
</tr>
<tr>
<td>FortiGuard Management Service</td>
<td>Select to use the FortiGuard Management Service as the central management service for the unit.</td>
</tr>
<tr>
<td></td>
<td>Enter the Account ID in the Account ID field. If you do not have an account ID, register for the FortiGuard Management Service on the FortiGuard Management Service website.</td>
</tr>
<tr>
<td></td>
<td>Select Change to go directly to System &gt; Maintenance &gt; FortiGuard Under Analysis &amp; Management Service Options, enter the account ID in the Account ID field.</td>
</tr>
</tbody>
</table>

Settings
The Settings menu includes the following features that you can configure:

• ports for HTTP/HTTPS administrative access and SSL VPN login
• password policy for administrators and IPsec pre-shared keys
• the idle timeout setting
• settings for 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)
• SCP capability for users logged in via SSH
• Wireless controller capability
• IPv6 support on the web based manager.
Configure administrative settings in System > Admin > Settings using the following table.

**Administrators Settings page**
Provides settings for configuring different system options, such as enabling IPv6 on the web-based manager.

### Web Administration Ports

<table>
<thead>
<tr>
<th>Port Type</th>
<th>TCP Port to be used for administrative access. Default values are indicated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>TCP port to be used for administrative HTTP access. The default is 80.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP port to be used for administrative HTTPS access. The default is 443.</td>
</tr>
<tr>
<td>SSLVPN Login Port</td>
<td>An alternative HTTPS port number for remote client web browsers to connect to the FortiGate unit. The default port number is 10443.</td>
</tr>
<tr>
<td>Telnet Port</td>
<td>TCP port to be used for administrative telnet access. The default is 23.</td>
</tr>
<tr>
<td>SSH Port</td>
<td>TCP port to be used for administrative SSH access. The default is 22.</td>
</tr>
<tr>
<td>Enable SSH v1 compatibility</td>
<td>Enable compatibility with SSH v1 in addition to v2. (Optional)</td>
</tr>
</tbody>
</table>

### Password Policy

- **Enable**
  - Select to enable the password policy.
- **Minimum Length**
  - Set the minimum acceptable length for passwords.
- **Must contain**
  - Select any of the following special character types to require in a password. Each selected type must occur at least once in the password.
    - Upper Case Letters — A, B, C, ... Z
    - Lower Case Letters — a, b, c, ... z
    - Numerical digits — 0, 1, 2, 3, 4, 5, 6, 7 8, 9
    - Non-alphanumeric Letters — punctuation marks, @, #, ... %

- **Apply Password Policy to**
  - **Admin Password** — Apply to administrator passwords. If any password does not conform to the policy, require that administrator to change the password at the next login.
  - **IPSEC Preshared Key** — Apply to preshared keys for IPSec VPNs. The policy applies only to new preshared keys. You are not required to change existing preshared keys.

- **Admin Password Expires after n days**
  - Require administrators to change password after a specified number of days. Specify 0 to remove required periodic password changes.

### Timeout Settings

- **Idle Timeout**
  - The number of minutes an administrative connection must be idle before the administrator has to 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**
  - The language the web-based manager uses. Choose from English, Simplified Chinese, Japanese, Korean, Spanish, Traditional Chinese or French.
  - You should select the language that the operating system of the management computer uses.
- **Lines per Page**
  - Number of lines per page to display in table lists. The default is 50. Range is from 20 - 1000.
- **IPv6 Support on GUI**
  - Enable to configure IPv6 options from the GUI (Firewall policy, route, address and address group). Default allows configuration from CLI only.
LCD Panel (LCD-equipped models only)

**PIN Protection**
Select and enter a 6-digit PIN. Administrators must enter the PIN to use the control buttons and LCD.

**Enable SCP**
Enable users logged in through the SSH to be able to use Secure Copy (SCP) to copy the configuration file.

**Enable Wireless Controller**
Enable the Wireless Controller feature. Then you can access the Wireless Controller menu in the web-based manager and the corresponding CLI commands. For more information, see "Wireless Controller" on page 355.

Note: If you make a change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is unique.

## Certificates

The Certificate menu allows users to import and manage security certificates (X.509). Certificate authentication allows administrators 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.

There are several certificates on the unit that have been automatically generated, and are explained in detail in Table 18 on page 123. System administrators can use these certificates wherever they may be required, for example, with SSL VPN, IPSec, LDAP, and PKI.

### Table 18: Automatically generated FortiGate certificates

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fortinet_Firmware</strong></td>
<td>Embedded inside the firmware. Signed by Fortinet_CA. Same on all FortiGate units. Used so FortiGate units without Fortinet_Factory2 certificates have a built-in certificate signed by a FortiGate CA. Listed under Certificates &gt; Local, or in FortiGate CLI under vpn certificate local.</td>
</tr>
<tr>
<td><strong>Fortinet_Factory</strong></td>
<td>Embedded inside BIOS. Signed by Fortinet_CA. Unique to each FortiGate unit. Used for FortiGate/FortiManager tunnel, HTTPS administrative access if Fortinet_Factory2 is not available. Listed under Certificates &gt; Local, or in FortiGate CLI under vpn certificate local.</td>
</tr>
<tr>
<td><strong>Fortinet_Factory2</strong></td>
<td>Embedded inside BIOS. Signed by Fortinet_CA2. Unique to each FortiGate unit. Used for FortiGate/FortiManager tunnel and HTTPS administrative access. Listed under Certificates &gt; Local, or in FortiGate CLI under vpn certificate local. Found only on units shipped at the end of 2008 onward.</td>
</tr>
<tr>
<td><strong>Fortinet_CA</strong></td>
<td>Embedded inside firmware and BIOS. Fortinet's CA certificate. Used to verify certificates that claim to be signed by Fortinet, for example with a FortiGate/FortiManager tunnel or an SSL connection to a FortiGuard server. Listed under Certificates &gt; CA, or in FortiGate CLI under vpn certificate ca or vpn certificate ocsp.</td>
</tr>
<tr>
<td><strong>Fortinet_CA2</strong></td>
<td>Embedded inside BIOS. Fortinet’s CA certificate. Will eventually replace Fortinet_CA, as Fortinet_CA will expire in 2020. Listed under Certificates &gt; CA, or in FortiGate CLI under vpn certificate ca or vpn certificate ocsp. Found only on units shipped at the end of 2008 onward.</td>
</tr>
</tbody>
</table>
This topic contains the following:

- Local Certificates
- Remote Certificates
- CA Certificates
- CRL

**Note:** SSL sessions that use client-certificates can now bypass the SSL inspection. For this to work properly, an SSL server should be set up that requires client-side certificates. These certificates are then uploaded to the client, making a connection through the unit with the SSL inspection feature enabled on the unit.

### Local Certificates

Certificate requests and installed server certificates are displayed in list on the Local Certificates page. 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 the certificate and send it to you to install on the FortiGate unit.

Local certificates can update automatically online prior to expiry. This must be configured in the CLI.

View and import signed local certificates from **System > Certificates > Local Certificates** using the following table.

<table>
<thead>
<tr>
<th>Local Certificates page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists the default local certificates as well as the certificates that you have imported. You can also generate certificates from this page.</td>
</tr>
</tbody>
</table>

**Generate**
Generates a local certificate request. When you select Generate, you are automatically redirected to the Generate Certificate Signing Request page.

**Import**
Import a signed local certificate. When you select Import, you are automatically redirected to the Import Certificate page. From this page, you can import a local certificate, PKCS12 certificate, or a certificate containing a key file and password.

**Name**
The names of existing local certificates and pending certificate requests.

**Subject**
The Distinguished Names (DNs) of local signed certificates.

**Comments**
A description of the certificate.

**Status**
The status of the local certificate. **PENDING** designates a certificate request that needs to be downloaded and signed.

**View Certificate Detail**
Display certificate details such as the certificate name, issuer, subject, and valid certificate dates.

**Delete**
Removes the selected certificate request or installed server certificate from the FortiGate configuration. This is available only if the certificate has **PENDING** status.

You cannot remove default Fortinet certificates.

To remove multiple local certificates from within the list, on the Local Certificates page, in each of the rows of certificates you want removed, select the check box and then select Delete.

To remove all local certificates from within the list, on the Local Certificates page, select the check box in the check box column and then select Delete.
Generating a certificate request

The unit generates a certificate request based on the information you enter to identify the unit. Generated requests are displayed in the list on the Local Certificates page with a status of PENDING. After generating a certificate request, you can download the request to a computer that has management access to the unit and then forward the request to a CA.

Fill out a certificate request in System > Certificates > Local Certificates by selecting Generate and then using the following table.

Download
Save a copy of the certificate request to a local computer. You can send the request to your CA to obtain a signed server certificate for the unit (SCEP-based certificates only).

You have to fill out a certificate request and generate the request before you can submit the results to a CA.

Submit the request to your CA as follows:
- Using the web browser on the management computer, browse to the CA web site.
- Follow the CA instructions to place a base-64 encoded PKCS#12 certificate request and upload your certificate request.
- 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).
- When you receive the signed certificate from the CA, install the certificate on the FortiGate unit. See “Importing a signed server certificate” on page 126.

Edit Comments
Modifies the description of a certificate. You cannot modify the description of the default certificates.

Certification Name
Enter 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.

Subject Information section of the page
Enter the information needed to identify the unit.

ID Type
Select an ID type from the drop-down list. You can choose Host IP, Domain Name, or E-Mail.
- If the unit has a static IP address, select Host IP and enter the public IP address of the unit.
- If the unit does not have a public IP address, use an email address (or domain name if available) instead.

IP
If the unit has a static IP address and subscribes to a dynamic DNS service, use a domain name, if available, to identify the unit.

Domain Name
If you select Domain Name, enter the fully qualified domain name of the unit. Do not include the protocol specification (http://) or any port number or path names. If a domain name is not available and the unit subscribes to a dynamic DNS service, an “unable to verify certificate” message may be displayed in the user’s browser whenever the public IP address of the unit changes.

E-Mail
If you select E-Mail, enter the email address of the owner of the unit.

Optional Information section of the page
Complete as described or leave blank.

Organization Unit
Enter the name of your department or departments. You can enter a maximum of 5 Organization Units. To add or remove a unit, use the plus (+) or minus (-) icon.
Importing a signed server certificate

Your CA will provide you with a signed server certificate to install on the unit. When you receive the signed certificate from the CA, save the certificate on a computer that has management access to the unit. The certificate file can be in either PEM or DER format.

Import signed server certificates in System > Certificates > Local Certificates using the following table.

| Organization | Enter the legal name of your company or organization. |
| Locality (City) | Enter the name of the city or town where the FortiGate unit is installed. |
| State/Province | Enter the name of the state or province where the FortiGate unit is installed. |
| Country/Region | Select the country where the FortiGate unit is installed. |
| e-mail | Enter the contact email address. |
| Key Type | Only RSA is supported. |
| Key Size | Select 1024 Bit, 1536 Bit or 2048 Bit. Larger keys are slower to generate but they provide better security. |
| Enrollment Method | Select one of the following methods: |
| File Based | Select to generate the certificate request. |
| Online SCEP | Select to obtain a signed SCEP-based certificate automatically over the network. |
| CA Server URL | Enter the URL of the SCEP server from which to retrieve the CA certificate. |
| Challenge Password | Enter the CA server challenge password. |

Importing an exported server certificate and private key

You will need to know the password in order to import the certificate file. Before you begin, save a copy of the file on a computer that has management access to the unit.

Import the PKC S12 file in System > Certificates > Local Certificates using the following table.

| Type | Select PKCS12 Certificate. |
| Certificate with key file | Enter the full path to and file name of the previously exported PKCS12 file. |
| Browse | Alternatively, browse to the location on the management computer where the PKCS12 file has been saved, select the file, and then select OK. |
| Password | Type the password needed to upload the PKCS12 file. |
Importing separate server certificate and private key files

When the server certificate request and private key were not generated by the unit, you will receive them as separate files. Copy the two files to the management computer.

Import the certificate and private key files in System > Certificates > Local Certificates using the following table.

<table>
<thead>
<tr>
<th>Import Certificate page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides settings for importing a specific signed certificate from the CA. The following settings are available when you select Certificate from the Type drop-down list.</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Certificate file</td>
</tr>
<tr>
<td>Browse</td>
</tr>
<tr>
<td>Key file</td>
</tr>
<tr>
<td>Browse</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

Note: The certificate file must not use 40-bit RC2-CBC encryption.

Remote Certificates

For dynamic certificate revocation, you need to use an Online Certificate Status Protocol (OCSP) server. Remote certificates are public certificates without a private key. The OCSP is configured in the CLI only.

Installed Remote (OCSP) certificates are displayed in the Remote Certificates list. 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).

Note: There is one OCSP per VDOM.

Import remote OCSP certificates in System > Certificates > Remote using the following table.

<table>
<thead>
<tr>
<th>Remote page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists the public certificates. On this page you can import, delete and view certificates.</td>
</tr>
<tr>
<td>Import</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Subject</td>
</tr>
<tr>
<td>Delete</td>
</tr>
<tr>
<td>View Certificate Detail</td>
</tr>
<tr>
<td>Download</td>
</tr>
</tbody>
</table>
CA Certificates

When you apply for a signed personal 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 certificate, install it on the remote clients according to the browser documentation. Install the corresponding root certificate and CRL from the issuing CA on the FortiGate unit.

CA certificates can update automatically online prior to expiry. This must be configured in the CLI using the `vpn certificate local` command.

Installed CA certificates are displayed in the CA Certificates list. You cannot delete the Fortinet_CA certificate.

After you download the root certificate of the CA, save the certificate on a PC that has management access to the unit. If you choose SCEP, the system starts the retrieval process as soon as you select OK.

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).

Import CA certificates in System > Certificates > CA Certificates using the following table.

---

**Upload Remote Certificate**
Provides settings for uploading a remote certificate to the unit.

- **Local PC** Enter the location in a management PC to upload a public certificate.
- **Browse** Alternatively, browse to the location on the management computer where the certificate has been saved, select the certificate, and then select OK.

---

**CA Certificates page**
Lists the CA certificates that you have created as well as the default CA certificate. You can also import a CA certificate.

- **Import** Import a CA root certificate. See “Importing a signed server certificate” on page 126.
- **Name** The names of existing CA root certificates. The unit assigns unique names (CA_Cert_1, CA_Cert_2, CA_Cert_3, and so on) to the CA certificates when they are imported.
- **Subject** Information about the issuing CA.
- **Delete** Removes a CA root certificate from the list on the page.
- **View Certificate Detail** Displays a certificate’s details.
- **Download** Saves a copy of the CA root certificate to a local computer.

---

**Import CA Certificate**
Provides settings for importing certificates using an SCEP server or Local PC.

- **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.
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.

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.

The system assigns a unique name to each CRL. The names are numbered consecutively (CRL_1, CRL_2, CRL_3, and so on).

Import CRLs in System > Certificates > CRL using the following table.

<table>
<thead>
<tr>
<th><strong>CRL page</strong></th>
<th>Lists each individual CRL. On this page you can import, view or download CRLs.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import</strong></td>
<td>Import a CRL. For more information, see “CRL” on page 129.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The names of existing certificate revocation lists. The unit assigns unique names (CRL_1, CRL_2, CRL_3, and so on) to certificate revocation lists when they are imported.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>Information about the certificate revocation lists.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Removes the selected CRL from the list on the page.</td>
</tr>
<tr>
<td><strong>View Certificate Detail</strong></td>
<td>Displays a CRL certificate's details, such as the issuer name and CRL update dates.</td>
</tr>
<tr>
<td><strong>Download</strong></td>
<td>Saves a copy of the CRL to a local computer.</td>
</tr>
</tbody>
</table>

**Import CRL page**

Provides settings to import CRLs from a HTTP, LDAP, SCEP server, or local PC.

<table>
<thead>
<tr>
<th><strong>HTTP</strong></th>
<th>Select to use an HTTP server to retrieve the CRL. Enter the URL of the HTTP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LDAP</strong></td>
<td>Select to use an LDAP server to retrieve the CRL, then select the LDAP server from the list.</td>
</tr>
<tr>
<td><strong>SCEP</strong></td>
<td>Select to use an SCEP server to retrieve the CRL, then select the Local Certificate from the list. Enter the URL of the SCEP server from which the CRL can be retrieved.</td>
</tr>
<tr>
<td><strong>Local PC</strong></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>

**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 unit does not have a copy of it or when the current copy expires.

Wireless

The Wireless menu appears only on FortiWiFi units. The majority of this section is applicable to all FortiWiFi units.

This topic contains the following:

- FortiWiFi wireless interfaces
- Wireless settings
- MAC Filter
- Wireless Monitor
Wireless

- Rogue AP detection

FortiWiFi wireless interfaces

FortiWiFi 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 more information on adding wireless interfaces, see “Adding a wireless interface” on page 132.

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. All FortiWiFi units can have up to 4 wireless interfaces.

or

- Connect the FortiWiFi unit to another wireless network. This is called Client mode. A FortiWiFi unit operating in client mode can also can only have one wireless interface.

or

- Monitor access points within radio range. This is called Monitoring mode. You can designate the detected access points as Accepted or Rogue for tracking purposes. No access point or client operation is possible in this mode. But, you can enable monitoring as a background activity while the unit is in Access Point mode.

FortiWiFi units support the following wireless network standards:

- IEEE 802.11a (5-GHz Band)
- IEEE 802.11b (2.4-GHz Band)
- IEEE 802.11g (2.4-GHz Band)
- IEEE 802.11n (5-GHz and 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

Wireless settings

By default, the FortiWiFi unit includes one wireless interface, called wlan. If you are operating your FortiWiFi unit in access point mode, you can add up to three virtual wireless interfaces. All wireless interfaces use the same wireless parameters. That is, you configure the wireless settings once, and all wireless interfaces use those settings. For more information on adding more wireless interfaces, see “Adding a wireless interface” on page 132.

When operating the FortiWiFi unit in Client mode, radio settings are not configurable.
Configure wireless settings in **System > Wireless > Radio Settings** using the following table.

**Radio Settings page**
Provides settings for configuring wireless parameters. On this page you can also change the operation mode. When you change modes, some settings are hidden. For example, in Client Mode, you cannot view the settings that were available when in Access Point, such as Band. When you are in Monitoring mode, only Operation Mode is available.

**Operation Mode**
Select *Change* to switch operation modes. When you select *Change*, you are automatically redirected to the Change operation mode for wireless page.

- **Access Point** — The FortiWiFi unit acts as an access point for wireless users to connect to send and receive information over a wireless network. It enables multiple wireless network users access to the network without the need to connect to it physically. The FortiWiFi unit can connect to the internal network and act as a firewall to the Internet.

- **Client** — The FortiWiFi unit is set to receive transmissions from another access point. This enables you to connect remote users to an existing network using wireless protocols.

- **Monitoring** — Scan for other access points. These are listed in the Rogue AP list. See “Rogue AP detection” on page 135.

**Note:** You cannot switch to Client mode or Monitoring mode if you have added virtual wireless interfaces. For these modes, there must be only one wireless interface, wlan.

**Band**
Select the wireless frequency band. Be aware what wireless cards or devices your users have as it may limit their use of the wireless network. For example, if you configure the FortiWiFi unit for 802.11g and users have 802.11b devices, they may not be able to use the wireless network.

**Geography**
Select your country or region. This determines which channels are available.

**Channel**
Select a channel for your wireless network or select Auto. The channels that you can select depend on the Geography setting.

**Tx Power**
Set the transmitter power level. The higher the number, the larger the area the FortiWiFi will broadcast. If you want to keep the wireless signal to a small area, enter a smaller number.

**Beacon Interval**
Set the interval between beacon packets. Access Points broadcast Beacons or Traffic Indication Messages (TIM) to synchronize wireless networks. A higher value decreases the number of beacons sent, however it may delay some wireless clients from connecting if it misses a beacon packet. Decreasing the value will increase the number of beacons sent, while this will make it quicker to find and connect to the wireless network, it requires more overhead, slowing throughput.

**Background Rogue AP Scan**
Perform the Monitoring mode scanning function while the unit is in Access Point mode. Scanning occurs while the access point is idle. The scan covers all wireless channels. Background scanning can reduce performance if the access point is busy. See “Rogue AP detection” on page 135.

**Interface**
The name of the wireless interface. To modify wireless interface settings, select the interface name. To add more wireless interfaces in Access Point mode, see “Adding a wireless interface” on page 132.

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

**SSID**
The wireless service set identifier (SSID) or network name for the wireless interface. To communicate, an Access Point and its clients must use the same SSID.
Adding a wireless interface

You can add up to three virtual wireless interfaces to your access point. These additional interfaces share the same wireless parameters configured for the WLAN interface for Band, Geography, Channel, Tx Power, and Beacon Interval. Ensure each wireless interface has a unique SSID.

Note: You cannot add additional wireless interfaces when the FortiWiFi unit is in Client mode or Monitoring mode.

Add a wireless interface in **System > Network > Interface** using the following table. Make sure to select **Wireless** in the **Type** drop-down list, so that you can access the wireless settings for the wireless interface.

### Wireless Settings section on the New Interface page

**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 with this network name.

**SSID Broadcast**
Select to broadcast the SSID. Broadcasting the SSID enables clients to connect to your wireless network without first knowing the SSID. For better security, do not broadcast the SSID. If the interface is not broadcast, there is less chance of an unwanted user connecting to your wireless network. If you choose not to broadcast the SSID, you need to inform users of the SSID so they can configure their wireless devices.

**Security mode**
Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface.

- **None** — has no security. Any wireless user can connect to the wireless network.
- **WEP64** — 64-bit web equivalent privacy (WEP). To use WEP64 you must enter a Key containing 10 hexadecimal digits (0-9 a-f) and inform wireless users of the key.
- **WEP128** — 128-bit WEP. To use WEP128 you must enter a Key containing 26 hexadecimal digits (0-9 a-f) and inform wireless users of the key.
- **WPA** — 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 eight characters or select a RADIUS server. If you select a RADIUS server the wireless clients must have accounts on the RADIUS server.
- **WPA2** — WPA with more security features. To use WPA2 you must select a data encryption method and enter a pre-shared key containing at least eight characters or select a RADIUS server. If you select a RADIUS server the wireless clients must have accounts on the RADIUS server.
- **WPA2 Auto** — the same security features as WPA2, but 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. If you select a RADIUS server the wireless clients must have accounts on the RADIUS server.

**Key**
Enter the security key. This field appears when selecting WEP64 or WEP128 security.
MAC Filter

To improve the security of your wireless network, you can enable MAC address filtering on the FortiWiFi unit. By enabling MAC address filtering, you define the wireless devices that can access the network based on their system MAC address. When a user attempts to access the wireless network, the FortiWiFi unit checks the MAC address of the user to the list you created. If the MAC address is on the approved list, the user gains access to the network. If the user is not in the list, the user is rejected.

Alternatively, you can create a deny list. Similar to the allow list, you can configure the wireless interface to allow all connections except those in the MAC address list.

Using MAC address filtering makes it more difficult for a hacker using random MAC addresses or spoofing a MAC address to gain access to your network. Note you can configure one list per WLAN interface.

The MAC Filter list enables you to view the MAC addresses you have added to a wireless interface and their status; either allow or deny. It also enables you to edit and manage MAC Filter lists.

Use the following table to view and modify settings for existing MAC addresses.

<table>
<thead>
<tr>
<th>MAC Filter page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
</tr>
<tr>
<td><strong>MAC address</strong></td>
</tr>
<tr>
<td><strong>List Access</strong></td>
</tr>
<tr>
<td><strong>Enable</strong></td>
</tr>
<tr>
<td><strong>Edit</strong></td>
</tr>
</tbody>
</table>

Lists the MAC addresses that you added to a wireless interface, including their status. When you edit a MAC address, you are automatically redirected to the MAC Filter Settings page.

**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 MAC filtering for the wireless interface.

**Edit**
- Modifies settings within a MAC address list for an interface. When you select Edit, you are automatically redirected to the MAC Filter Settings page.
MAC Filter Settings page
Provides settings to modify the existing MAC addresses that you added to a wireless interface. When you select Edit in the row of a MAC filter on the MAC Filter page, you are automatically redirected to the MAC Filtering Settings page.

List Access Select 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 Adds the entered MAC address to the list.
Remove Select one or more MAC addresses in the list and then select Remove to deleted the MAC addresses from the list.

Wireless Monitor
Go to System > Wireless > Monitor to view information about your wireless network. In Access Point mode, you can see who is connected to your wireless LAN. In Client mode, you can see which access points are within radio range.

Monitor page
Lists the wireless interfaces and clients or neighbors that are currently active. The information is grouped and placed in their own section within the page.

Statistics section
Statistical information about wireless performance for each wireless interface.

AP Name / 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.
Rx (KBytes) The amount of data in kilobytes received this session.
Tx (KBytes) The amount of data in kilobytes sent this session.

Clients list section (AP mode)
Real-time details about the client wireless devices that can reach this FortiWiFi unit access point. Only devices on the same radio band are listed.

MAC Address The MAC address of the connected wireless client.
IP Address The IP address assigned to the connected wireless client.
AP Name The name of the wireless interface that the client is connected to.

Neighbor AP list section (Client mode)
Real-time details about the access points that the client can receive.

MAC Address The MAC address of the connected wireless client.
SSID The wireless service set identifier (SSID) that this access point broadcasts.
Channel The wireless radio channel that the access point uses.
Rate (M) The data rate of the access point in Mbits/s.
RSSI The received signal strength indication, a relative value between 0 (minimum) and 255 (maximum).
Rogue AP detection

On models that support Rogue Access Point Detection, you can select Monitoring mode to scan for available wireless access points. You can also enable scanning in the background while the unit is in Access Point mode.

To enable the monitoring mode
1. Go to System > Wireless > Radio Settings.
2. Select Change beside the current operation mode.
3. Select Monitoring and then select OK.
4. Select OK to confirm the mode change.
5. Select Apply.

To enable background scanning
1. Go to System > Wireless > Radio Settings.
2. On the Wireless Parameters page, select the check box for Background Rogue AP Scan.
3. Select Apply.

Viewing wireless access points

Access points are listed in the Unknown Access Points list until you mark them as either Accepted or Rogue access points. This designation helps you to track access points. It does not affect anyone’s ability to use these access points.

You can also enter information about accepted and rogue APs in the CLI without having to detect them first using the system wireless ap-status command.

Go to System > Wireless > Rogue AP to view detected access points. This is available in Monitoring mode, or in Access Point mode with Background Rogue AP Scan enabled.

Rogue AP page
Lists the detected access points that are active.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Interval</td>
<td>Set time between information updates. none means no updates.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Updates the displayed information immediately so that you can view current information.</td>
</tr>
<tr>
<td>Inactive Access Points</td>
<td>Select which inactive access points to show: all, none, those detected less than one hour ago, or those detected less than one day ago.</td>
</tr>
<tr>
<td>Online</td>
<td>A green checkmark indicates an active access point. A grey X indicates that the access point is inactive.</td>
</tr>
<tr>
<td>SSID</td>
<td>The wireless service set identifier (SSID) or network name for the wireless interface.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the Wireless interface.</td>
</tr>
<tr>
<td>Signal Strength /Noise</td>
<td>The signal strength and noise level.</td>
</tr>
<tr>
<td>Channel</td>
<td>The wireless radio channel that the access point uses.</td>
</tr>
<tr>
<td>Rate</td>
<td>The data rate of the access point.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The data and time when the FortiWifi unit first detected the access point.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The data and time when the FortiWifi unit last detected the access point.</td>
</tr>
<tr>
<td>Mark as ‘Accepted AP’</td>
<td>Select the icon to move this entry to the Accepted Access Points list.</td>
</tr>
</tbody>
</table>
Maintenance

This section describes how to maintain your system configuration as well as how to enable and update FDN services. This section also explains the types of FDN services that are available for your unit.

The maintenance menu provides help with maintaining and managing firmware, configuration revisions, script files, and FortiGuard subscription-based services. From this menu, you can upgrade or downgrade the firmware, view historical backups of configuration files, or update FortiGuard services.

The maintenance menu has the following menus:

- **Revision Control** - displays all system configuration backups with the date and time of when they were backed up. Before you can use revision control, a Central Management server must be configured and enabled.

- **Firmware** - displays the firmware images that are currently stored on the unit as well as the firmware image currently running on the unit.

- **Advanced** - displays advanced settings for scripts, USB auto-install and allows downloads of the debug log.

- **FortiGuard** - displays all FDN subscription services, such as antivirus and IPS definitions as well as the FortiGuard Analysis & Management Service. This tab also provides configuration options for antivirus, IPS, web filtering, and antispam services.

- **License** - allows you to increase the maximum number of VDOMs (on some models).

- **Disk** - displays detailed information about the status of multiple local disks.

When backing up the system configuration, web content files and email filtering files are also included. You can save the configuration to the management computer, a USB disk if your unit includes a USB port (see “Formatting USB Disks” on page 139), or to its local hard disk. You can also restore the system configuration from previously downloaded backup files in the Backup & Restore menu.

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 included in 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 that the regular administrator belongs to. A regular administrator is the only user account that can restore the configuration from this file.

Some models support FortiClient by storing a FortiClient image that users can download. The FortiClient section of Backup & Restore is available if your FortiGate model supports FortiClient.

**Tip:** For simplified procedures on managing firmware, including backup and restore options as well as uploading and downloading firmware for your unit, see “Firmware management practices” on page 161.

This topic contains the following:
Configuration Revision

The Configuration Revisions menu enables you to manage multiple versions of configuration files. Revision control requires either a configured central management server, or the local hard drive. The central management server can either be a FortiManager unit or the FortiGuard Analysis & Management Service.

If central management is not configured on your unit, a message appears to tell you to do one of the following:

- enable central management (see “Central Management” on page 120)
- obtain a valid license.

When revision control is enabled on your unit, and configurations have been backed up, a list of saved revisions of those backed-up configurations appears.

Configuration revisions are viewed in System > Maintenance > Configuration Revision.

Configuration Revision page

Lists all the configuration revisions. On this page, you can delete, edit or upload a configuration file. This page also allows you to change comments, view the differences between revisions, and revert to a previous configuration.

OS Version

<firmware_version_build>
(appears as sections on the page)

The section of the page that contains the configuration files that belong to the specified FortiOS firmware version and build number. For example, if you have four configuration revisions for 4.0 MR1 (build-178) they appear in the section OS Version 4.00 build178 on the Configuration Revision page.

Revision

An incremental number indicating the order in which the configurations were saved. These may not be consecutive numbers if configurations are deleted.

The most recent, and highest, number is first in the list.

Date/Time

The date and time this configuration was saved on the FortiGate unit.

Administrator

The administrator account that was used to back up this revision.

Comments

Any relevant information saved with the revision, such as why the revision was saved, who saved it, and if there is a date when it can be deleted to free up space.

Diff

Select to compare two revisions.

A window will appear, from which you can view and 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

Downloads this revision to your local PC.

Revert

Restores the previous selected revision. You will be prompted to confirm this action.
Firmware

The Firmware menu allows you to install firmware on your unit, as well as upload a firmware image to install at a later date. You can also view what firmware is currently running on the unit from this menu.

To view firmware images, as well as upload and install an image, go to System > Maintenance > Firmware.

**Firmware page**

Lists all firmware images that have been uploaded to the unit.

- **Currently Running Firmware**: Displays the firmware image that is currently running on the unit.
- **Delete**: Removes the firmware image from the list.
- **Change Comments**: Changes the description for the firmware image.
- **Upgrade**: You must select the firmware image in the list to install that image on the unit.
- **Upload**: When you select Upload, you are automatically redirected to the Upload page. On this page you can select the firmware image to upload, enable Boot New Firmware (which installs the selected firmware on the unit), and enter any description about the firmware that you want.

**Firmware Version**: The firmware version number of the firmware image.

**Date**: The date the firmware image was created on.

**Create by**: The administrator who uploaded the firmware image.

**Comments**: The description about the image.

Back up and restoring configuration files

You can back up or restore your FortiGate configuration to your management PC, a central management server, or a USB disk. You can back up and restore your configuration to a USB disk if the unit includes a USB port and if you have connected a USB disk to the USB port. FortiGate units support most USB disks including USB keys and external USB hard disks (see "Formatting USB Disks" on page 139). The central management server is whatever remote management service the unit is connected to. For example, if the current configuration on a FortiGate-60 is backed up to a FortiManager unit, the central management server is the FortiManager unit.

You must configure central management in System > Admin > Central Management before these options are available in the Backup & Restore section.

Backup and restore settings are available only in the CLI. The `execute backup config` command and `execute restore config` command are used to backup and restore the unit’s configuration file.
Formatting USB Disks

Caution: Formatting the USB disk deletes all information on the disk. Back up the information on the USB disk before formatting to ensure all information on the disk is recoverable.

FortiGate units with USB ports support USB disks for backing up and restoring configurations.

FortiUSB and generic USB disks are supported, but the generic USB disk must be formatted as a FAT16 disk. No other partition type is supported.

There are two ways that you can format the USB disk, either by using the CLI or a Windows system. You can format the USB disk in the CLI using the command syntax, `exe usb-disk format`. When using a Windows system to format the disk, at the 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.

Remote FortiManager backup and restore options

Your FortiGate unit can be remotely managed by a FortiManager unit. The FortiGate unit connects using the FortiGuard-FortiManager protocol. This protocol provides communication between a FortiGate unit and a FortiManager unit, and runs over SSL using IPv4/TCP port 541.

After successfully connecting to the FortiManager unit from your FortiGate unit, you can back up your configuration to the FortiManager unit. You can also restore your configuration.

The automatic configuration backup is available only in local mode on the FortiManager unit.

A list of revisions is displayed when restoring the configuration from a remote location. The list allows you to choose the configuration to restore.

Remote FortiGuard backup and restore options

Your unit can be remotely managed by a central management server, which is available when you register for the FortiGuard Analysis & Management Service. The FortiGuard Analysis & Management Service is a subscription-based service and is purchased by contacting support.

After registering, you can back up or restore your configuration. The FortiGuard Analysis & Management Service is useful when administering multiple FortiGate units without having a FortiManager unit.

You can also upgrade the firmware on your unit using the FortiGuard Analysis & Management Service. Upgrading the firmware is available in the Firmware Upgrade section of the backup and restore menu.

When restoring the configuration from a remote location, a list of revisions is displayed so that you can choose the configuration file to restore.

Note: The FortiGuard-FortiManager protocol is used when connecting to the FortiGuard Analysis & Management Service. This protocol runs over SSL using IPv4/TCP port 541 and includes the following functions:

- detects FortiGate unit dead or alive status
- detects management service dead or alive status
- notifies the FortiGate units about configuration changes, AV/IPS database update and firewall changes.
FortiGuard

The FortiGuard Distribution Network (FDN) and FortiGuard Services provides updates to antivirus definitions, IPS definitions, and the Antispam rule set. FortiGuard Services include FortiGuard web filtering and the FortiGuard Analysis and Management Service.

This topic contains the following:

- FortiGuard Distribution Network
- FortiGuard services
- Configuring the FortiGate unit for FDN and FortiGuard subscription services

FortiGuard Distribution Network

The FDN is a world-wide network of FortiGuard Distribution Servers (FDS). The FDN provides updates to antivirus (including grayware) definitions, IPS definitions, and the antispam rule set. When the FortiGate unit contacts the FDN, it connects to the nearest FDS based on the current time zone setting.

The FortiGate unit supports the following update options:

- user-initiated updates from the FDN
- hourly, daily, or weekly scheduled antivirus definition, IPS definition, and antispam rule set 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.

The unit must be able to connect to the FDN using HTTPS on port 443 to receive scheduled updates. For more information, see “To enable scheduled updates” on page 146.

You can also configure the unit to receive push updates. When the unit is receiving push updates, the FDN must be able to route packets to the unit using UDP port 9443. For more information, see “Enabling push updates” on page 147. If the FortiGate unit is behind a NAT device, see “Enabling push updates through a NAT device” on page 148.

FortiGuard services

Worldwide coverage of FortiGuard services is provided by FortiGuard service points. When the unit is connecting to the FDN, it is connecting to the closest FortiGuard service point. Fortinet adds new service points as required.

If the closest service point becomes unreachable for any reason, the unit contacts another service point and information is available within seconds. By default, the unit communicates with the service point via UDP on port 53. Alternately, you can switch the UDP port used for service point communication to port 8888 by going to System > Maintenance > FortiGuard.

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 more 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, email filtering tools, contained in an antispam rule set that is downloaded to the unit. The IP address black list contains IP addresses of email servers known to generate spam. The URL black list contains URLs that are 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. You can either enable or disable FortiGuard Antispam in an email filter profile. For more information, see “Email Filter” on page 272.

Every 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 unit automatically contacts a FortiGuard Antispam service point when enabling FortiGuard Antispam. Contact Fortinet Technical Support to renew the FortiGuard Antispam license after the free trial expires.

You can globally enable FortiGuard Antispam (Email Filter) in System > Maintenance > FortiGuard and then configure Email Filtering options in UTM > Email Filtering > Profile. For more information, see “Email Filter” on page 272.

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 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 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 unit automatically contacts a FortiGuard service point when enabling FortiGuard category blocking. Contact Fortinet Technical Support to renew a FortiGuard license after the free trial.

You can globally enable FortiGuard Web Filtering in System > Maintenance > FortiGuard and then configure FortiGuard Web Filtering options in UTM > Web Filtering > Profile. For more information, see “Web Filter” on page 259.

FortiGuard Analysis & Management Service

FortiGuard Analysis & Management Service is a subscription-based service that provides remote management services, including logging and reporting capabilities for all FortiGate units. These services were previously available only on FortiAnalyzer and FortiManager units.

The subscription-based service is available from the FortiGuard Analysis & Management Service portal web site, which provides a central location for configuring logging and reporting and remote management, and for viewing subscription contract information, such as daily quota and the expiry date of the service.

Configuring the FortiGate unit for FDN and FortiGuard subscription services

FDN updates, as well as FortiGuard services, are configured in System > Maintenance > FortiGuard. The FDN page contains four sections of FortiGuard services:

- Support Contract and FortiGuard Subscription Services
- Downloading antivirus and IPS updates
- Configuring Web Filtering and Email Filtering Options
• Configuring FortiGuard Analysis & Management Service Options

Support Contract and FortiGuard Subscription Services

The Support Contract and FortiGuard Subscription Services sections are displayed in abbreviated form within the License Information widget. You can view FortiGuard options and subscription services from System > Maintenance > FortiGuard.

FortiGuard Distribution Network page

Lists detailed information about your unit’s support contract and FortiGuard subscription services. On this page, you can also enter the Analysis and Management Services contact account ID, as well as antivirus and IPS options and web filtering and email filtering options.

Support Contract

The availability or status of your unit’s support contract. The status displays can be one of the following: Unreachable, Not Registered or Valid Contract.

If Valid Contract is shown, the FortiOS firmware version and contract expiry date appear. A green checkmark also appears.

[Register] Select to register your unit’s support contract.
This option is available only when the support contract is not registered.
The following options are available if you have registered the unit:
• Hardware
• Firmware
• Enhanced Support
• Comprehensive Support

FortiGuard Subscription Services

Availability and status information for each of the FortiGuard subscription services including:
• AntiVirus
• Intrusion Protection
• Vulnerability Compliance and Management
• Web Filtering
• Email Filtering
• Analysis & Management Service

[Availability] The availability of this service on this unit, dependent on your service subscription. The status can be Unreachable, Not Registered, Valid License, or Valid Contract.
The option Subscribe appears if Availability is Not Registered.
The option Renew appears if Availability has expired.

[Update] Select to manually update this service on your unit. This will prompt you to download the update file from your local computer. Select Update Now to immediately download current updates from FDN directly.

[Subscribe] Select to subscribe for the FortiGuard subscription service.

[Login Now] Select to log in to the Fortinet Support web site. This displays in the Registration row in Support Contract.

[Register] Select to register the service. This is displayed in Analysis & Management Service.
Downloading antivirus and IPS updates

In the Antivirus and IPS Options section, you can schedule antivirus and IPS updates, configure an override server, or allow push updates. You can access these options by selecting the expand arrow.

The SETUP message that the unit sends when you enable push updates includes the IP address of the FortiGate interface that the FDN connects to. Use the Use override push IP option when your unit is behind a NAT device. The unit sends the FDS the IP and port numbers of the NAT device to the FDS. The NAT device must also be configured to forward the FDS traffic to the unit on port 9443.

Expand the Antivirus and IPS Options section to configure these options using the following table.

<table>
<thead>
<tr>
<th>Status Icon</th>
<th>Indicates the status of the subscription service. The icon corresponds to the availability description.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Gray (Unreachable) – FortiGate unit is not able to connect to service.</td>
</tr>
<tr>
<td></td>
<td>• Orange (Not Registered) – FortiGate unit can connect, but is not subscribed to this service.</td>
</tr>
<tr>
<td></td>
<td>• Yellow (Expired) – FortiGate unit had a valid license that has expired.</td>
</tr>
<tr>
<td></td>
<td>• Green (Valid license) – FortiGate unit can connect to FDN and has a registered support contract.</td>
</tr>
</tbody>
</table>

If the Status icon is green, the expiry date is displayed.

<table>
<thead>
<tr>
<th>[Version]</th>
<th>The version number of the definition file currently installed on the unit for this service.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>[Updated yyyy-mm-dd via &lt;method&gt;]</th>
<th>The date of the last update and method used for last attempt to download definition updates for this service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Date]</td>
<td>Local system date when the FortiGate unit last checked for updates for this service.</td>
</tr>
</tbody>
</table>

**Antivirus and IPS Options section of the FortiGuard Distribution Network page**

Provides settings for scheduling updates, configuring an override server or allowing push updates.

<table>
<thead>
<tr>
<th>Use override server address</th>
<th>Select to configure an override server if you cannot connect to the FDN or if your organization provides updates using their own FortiGuard server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 145.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Push Update</th>
<th>Select to allow push updates. Updates are then sent automatically to your unit when they are available, eliminating any need for you to check if they are available.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Allow Push Update status icon</th>
<th>The status of the unit for receiving push updates:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Gray (Unreachable) - the unit is not able to connect to push update service</td>
</tr>
<tr>
<td></td>
<td>• Yellow (Not Available) - the push update service is not available with current support license</td>
</tr>
<tr>
<td></td>
<td>• Green (Available) - the push update service is allowed. See “Enabling push updates” on page 147.</td>
</tr>
<tr>
<td></td>
<td>If the icon is gray or yellow, see “Troubleshooting FDN connectivity” on page 145.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use override push IP</th>
<th>Available only if both Use override server address and Allow Push Update are enabled. Enter the IP address of the NAT device in front of your unit. FDS will connect to this device when attempting to reach the unit. The NAT device must be configured to forward the FDS traffic to the unit on UDP port 9443. See “Enabling push updates through a NAT device” on page 148.</th>
</tr>
</thead>
</table>
### 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 unit. Available only if *Use override push* is enabled.

### Schedule Updates
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 to manually initiate an FDN update.

### Submit attack characteristics…
Fortinet recommends that you select this check box. It helps to improve the quality of IPS signature.

### Configuring Web Filtering and Email Filtering Options
You can access this section by selecting the expand arrow to view *Web Filtering* and *Email Filtering* options.

#### Web Filtering and Email Filtering Options section of the FortiGuard Distribution Network page
Provides settings for enabling the FortiGuard web filter service, cache, and email filter service.

- **Enable Web Filter**
  Select to enable the FortiGuard Web Filter service.

  - **TTL**
    Time to live. The number of seconds to store blocked IP addresses and URLs in the cache before contacting the server again. TTL must be between 300 and 86400 seconds. Available only if both *Enable Web Filter* and *Enable Cache* are selected.

- **Enable Email Filter**
  Select to enable the FortiGuard AntiSpam service.

  - **TTL**
    Time to live. The number of seconds to store blocked IP addresses and URLs in the cache before contacting the server again. TTL must be between 300 and 86400 seconds.

#### Port Section
Select one of the following ports for your web filtering and antispam requirements:

- **Use Default Port (53)**
  Select to use port 53 for transmitting with FortiGuard Antispam servers.

- **Use Alternate Port (8888)**
  Select to use port 8888 for transmitting with FortiGuard Antispam servers.

### Test Availability
Select to test the connection to the servers. Results are shown below the button and on the Status indicators.

### Configuring FortiGuard Analysis & Management Service Options
The *Analysis & Management Service Options* section contains the Account ID and other options regarding the FortiGuard Analysis & Management Service.

You can access this section by selecting the expand arrow.
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 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. For more information, see “To add an override server” on page 146. If this is not successful, check your configuration to make sure you can connect to the override FortiGuard server from the unit.

Push updates might be unavailable if:

• you have not registered the unit (go to Product Registration and follow the instructions on the web site if you have not already registered your unit)

• there is a NAT device installed between the unit and the FDN (see “Enabling push updates through a NAT device” on page 148)

• your unit connects to the Internet using a proxy server (see “To enable scheduled updates through a proxy server” on page 147).

Updating antivirus and attack definitions

Use the following procedures to configure the unit to connect to the FDN to update the antivirus (including grayware) definitions and IPS attack definitions.

Note: Updating antivirus and IPS attack definitions can cause a very short disruption in traffic scanning while the unit applies the new signature definitions. Fortinet recommends scheduling updates when traffic is light to minimize disruption.

To verify that the unit can connect to the FDN

1. Locate the System Information widget and, from the widget, verify that the time zone is correct.

   The time zone should correspond to the region where your unit is located.
2. Go to System > Maintenance > FortiGuard.

3. Expand the Web Filtering and Email Filtering Options to reveal the available options.

4. Select Test Availability.

The following message appears:

This might take a few minutes, do you want to continue?

5. Select OK to continue.

The unit tests its connection to the FDN. The test results displays at the top of the FortiGuard page.

To update antivirus and attack definitions

1. Go to System > Maintenance > FortiGuard.

2. Expand the Antivirus and IPS Options to reveal the available options.

3. 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 FortiGuard page lists new version information for antivirus definitions and IPS attack definitions. The page also displays new dates and version numbers for the updated definitions and engines. Messages are recorded to the event log, indicating whether the update was successful or not.

To enable scheduled updates

1. Go to System > Maintenance > FortiGuard.

2. Expand arrow beside AntiVirus and IPS Options to reveal the available options.

3. Select the Scheduled Update check box.

4. Select one of the following:

   - 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.

5. Select Apply.

The unit starts the next scheduled update according to the new update schedule.

Whenever the unit runs a scheduled update, the event is recorded in the event log.

If you cannot connect to the FDN, or if your organization provides antivirus and IPS attack updates using its own FortiGuard server, you can use the following procedure to add the IP address of an override FortiGuard server.

To add an override server

1. Go to System > Maintenance > FortiGuard.

2. Expand the AntiVirus and IPS Options to reveal the available options.

3. Select the check box beside Use override server address.
4 Type the fully qualified domain name or IP address of the FortiGuard server in the field provided.

5 Select Apply.

The unit tests the connection to the override server.

If the FortiGuard Distribution Network availability icon changes from gray to green, the unit has successfully connected to the override server.

If the FortiGuard Distribution Network availability icon stays gray, the unit cannot connect to the override server. Check the FortiGate configuration and network configuration for settings that may prevent the unit from connecting to the override FortiGuard server.

To enable scheduled updates through a proxy server

If your unit must connect to the Internet through a proxy server, you can use the config system autoupdate tunneling command syntax to allow the unit to connect (or tunnel) to the FDN using the proxy server.

Enabling push updates

The FDN can push updates to units to provide the fastest possible response to critical situations. You must register the unit before it can receive push updates. Register your unit by going to the Fortinet Support web site, Product Registration, and following the instructions.

When you configure a unit to allow push updates, the unit sends a SETUP message to the FDN. The next time new antivirus or IPS attack definitions are released, the FDN notifies all units that are configured for push updates, that a new update is available. Within 60 seconds of receiving a push notification, the unit requests the update from the FDN.

When the network configuration permits, configuring push updates is recommended in addition to scheduled updates. Scheduled updates ensure that the unit receives current updates, but if push updates are also enabled, the unit will usually receive new updates sooner.

Fortinet does not recommend enabling push updates as the only method for obtaining updates. The unit might not receive the push notification. When the unit receives a push notification, it makes only one attempt to connect to the FDN and download updates.

Enabling push updates when a unit’s IP address changes

The SETUP message that the unit sends when you enable push updates includes the IP address of the FortiGate interface that the FDN connects to. The interface used for push updates is the interface configured in the default route of the static routing table.

The unit sends the SETUP message if you:

• change the IP address of this interface manually
• 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 so that your unit can receive push update messages. If your unit is behind a NAT device, see “Enabling push updates through a NAT device” on page 148.

If you have redundant connections to the Internet, the unit also sends the SETUP message when one Internet connection goes down and the unit fails over to another Internet connection.
In transparent mode, if you change the management IP address, the unit also sends the SETUP message to notify the FDN of the address change.

**Enabling push updates through a NAT device**

If the FDN connects only to the 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. Port forwarding enables the FDN to connect to the unit using UDP on either port 9443 or an override push port that you specify.

If the external IP address of the NAT device is dynamic (PPPoE or DHCP), the unit is unable to receive push updates through a NAT device.

The following procedures configure the unit to push updates through a NAT device. These procedures also include adding port forwarding virtual IP and a firewall policy to the NAT device.

The overall process is:

1. Register the unit on the internal network so that it has a current support license and can receive push updates.
2. Configure the following FortiGuard options on the unit on the internal network.
   - Enable *Allow push updates*.
   - Enable *Use override push IP* and enter the IP address. Usually this is 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 is the IP address of the external interface of the NAT device.

Add a firewall policy to the FortiGate NAT device that includes the port forwarding virtual IP.

![Note: Push updates are not supported if the unit must use a proxy server to connect to the FDN.](image)

**To configure FortiGuard options on the unit on the internal network**

1. Go to System > Maintenance > FortiGuard.
2. Select the expand arrow beside *AntiVirus and IPS Options* to reveal the available options.
3. Select the *Allow Push Update* check box.
4. Select the *Use override push IP* check box.
5. Enter the IP address of the external interface of the NAT device.
   - UDP port 9943 is changed only if it is blocked or in use.
6. Select *Apply*.

You can change to the push override configuration if the external IP address of the external service port changes; select *Apply* to have the unit send the updated push information to the FDN.

When the unit sends the override push IP address and port to the FDN, the FDN uses this IP address and port for push updates to the unit. However, push updates will not actually work until a virtual IP is added to the NAT device so that the NAT device accepts push update packets and forwards them to the unit on the internal network.
If the NAT device is also a unit, the following procedure, To add a port forwarding virtual IP to the FortiGate NAT device, allows you to configure the NAT device to use port forwarding to push update connections from the FDN to the unit on the internal network.

To add a port forwarding virtual IP to the FortiGate NAT device

1. Go to Firewall > Virtual IP > Virtual IP.
2. Select Create New.
3. Enter the appropriate information for the following:

   Name
   Enter a name for the Virtual IP.

   External Interface
   Select an external interface from the list. This is the interface that connects to the Internet.

   External IP Address/Range
   Enter the IP address and/or range. This is the IP address to which the FDN sends the push updates. This is usually the IP address of the external interface of the NAT device. This IP address must be the same as the IP address in User override push update for the FortiGate unit on the internal network.

   Mapped IP Address/Range
   Enter the IP address and/or range of the FortiGate unit on the internal network.

   Port Forwarding
   Select Port Forwarding. When you select Port Forwarding, the options Protocol, External Services Port and Map to Port appear.

   Protocol
   Select UDP.

   External Service Port
   Enter the external service port. The external service port is the 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 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
   Enter 9443. This is the port number to which the NAT FortiGate unit will send the push update after it comes through the virtual IP. FortiGate units expect push update notifications on port 9443.

4. Select OK.

To add a firewall policy to the FortiGate NAT device

1. Go to Firewall > Policy > Policy.
2. Select Create New.
3. Configure the external to internal firewall policy.

   Source Interface/Zone
   Select the name of the interface that connects to the Internet.

   Source Address
   Select All.

   Destination Interface/Zone
   Select the name of the interface of the NAT device that connects to the internal network.

   Destination Address
   Select the virtual IP added to the NAT device.

   Schedule
   Select Always.

   Service
   Select ANY.

   Action
   Select Accept.

   NAT
   Select NAT.

4. Select OK.

Verify that push updates to the unit on the internal network are working by going to System > Maintenance > FortiGuard and selecting Test Availability under Web Filtering and AntiSpam Options. The Push Update indicator should change to green.
Advanced

The Advanced menu allows you to configure and upload script files, configure settings for the USB Auto-install feature, and download the debug log.

Scripts are text files containing CLI command sequences. These can be uploaded and executed to run complex command sequences easily. Scripts can be used to deploy identical configurations to many devices. For example, if all of your devices use identical administrator admin profiles, you can enter the commands required to create the admin profiles in a script, and then deploy the script to all the devices which should use those same settings.

If you are using a FortiGate unit that is not remotely managed by a FortiManager unit or the FortiGuard Analysis & Management Service, the scripts you upload are executed and discarded. If you want to execute a script more than once, you must keep a copy on your management PC.

If your FortiGate unit is configured to use a FortiManager unit, you can upload your scripts to the FortiManager unit, and run them from any FortiGate unit configured to use the FortiManager unit. If you upload a script directly to a FortiGate unit, it is executed and discarded.

If your unit is configured to use the FortiGuard Analysis & Management Service, scripts you upload are executed and stored. You can run uploaded scripts from any unit configured with your FortiGuard Analysis & Management Service account. The uploaded script files appear on the FortiGuard Analysis & Management Service portal web site.

After executing scripts, you can view the script execution history on the script page. The list displays the last 10 executed scripts.

Configure settings for scripts, the USB auto-install, or download the debug log in System > Maintenance > Advanced using the following table.

### Advanced page
Lists all settings for configuring scripts, USB-Auto install, and download the debug log.

### Scripts section
Provides settings for uploading script files. You can also view script execution history from this section.

**Execute Script from**
Scripts can be uploaded directly to the unit from the management PC. If you have configured either a FortiManager unit or the FortiGuard Analysis & Management Service, scripts that have been stored remotely can also be run on the FortiGate unit.

**Upload Bulk CLI Command File**
Select Browse to locate the script file and then select Apply to upload and execute the file.
If the unit is configured to use the FortiGuard Analysis & Management Service, the script will be saved on the server for later use.

**Select From remote management station**
Select to execute a script from the FortiManager unit or the FortiGuard Analysis & Management Service. Choose the script you want to run from the list of all scripts stored remotely.

**Script Execution History**
A list of the 10 most recently executed scripts.

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the script file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The source of the script file. A local file is uploaded directly to the FortiGate unit from the management PC and executed. A remote file is executed on the FortiGate unit after being sent from a FortiManager unit or the FortiGuard Analysis &amp; Management Service.</td>
</tr>
<tr>
<td>Time</td>
<td>The date and time the script file was executed.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the script file, if its execution succeeded or failed.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the script entry from the list.</td>
</tr>
</tbody>
</table>
Creating script files

Script files are text files with CLI command sequences. When a script file is uploaded to a unit, the commands are executed in sequence.

To create a script file

1. Open a text editor application. Notepad on Windows, GEdit on Linux, Textedit on the Mac, or any editor that will save plain text can create a script file.

2. Enter the CLI commands you want to run.
   The commands must be entered in sequence, with one command per line.

3. Save the file to your maintenance PC.

   Tip: An unencrypted configuration file uses the same structure and syntax as a script file. You can save a configuration file and copy the required parts to a new file, making any edits you require. You can generate script files more quickly this way.

Uploading script files

Caution: Commands that require the unit to reboot when entered in the command line will also force a reboot if included in a script.

After you have created a script file, you can then upload it through System > Maintenance > Advanced. When a script is uploaded, it is automatically executed.

To execute a script

1. Go to System > Maintenance > Advanced.

2. Verify that Upload Bulk CLI Command File is selected.

3. Select Browse to locate the script file.

4. Select Apply.

If the unit is not configured for remote management, or if it is configured to use a FortiManager unit, uploaded scripts are discarded after execution. Save script files to your management PC if you want to execute them again later.

If the unit is configured to use the FortiGuard Analysis & Management Service, the script file is saved to the remote server for later reuse. You can view the script or run it from the FortiGuard Analysis & Management Service portal web site.
Adding VDOM Licenses

Caution: Back up current configuration settings before upgrading VDOM licenses to ensure these settings are not lost. Use one of the procedures in “Backing up your configuration” on page 161 to properly back up your current configuration.

If you have you can increase the maximum number of VDOMs on your unit you can purchase a license key from Fortinet to increase the maximum number of VDOMs to 25, 50, 100 or 250. By default, units support a maximum of 10 VDOMs.

The license key is a 32-character string supplied by Fortinet. Fortinet requires the serial number of the unit to generate the license key.

The license key is entered in System > Maintenance > License in the Input License Key field. This appears only on high-end models.

License page
Displays the current maximum number of virtual domains allowed on the FortiGate unit as well as a field for inputting a license key to add more virtual domains.

Current License The current maximum number of virtual domains.
Input License key Enter the license key supplied by Fortinet and select Apply.

Note: VDOMs created on a registered FortiGate unit are recognized as real devices by any connected FortiAnalyzer unit. The FortiAnalyzer unit includes VDOMs in its total number of registered devices. For example, if three FortiGate units are registered on the FortiAnalyzer unit and they contain a total of four VDOMs, the total number of registered FortiGate units on the FortiAnalyzer unit is seven.

Disk

You can view the status of each available local disk on your unit from System > Maintenance > Disk. The Disk menu allows you to view the amount of storage space that is currently left as well as what has been stored on and how much storage space that data is taking up. This menu provides detailed information about that storage space for each of the following:

- Disk logging
- SQL database
- Historic reports
- IPS Packet archives
- Quarantine
- WAN optimization and Web Cache

The Disk menu also provides information about quota usage, for each of the above features. The Disk menu appears only on models with multiple disks.

Disk page
Displays the detailed information about the status of each disk and how each disk is managing the storage of the information on the disk. You can view the storage of information for each feature in the Disk Management section of this page.

Disk Status section
Displays a pie chart explaining the storage space on the disk. There is a pie chart for each disk currently installed on that unit.

# The order of the disk within the list.
Name The name of the disk, such as internal.
Total The total amount of disk space available on that disk.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Used</strong></td>
<td>The total amount of space that is already used on the disk.</td>
</tr>
<tr>
<td><strong>Free</strong></td>
<td>The total amount of space that is available for storage. You can select Format to format the disk; however, formatting the disk will remove all data from the disk.</td>
</tr>
</tbody>
</table>

**Disk Management section**
Provides detailed information about how much disk space is used, free space that is available, and quota usage.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Feature</strong></td>
<td>The feature that will be storing information on the disk. The following are the available features:</td>
</tr>
<tr>
<td></td>
<td>• Disk logging</td>
</tr>
<tr>
<td></td>
<td>• DLP archive</td>
</tr>
<tr>
<td></td>
<td>• Historic reports</td>
</tr>
<tr>
<td></td>
<td>• IPS Packet archive</td>
</tr>
<tr>
<td></td>
<td>• Quarantine</td>
</tr>
<tr>
<td></td>
<td>• SQL Database</td>
</tr>
<tr>
<td></td>
<td>• WAN optimization and Web Cache</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Storage Size</th>
<th>The size of the storage space on the disk.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocated</td>
<td>The amount of space that is allowed for storage of a feature.</td>
</tr>
<tr>
<td>Used</td>
<td>The current amount of space that has been used to store information of a feature.</td>
</tr>
<tr>
<td>Quota Usage</td>
<td>The quota amount that is currently being used. This number is in percent. If there is no quota being used, the number is 100 percent.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies the current amount of space that is being used.</td>
</tr>
</tbody>
</table>
Using virtual domains

This section introduces you to virtual domains on the FortiGate unit. For more information about virtual domains, including how to configure them on your unit, see the Virtual Domains chapter of the FortiOS Handbook.

If you enable VDOMs on the unit, you configure virtual domains globally for the unit. The following topics are included in this section:

- Virtual domains overview
- VDOM configuration settings
- VDOM licenses
- Global VDOM resource limits

Virtual domains overview

Virtual domains (VDOMs) is a method of dividing a unit into two or more virtual units that function as multiple independent units. A single unit is then flexible enough to serve multiple departments of an organization, separate organizations, or to act as the basis for a service provider’s managed security service.

VDOMs provide the following benefits:

- improving Transparent mode configuration
- easier administration
- continued security
- savings in physical space and power
- more flexible MSSP configurations

The unit automatically contains a default VDOM, called root. The root VDOM is the VDOM where your current configuration is, when you first start configuring settings on your unit. The root VDOM is always there in the background and is indicated in the vd field of a log message when there are no VDOMs configured. The root VDOM must be there because the unit needs a management VDOM for management traffic, among other things.

VDOMs are essentially the same as your regular unit for menu configuration, CLI command structure, and generated task flow, there are some small differences. For example, you may not be able to access log messages within the global VDOM, but can within each configured VDOM.

This topic contains the following:

- VDOMs and global settings
- Switching between VDOMs
- Per-VDOM configurations
- Global configurations
VDOMs and global settings

A VDOM is not useful unless it contains at least two physical interfaces or virtual subinterfaces for incoming and outgoing traffic. Availability of the associated tasks depends on the permissions of the admin. If your are using a super_admin profile account, you can perform all tasks. If you are using a regular admin account, the tasks available to you depend on whether you have read only or read/write permissions. The following table shows what roles can perform which tasks.

Table 19: Admin VDOM permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Regular administrator account</th>
<th>Super_admin profile administrator account</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Read only permission</td>
<td>Read/write permission</td>
</tr>
<tr>
<td>View global settings</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Configure global settings</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Create or delete VDOMs</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Configure multiple VDOMs</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Assign interfaces to a VDOM</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Create VLANs</td>
<td>no</td>
<td>yes - for 1 VDOM</td>
</tr>
<tr>
<td>Assign an administrator to a VDOM</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Create additional admin accounts</td>
<td>no</td>
<td>yes - for 1 VDOM</td>
</tr>
<tr>
<td>Create and edit profiles</td>
<td>no</td>
<td>yes - for 1 VDOM</td>
</tr>
</tbody>
</table>

Switching between VDOMs

You can easily switch between VDOMs using the Current VDOM menu that appears after you have enabled VDOMs on your FortiGate unit. The Current VDOM menu contains a drop-down list which is located beside the menu’s name. The drop-down list contains all VDOMs that you created, including the default root VDOM and Global.

To switch to another VDOM, in the Current VDOM menu, select the VDOM that you want to switch to from the drop-down list. You are automatically redirected to that VDOM within the web-based manager.

Per-VDOM configurations

Settings that are configured within a VDOM are called VDOM settings. These settings affect only that specific VDOM and include areas such as operating mode, routing, firewall, VPN, some antivirus, logging, and reporting.

Global configurations

Settings that are configured outside of a VDOM are called global settings. These settings affect the entire FortiGate unit and include areas such as interfaces, HA, maintenance, some antivirus, and some logging. In general, any unit settings that should only be changed by the top level administrator, are global settings.

The following configuration settings affect all virtual domains. When virtual domains are enabled, only accounts with the default super_admin profile can access global settings.

The following are global VDOM configurations that you can access within the global VDOM.
**VDOM configuration settings**

Settings that are configured within a VDOM are called VDOM settings. These settings affect only that specific VDOM and include areas such as operating mode, routing, firewall, VPN, some antivirus, logging, and reporting.

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 menu appears called Current VDOM, which you can use to go from VDOM to VDOM. For more information, see “Switching between VDOMs” on page 156.
- A new VDOM entry appears under the System option.
- Within a VDOM, reduced dashboard menu options are available, and a new Global option appears. Selecting Global exits the current VDOM.
- There is no operation mode option at the Global level.
- Only super_admin profile accounts can view or configure Global level options.
- Super_admin profile accounts can configure configurations for all VDOM.
- One or more administrators can be configured for each VDOM; however, these admin accounts cannot edit settings for any VDOMs for which they are not configured.

When virtual domains are enabled, the current virtual domain is displayed at the bottom left of the screen, in the format Current VDOM: <name of the virtual domain>.

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

VDOMs are configured in System > VDOM > VDOM. Use the following table when configuring VDOMs.

<table>
<thead>
<tr>
<th>VDOM page</th>
<th>Lists all the VDOMs you configured. On this page, you can edit, delete or create a new VDOM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new VDOM. When you select Create New, you are automatically redirected to the New Virtual Domain page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies a VDOM’s settings.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a VDOM from the VDOM page.</td>
</tr>
<tr>
<td>Switch Management [current vdom name]</td>
<td>Select to switch to a VDOM and make it the management VDOM.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the VDOM.</td>
</tr>
<tr>
<td>Operation Mode</td>
<td>The type of operation mode that the VDOM is in. This mode is either NAT or Transparent.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>The interfaces associated with the VDOM.</td>
</tr>
<tr>
<td>Enable</td>
<td>Indicates whether the VDOM is enabled or disabled. A green check mark indicates that the VDOM is enabled. A gray x indicates that the VDOM is disabled.</td>
</tr>
<tr>
<td>Comments</td>
<td></td>
</tr>
</tbody>
</table>

New Virtual Domain page

Provides settings for configuring a virtual domain.

| Name | Enter a name for the virtual domain. For example, vdom_1 |
VDOM licenses

Caution: Back up current configuration settings before upgrading VDOM licenses to ensure these settings are not lost. Use one of the procedures in “Backing up your configuration” on page 161 to properly back up your current configuration.

All units, except the FortiGate-30B, support 10 VDOMs by default. If you do not have the path System > Maintenance > License, your FortiGate model does not support more than 10 VDOMs.

High-end models support the purchase of a VDOM license key from customer service to increase their maximum allowed VDOMs to 25, 50, 100, 250, or 500. Configuring 250 or more VDOMs will result in reduced system performance.

Your unit has limited resources that are divided amongst all configured VDOMs. These resources include system memory and CPU. When running 250 or more VDOMs, you cannot run Unified Threat Management (UTM) features such as proxies, web filtering, or antivirus—your unit can only provide basic firewall functionality.

The VDOMs that are created on a registered unit are recognized as real devices by connected FortiAnalyzer units. FortiAnalyzer units include VDOMs in their total number of registered devices. For example, if three FortiGate units are registered on a FortiAnalyzer unit and they contain a total of four VDOMs, the total number of registered FortiGate units on the FortiAnalyzer unit is seven units. For more information, see the FortiAnalyzer Administration Guide.

Table 20: VDOM support by FortiGate model

<table>
<thead>
<tr>
<th>FortiGate model</th>
<th>Support VDOMs</th>
<th>Default VDOM maximum</th>
<th>Maximum VDOM license</th>
</tr>
</thead>
<tbody>
<tr>
<td>30B</td>
<td>no</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Low and mid-range models</td>
<td>yes</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>High-end models</td>
<td>yes</td>
<td>10</td>
<td>500</td>
</tr>
</tbody>
</table>

Global VDOM resource limits

Super administrators can configure VDOM resource limits to control how many resources each VDOM can use. This means you can provide tiered services for different VDOMs. You can also use resource limits to share resources evenly among VDOMs, preventing one VDOM from affecting the performance of others.

You can set limits for dynamic and some static resources. Dynamic resources are resources that are not controlled by the FortiGate configuration. You can limit dynamic resources to limit the amount of traffic that a VDOM processes and so limit the amount of FortiGate processing resources the VDOM can use. If you do not limit the number of dynamic resources each VDOM will use as many as it can until the capacity of the unit becomes the limiting factor. You can set the following dynamic resource limits:

- The total number of communication Sessions that can be started in a VDOM. When this limit is reached additional sessions are dropped.
• The number of IPSec VPN Dal-up Tunnels that can be started in a VDOM. When this limit is reached, additional tunnels are dropped.

• The number of SSL VPN user sessions that can be started in a VDOM. When this limit is reached the VDOM displays a system busy message instead of the login page when a user attempts to login to start an SSL VPN session.

Static resources are controlled by limits in the FortiGate configuration. These limits vary by model and are listed in the FortiGate Maximum Values Matrix. Limiting static resources does not limit the amount of traffic that the VDOM process. Instead limiting static resources controls the number of configuration elements that can be added to a VDOM.

You can set the following static resource limits:

• The number of VPN IPSec Phase 1 and Phase 2 tunnels that can be added to a VDOM configuration. The number of tunnels is limited by the maximum values for the model.

• The number of Firewall policies, Firewall Addresses, Firewall Address Groups, Firewall Custom Services, Firewall Service Groups, Firewall One-Time Schedules, and Firewall Recurring Schedules that can be added to a VDOM configuration.

• The number of Local Users and User Groups that can be added to a VDOM configuration.

Global resources are modified (as well as reset to default values) from System > VDOM > Global Resources.

Global Resources page
Lists the current resources that are available. On this page, you can only modify global resources or reset them to default settings.

Edit               Modifies a resource within the list.
Reset to default value   Resets the resource or resources within the list, to default settings.
Configured Maximum   The currently configured maximum for this resource.
Default Maximum      The factory configured maximum value for this resource. This number cannot be changed.
Current Usage        The amount of this resource that is currently being used. This value is useful for determining when and if you may need to adjust this value for some resources on your FortiGate unit.

Edit Global Resource Limits
Allows you to change the default global resource limits.

Sessions               Enter the number of sessions that will be applied to the resource.

Global resource usage for individual VDOMs
You can configure resource usage for individual VDOMS to override global limits and specify guaranteed usage for that VDOM.

When you add a new VDOM, after giving the VDOM a name and selecting OK you can configure resource usage for the VDOM. You can also configure resource usage for a VDOM at any time by going to System > VDOM > VDOM and editing a VDOM.

When configuring resource usage for a VDOM you can set the Maximum and Guaranteed value for each resource.
Global VDOM resource limits

Using virtual domains

• The **Maximum** value limits the amount of the resource that can be used by the VDOM. When you add a VDOM, all maximum resource usage settings are 0, indicating that resource limits for this VDOM are controlled by the global resource limits. You do not have to override the maximum settings unless you need to override global limits to further limit the resources available for the VDOM. You cannot set maximum resource usage higher in a VDOM than the corresponding global resource limit. To set global resource limits go to **System > VDOM > Global Resources**.

• The **Guaranteed** value represents the minimum amount of the resource available for that VDOM. Setting the guaranteed value makes sure that other VDOMs do not use all of a resource. A guaranteed value of 0 means that an amount of this resource is not guaranteed for this VDOM. You only have to change guaranteed settings if your FortiGate may become low on resources and you want to guarantee that a minimum level is available for this VDOM.

 resource usage section on the edit virtual domain page (System > VDOM > VDOM)

<table>
<thead>
<tr>
<th>Resource</th>
<th>Name of the resource. Includes dynamic and static resources.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>Override the global limit to reduce the amount of each resource available for this VDOM. The maximum must the same as or lower than the global limit. The default value is 0, which means the maximum is the same as the global limit. <strong>Note:</strong> If you set the maximum resource usage for a VDOM you cannot reduce the default maximum global limit for all VDOMs below this maximum.</td>
</tr>
<tr>
<td>Guaranteed</td>
<td>Enter the minimum amount of the resource available to this VDOM regardless of usage by other VDOMs. The default value is 0, which means that an amount of this resource is not guaranteed for this VDOM.</td>
</tr>
<tr>
<td>Current</td>
<td>The amount of the resource that this VDOM currently uses.</td>
</tr>
</tbody>
</table>
Firmware management practices

Fortinet recommends reviewing this section before upgrading because it contains important information about how to properly back up your current configuration settings and what to do if the upgrade is unsuccessful.

You should also review the What's New chapter of the FortiOS Handbook when a new firmware maintenance release is released. This chapter contains valuable information about the changes and new features that may cause issues with the current configuration.

In addition to firmware images, Fortinet releases patch releases—maintenance release builds that resolve important issues. Fortinet strongly recommends reviewing the release notes for the patch release before upgrading the firmware. Follow the steps below:

- Download and review the release notes for the patch release.
- Download the patch release.
- Back up the current configuration.
- Install the patch release using the procedure "Testing firmware before upgrading" on page 164.
- Test the patch release until you are satisfied that it applies to your configuration.

Installing a patch release without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

With FortiOS 4.0, you can also configure your unit to use NAT while in transparent mode. For more information, see the Fortinet Knowledge Center article, Configuring NAT in Transparent mode.

If you enable virtual domains (VDOMs) on the FortiGate unit, system firmware versions are configured globally. For more information, see the Virtual Domains chapter of the FortiOS Handbook.

The following topics are included in this section:

- Backing up your configuration
- Testing firmware before upgrading
- Upgrading your FortiGate unit
- Reverting to a previous firmware image
- Restoring your configuration

Backing up your configuration

Caution: Always back up your configuration before installing a patch release, upgrading/downgrading firmware, or resetting configuration to factory defaults.

You can back up configuration settings to a local PC, a FortiManager unit, FortiGuard Management server, or to a USB key. You can also back up to a FortiGuard Management server if you have FortiGuard Analysis and Management Service enabled. If you have a local hard drive, you can also back up the configuration file to it. If you have partitions enabled on the drive, any configuration files that you back up are stored on a specific partition that you have created for log and system data.
Fortinet recommends backing up all configuration settings from your unit before upgrading to FortiOS 4.0. This ensures all configuration settings are still available if you require downgrading to FortiOS 3.0 MR7 and want to restore those configuration settings.

**Backing up your configuration through the web-based manager**

You can back up your configuration to a variety of locations, such as a FortiManager unit or a FortiGuard Management server. The following procedure describes how to properly back up your current configuration in the web-based manager.

**To back up your configuration file through the web-based manager**

1. Go to *System > Dashboard*.
2. In the System Information widget, select *Backup* in the *System Configuration* line. You are automatically redirected to the Backup page.
3. Select the location where the configuration file will be stored on.
4. Select the check box beside *Encrypt configuration file* to encrypt the configuration file. If you want to encrypt your configuration file to save VPN certificates, select the *Encrypt configuration file* check box, enter a password, and then enter it again to confirm.
5. Select *Backup*.
6. Save the file.

**Backing up your configuration through the CLI**

You can back up your configuration file using a TFTP or FTP server, or the USB key. If you have the FortiGuard Analysis and Management Service configured, you can also back up your configuration to the FortiGuard Management server.

When backing up your configuration in the CLI, you can choose to back up the entire configuration (*execute backup full-config*) or part of the configuration (*execute backup config*). If you have virtual domains, there are limitations to what certain administrators are allowed to back up.

The following procedure describes how to back up your current configuration in the CLI and assumes that you are familiar with the following commands.

**To back up your configuration file through the CLI**

1. Enter the following to back up the configuration file to a USB key:
   ```bash
   execute backup config usb <backup_filename> <encrypt_passwd>
   ```
2. Enter the following to back up the configuration file to a TFTP or FTP server:
   ```bash
   execute backup config {tftp | ftp}<backup_filename> <tftp_server_ipaddress> <ftp server [:ftp port] <ftp_username> <ftp_passwd> <encrypt_passwd>
   ```
3. Enter the following to back up the configuration to a FortiGuard Management server:
   ```bash
   execute backup config management-station <comment>
   ```
To back up the entire configuration file through the CLI

Enter the following to back up the entire configuration file:

    execute backup full-config {tftp | ftp | usb} <backup_filename>
    <backup_filename> <tftp_server_ipaddress> <ftp server [:ftp port] <ftp_username> <ftp_passwd> <encrypt_passwd>

Backing up your configuration to a USB key

If your unit has a USB port, you can back up your current configuration to a USB key. When backing up a configuration file to a USB key, verify that the USB key is formatted as a FAT16 disk. The FAT16 format is the only supported partition type. For more information, see “Formatting USB Disks” on page 139.

Before proceeding, ensure that the USB key is inserted in the unit’s USB port.

To back up your configuration to the USB key

1. Go to System > Dashboard > Status.
2. In the System Information widget, select Backup in the System Configuration line. You are automatically redirected to the Backup page.
3. Select USB Disk.
   If you want to encrypt your configuration file to save VPN certificates, select the Encrypt configuration file check box, enter a password, and then enter it again to confirm.
4. Select Backup.
5. Save the file.

After successfully backing up your configuration file, either from the CLI or the web-based manager, proceed with upgrading to FortiOS 4.0.
Testing firmware before upgrading

You may want to test the firmware that you need to install before upgrading to a new firmware version, or to a maintenance or patch release. By testing the firmware, you can familiarize yourself with the new features and changes to existing features, as well as understand how your configuration works with the firmware. A firmware image is tested by installing it from a system reboot, and then saving it to system memory. After the firmware is saved to system memory, the unit operates using the firmware with the current configuration.

The following procedure does not permanently install the firmware; the next time the unit restarts, it operates using the firmware originally installed on the unit. You can install the firmware permanently by using the procedures in "Upgrading your FortiGate unit" on page 165.

You can use the following procedure for either a regular firmware image or a patch release.

The following procedure assumes that you have already downloaded the firmware image to your management computer.

To test the firmware image before upgrading

1. Copy the new firmware image file to the root directory of the TFTP server.
2. Start the TFTP server.
3. Log in to the CLI.
4. Enter the following command to ping the computer running the TFTP server:
   ```
   execute ping <server_ipaddress>
   ```
   Pinging the computer running the TFTP server verifies that the FortiGate unit and TFTP server are successfully connected.
5. Enter the following to restart the FortiGate unit:
   ```
   execute reboot
   ```
6. As the unit reboots, a series of system startup messages appears. When the following message appears, immediately press any key to interrupt the system startup:
   ```
   Press any key to display configuration menu...
   ```
   You have only three seconds to press any key. If you do not press a key soon enough, the unit reboots and you must log in and repeat steps 5 to 6 again.
   If you successfully interrupt the startup process, the following message appears:
   ```
   [G]: Get firmware image from TFTP server.
   [F]: Format boot device.
   [Q]: Quit menu and continue to boot with default firmware.
   [H]: Display this list of options.
   ```
7. Type G to get the new firmware image from the TFTP server.
   The following message appears:
   ```
   Enter TFTP server address [192.168.1.168]:
   ```
8. Type the address of the TFTP server and press Enter.
   The following message appears:
   ```
   Enter Local Address [192.168.1.188]:
   ```
9 Type the internal IP address of the unit. This IP address connects the unit to the TFTP server. This IP address must be on the same network as the TFTP server, but make sure you do not use an IP address of another device on the network.

The following message appears:

Enter File Name [image.out]:

10 Enter the firmware image file name and press Enter. The TFTP server uploads the firmware image file to the unit and the following appears:

Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]

11 Type R.

The FortiGate firmware image installs and saves to system memory. The unit starts running the new firmware image with the current configuration.

When you have completed testing the firmware, you can reboot the unit and resume using the original firmware.

Upgrading your FortiGate unit

If your upgrade is successful, and your unit has a hard drive, you can use the Boot alternate firmware option located in System > Maintenance > Backup and Restore. This option enables you to have two firmware images, such as FortiOS 3.0 MR7 and FortiOS4.0, available for downgrading or upgrading.

If the upgrade was not successful, go to “Reverting to a previous firmware image” on page 168.

You can also use the following procedure when installing a patch release. A patch release is a firmware image that resolves specific issues, but does not contain new features or changes to existing features. You can install a patch release whether or not you upgraded to the current firmware version.

Upgrading to FortiOS 4.0 through the web-based manager

Caution: Always back up your configuration before installing a patch release, upgrading/downgrading firmware, or resetting configuration to factory defaults.

The following procedure describes how to upgrade to FortiOS 4.0 in the web-based manager. Fortinet recommends using the CLI to upgrade to FortiOS 4.0. The CLI upgrade procedure reverts all current firewall configurations to factory default settings.

To upgrade to FortiOS4.0 through the web-based manager

1 Download the firmware image file to your management computer.
2 Log in to the web-based manager.
3 Go to System > Status and locate the System Information widget.
4 Beside Firmware Version, select Update.
5 Enter the path and filename of the firmware image file, or select Browse and locate the file.
6 Select OK.

The unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process may take a few minutes.

When the upgrade is successfully installed:

- ping to your unit to verify there is still a connection.
- clear the browser’s cache and log in to the web-based manager.

After logging back in to the web-based manager, you should save the configuration settings that carried forward. Some settings may have carried forward from FortiOS 3.0 MR7, while others may not have, such as certain IPS group settings. Go to System > Maintenance > Backup and Restore to save the configuration settings that carried forward.

Note: After upgrading to FortiOS 4.0, perform an “Update Now” to retrieve the latest FortiGuard signatures from the FortiGuard Distribution Network (FDN) as these signatures included in the firmware may be older than those currently available on the FDN.

Upgrading to FortiOS 4.0 through the CLI

Caution: Always back up your configuration before installing a patch release, upgrading/downgrading firmware, or resetting configuration to factory defaults.

The following procedure uses a TFTP server to upgrade the firmware. The CLI upgrade procedure reverts all current firewall configurations to factory default settings.

See the Fortinet Knowledge Base article, Loading FortiGate firmware using TFTP, for additional information about upgrading firmware in the CLI.

The following procedure assumes that you have already downloaded the firmware image to your management computer.

To upgrade to FortiOS 4.0 through the CLI

1 Copy the new firmware image file to the root directory of the TFTP server.
2 Start the TFTP server.
3 Log in to the CLI.
4 Enter the following command to ping the computer running the TFTP server:
   execute ping <server_ipaddress>
   Pinging the computer running the TFTP server verifies that the unit and TFTP server are successfully connected.
5 Enter the following command to copy the firmware image from the TFTP server to the unit:
   execute restore image <name_str> <tftp_ipv4>
   Where <name_str> is the name of the firmware image file and <tftp_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is image.out and the IP address of the TFTP server is 192.168.1.168, enter:
   execute restore image.out 192.168.1.168
   The unit responds with a message similar to the following:
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
6 Type y.
   The unit uploads the firmware image file, upgrades to the new firmware version, and
   restarts. This process takes a few minutes.

7 Reconnect to the CLI.

8 Enter the following command to confirm the firmware image installed successfully:
   get system status

9 To update antivirus and attack definitions from the CLI, enter the following:
   execute update-now

   If you want to update antivirus and attack definitions from the web-based manager
   instead, log in to the web-based manager and go to System > Maintenance >
   FortiGuard.

Verifying the upgrade

After clearing your browser’s cache and then logging back in to the web-based manager,
most of your previous configuration settings have been carried forward. For example, if
you go to System > Network > Options you can see your DNS settings carried forward
from your previous configuration settings.

You should verify what configuration settings carried forward. You should also verify that
administrative access settings carried forward as well. Verifying your configuration
settings allows you to familiarize yourself with the new features and changes in FortiOS
4.0.

You can verify your configuration settings by:
   • going through each menu and tab in the web-based manager
   • using the show shell command in the CLI.
Reverting to a previous firmware image

You may need to revert to a previous firmware image (or version, for example, FortiOS 3.0) if the upgrade was not successfully installed. The following procedures describe how to properly downgrade to a previous firmware image using either the web-based manager or CLI, and include steps on how to restore your previous configuration.

The following are included in this topic:
- Downgrading to a previous firmware through the web-based manager
- Downgrading to a previous firmware through the CLI
- Restoring your configuration

Downgrading to a previous firmware through the web-based manager

Caution: Always back up your configuration before installing a patch release, upgrading/downgrading, or when resetting to factory defaults.

When downgrading to a previous firmware, only the following settings are retained:
- operation mode
- Interface IP/Management IP
- route static table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system accprofiles.

If you created additional settings in FortiOS 4.0, make sure to back up the current configuration before downgrading. For more information, see “Backing up your configuration” on page 161.

To downgrade through the web-based manager

1. Go to System > Dashboard > Status and locate the System Information widget.
3. Enter the path and filename of the firmware image file, or select Browse and locate the file.
4. Select OK.
   The following message appears:
   This version will downgrade the current firmware version. Are you sure you want to continue?
5. Select OK.
   The 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.
6. Log in to the web-based manager.
   Go to System > Dashboard > Status to verify that the firmware version under System Information has changed to the correct firmware.
Verifying the downgrade

After successfully downgrading to a previous firmware, verify your connections and settings. If you are unable to connect to the web-based manager, make sure your administration access settings and internal network IP address are correct. The downgrade may change your configuration settings to default settings.

Downgrading to a previous firmware through the CLI

Caution: Always back up your configuration before installing a patch release, upgrading/downgrading, or when resetting to factory defaults.

When downgrading to a previous firmware, only the following settings are retained:

- operation mode
- Interface IP/Management IP
- route static table
- DNS settings
- VDOM parameters/-settings
- admin user account
- session helpers
- system accprofiles.

If you have created additional settings in FortiOS 4.0, make sure you back up your configuration before downgrading. For more information, see "Backing up your configuration" on page 161.

The following procedure assumes that you have already downloaded the firmware image to your management computer.

To downgrade through the CLI

1. Copy the new firmware image file to the root directory of the TFTP server.
2. Start the TFTP server.
3. Log in to the CLI.
4. Enter the following command to ping the computer running the TFTP server:
   ```
   execute ping <server_ipaddress>
   ```

   Pinging the computer running the TFTP server verifies that the FortiGate unit and TFTP server are successfully connected.

5. Enter the following command to copy the firmware image from the TFTP server to the unit:
   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is `192.168.1.168`, enter:
   ```
   execute restore image tftp image.out 192.168.1.168
   ```

   The unit responds with the message:
   ```
   This operation will replace the current firmware version! Do you want to continue? (y/n)
   ```
6 Type y.

The unit uploads the firmware image file. After the file uploads, a message similar to the following is displayed:

Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)

7 Type y.

The unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.

After the unit uploads the firmware, you need to reconfigure your IP address since the unit reverts to default settings, including its default IP address. See your install guide for configuring IP addresses.

8 Reconnect to the CLI.

9 Enter the following command to confirm the firmware image installed successfully:

     get system status

See “Restoring your configuration” on page 171 to restore you previous configuration settings.
Restoring your configuration

Your configuration settings may not carry forward after downgrading to a previous firmware. You can restore your configuration settings for a previous firmware with the configuration file you saved before upgrading to FortiOS 4.0.

You can also use the following procedures for restoring your configuration after installing a current patch release or maintenance release.

Restoring your configuration settings in the web-based manager

The following procedure restores your previous firmware configuration settings in the web-based manager.

**To restore configuration settings in the web-based manager**

1. Log in to the web-based manager.
2. Go to **System > Dashboard > Status** and locate the System Information widget.
3. Select **Restore** in the System Configuration line to restore the configuration from either a **Local PC**, **FortiManager** or **FortiGuard** (if your FortiGate unit is configured for FortiGuard Analysis and Management Service).
   - You are automatically redirected to the Restore page.
4. Enter the location of the file or select **Browse** to locate the file.
   - If required, enter your password for the configuration file.
5. Select **Restore**.
   - The unit restores the configuration settings. This may take a few minutes since the unit will reboot.
   - You can verify that the configuration settings are restored by logging in to the web-based manager and going through the various menus and tabs.

Restoring your configuration settings in the CLI

The following procedure restores your previous firmware configuration settings in the CLI.

**To restore configuration settings in the CLI**

1. Copy the backed-up configuration file to the root directory of the TFTP server.
2. Start the TFTP server.
3. Log in to the CLI.
4. Enter the following command to ping the computer running the TFTP server:
   ```
   execute ping <server_ipaddress>
   ```
   - Pinging the computer running the TFTP server verifies that the unit and TFTP server are successfully connected.
5 Enter the following command to copy the backed-up configuration file to restore the file on the unit:

```
execute restore allconfig <name_str> <tftp_ipv4> <password>
```

Where `<name_str>` is the name of the backed up configuration file and `<tftp_ipv4>` is the IP address of the TFTP server and `<password>` is the password you entered when you backed up your configuration settings. For example, if the backed up configuration file is `confall` and the IP address of the TFTP server is `192.168.1.168` and the password is `ghrffdt123`:

```
execute restore allconfig confall 192.168.1.168 ghrffdt123
```

The unit responds with the message:

```
This operation will overwrite the current settings and the system will reboot!
Do you want to continue? (y/n)
```

6 Type `y`.

The unit uploads the backed up configuration file. After the file uploads, a message, similar to the following, is displayed:

```
Getting file confall from tftp server 192.168.1.168
##
Restoring files...
All done. Rebooting...
```

This may take a few minutes.

Use the CLI `show shell` command to verify your settings are restored, or log in to the web-based manager.
Router

This section introduces you to the Router menu. If you require more information about the features in the Routing menu, see the FortiOS Handbook.

This section contains the following topics:

- Static
- Dynamic
- Monitor

Static

The Static menu provides settings for configuring both static and policy routes. A route provides the 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. A policy route allows you to redirect traffic away from a static route, and can be useful when you want to route certain type of network traffic differently.

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 unit, or delete the factory configured route and specify your own static default route that points to the default gateway for the unit.

Static routes are defined manually and control traffic exiting from the unit—you can specify through which interface the packet will leave and to which device the packet should be routed.

Route policies or policy routes, specify additional criteria for examining the properties of incoming packets. Using route policies, you can configure the unit to route packets based on the IP source and destination addresses in packet headers and other criteria such as on which interface the packet was received and which protocol (service) and port are being used to transport the packet.

The following topics are included in this section:

- Static Route
- ECMP route failover and load balancing
- Policy Route

Static Route

Static routes are configured by defining the destination IP address and netmask of packets that you intend the unit to intercept, and by specifying a (gateway) IP address for those packets. The gateway address specifies the next-hop router to which traffic will be routed.

The Static Route page displays a list of routes that the unit compares to packet headers in order to route packets. Initially, the list contains the factory configured static default route. For more information, see “Default route and default gateway” on page 175. You can add new entries manually.
When you add a static route to the Static Route list, the unit performs a check to determine whether a matching route and destination already exist in the FortiGate routing table. If no match is found, the unit adds the route to the routing table.

When IPv6 is enabled in the web-based manager, IPv6 routes are visible on the Static Route list and you can select IPv6 when creating a new static route. Otherwise, IPv6 routes are not displayed.

Configure static routes in Router > Static > Static Route using the following table.

<table>
<thead>
<tr>
<th><strong>Static Route page</strong></th>
<th>Lists all the static routes that you created, including the default static route. On this page, you can edit, delete or create a new static route.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create New</strong></td>
<td>Creates a new static route. When you select Create New, you are automatically redirected to the New Static Route page. If you are configuring IPv6 addresses, select the down arrow beside Create New to create an IPv6 static Route.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Modifies settings within a static route. When you select Edit, you are automatically redirected to the Edit Static Route page.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Removes a static route from within the list on the Static Route page. To remove multiple static routes in the list, on the Static Route page, in each of the rows of the routes you want removed, select the check box and then select Delete. To remove all static routes in the list, on the Static Route page, select the check box in the check box column, and then select Delete.</td>
</tr>
<tr>
<td><strong>ECMP Route Failover &amp; Load Balance Method</strong></td>
<td>Select the load balancing and failover method for ECMP routes. See “ECMP route failover and load balancing” on page 177.</td>
</tr>
<tr>
<td><strong>Source based</strong></td>
<td>The unit load balances sessions among ECMP routes based on the source IP address of the sessions to be load balanced. This is the default load balancing method. No configuration changes are required to support source IP load balancing.</td>
</tr>
<tr>
<td><strong>Weighted</strong></td>
<td>The unit load balances sessions among ECMP routes based on weights added to ECMP routes. More traffic is directed to routes with higher weights. After selecting weight-based you must add weights to static routes. For more information, see “Configuring weighted static route load balancing” on page 181.</td>
</tr>
<tr>
<td><strong>Spill-over</strong></td>
<td>The unit distributes sessions among ECMP routes based on how busy the FortiGate interfaces associated with the routes are. After selecting Spill-over you add route Spillover Thresholds to interfaces added to ECMP routes. For more information, see “ECMP route failover and load balancing” on page 177. The unit sends all ECMP-routed sessions to the lowest numbered interface until the bandwidth being processed by this interface reaches its spillover threshold. The unit then spills additional sessions over to the next lowest numbered interface. For more information, including the order in which interfaces are selected, see “Configuring spill-over or usage-based ECMP” on page 178.</td>
</tr>
<tr>
<td><strong>Apply</strong></td>
<td>Select to save the ECMP Route Failover and load balance method.</td>
</tr>
<tr>
<td><strong>Route</strong></td>
<td>Select the Expand Arrow to display or hide the IPv4 static routes. By default these routes are displayed. This is displayed only when IPv6 is enabled in the web-based manager.</td>
</tr>
<tr>
<td><strong>IPv6 Route</strong></td>
<td>Select the Expand Arrow to display or hide the IPv6 static routes. By default these routes are hidden. This is displayed only when IPv6 is enabled in the web-based manager.</td>
</tr>
<tr>
<td><strong>IP/Mask</strong></td>
<td>The destination IP addresses and network masks of packets that the FortiGate unit intercepts.</td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td>The IP addresses of the next-hop routers to which intercepted packets are forwarded.</td>
</tr>
</tbody>
</table>
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 unit, the factory configured static default route causes the 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 unit, or delete the factory configured route and specify your own static default route that points to the default gateway for the unit.

For example, Figure 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.

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 (in this example “external”).
- Distance: 10

The Gateway setting specifies the IP address of the next-hop router interface to the FortiGate external interface. The interface connected to the router (192.168.10.1) is the default gateway for FortiGate_1.

<table>
<thead>
<tr>
<th>Device</th>
<th>The names of the FortiGate interfaces through which intercepted packets are received and sent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distance</td>
<td>The administrative distances associated with each route. The values represent distances to next-hop routers.</td>
</tr>
<tr>
<td>Weight</td>
<td>If ECMP Route Failover &amp; Load Balance Method is set to weighted, add weights for each route. Add higher weights to routes that you want to assign more sessions to when load balancing. For more information, see “Configuring weighted static route load balancing” on page 181.</td>
</tr>
</tbody>
</table>

**New Static Route page**

Provides settings for defining the destination IP address and netmask of packets that you intend the FortiGate unit to intercept, and by specifying a (gateway) IP address for those packets

**Destination IP/Mask** Enter the destination IP address and netmask of the packets that you intend the FortiGate unit to intercept.

**Device** Select the interface through which intercepted packets are received and sent.

**Gateway** Enter the gateway IP address for those packets that you intend the FortiGate unit to intercept.

**Distance** Enter the number that represents the distances to the next-hop routers.

**Priority** Enter the number for the priority of the static route.

**Note:** Unless otherwise specified, static route examples and procedures are for IPv4 static routes.

You can use the config router static6 CLI command to add, edit, or delete static routes for IPv6 traffic.

---

FortiGate Version 4.0 MR2 Administration Guide
01-420-89802-20101126
http://docs.fortinet.com/ • Feedback
In some cases, there may be routers behind the 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, the 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. Also firewall policies must be configured to allow traffic to pass through the unit along these routes. For more information, see “Policy” on page 203.

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 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 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.

If you are using DHCP or PPPoE over a modem interface on your unit, you may have problems configuring a static route on this interface. After trying to either renew your DHCP license, or reconnect the PPPoE connection, go to the CLI and enable `dynamic-gateway` under `config system interface` for the modem interface. This will remove the need to specify a gateway for this interface’s route.

**Note:** For network traffic to pass, even with the correct routes configured, you must have the appropriate firewall policies. For more information, see “Policy” on page 203.

### To change the gateway for the default route

1. Go to `Router > Static > Static Route`.
2. Edit the row 1.
3. If the unit reaches the next-hop router through an interface other than the interface that is currently selected in the `Device` field, select the name of the interface from the `Device` field.
4. In the `Gateway` field, type the IP address of the next-hop router to which outbound traffic may be directed.
5. In the `Distance` field, optionally adjust the administrative distance value. The default route distance should be set high enough to allow other routes to be configured at lower distances so they will be preferred over the default route.
6. Select OK.
Adding a static route to the routing table

Static routes are defined manually. They control traffic exiting the 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

1. Go to Router > Static > Static Route.
2. Select Create New.
3. Enter the IP address and netmask in the Destination IP/ Mask field.
   For example, 172.1.2.0/255.255.255.0 would be a route for all addresses on the subnet 172.1.2.x.
4. Enter the unit's interface that is closest to this subnet, or connected to it, from the Device drop-down list.
5. Enter the gateway IP address in the Gateway field.
   Continuing with the example, 172.1.2.11 would be a valid address.
6. Enter the administrative distance of this route in the Distance field and then entry the priority in the Priority field.
   The administrative distance allows you to weight one route to be preferred over another. This is useful when one route is unreliable. For example, if route A has an administrative distance of 30 and route B has an administrative distance of 10, the preferred route is route A with the smaller administrative distance of 10. If you discover that route A is unreliable, you can change the administrative distance for route A from 10 to 40, which will make the route B the preferred route.
7. Select OK to confirm and save your new static route.

When you add a static route through the web-based manager, the unit adds the entry to the Static Route list.

ECMP route failover and load balancing

FortiOS uses equal-cost multi-path (ECMP) to distribute traffic to the same destination such as the Internet or another network. By using ECMP, you can add multiple routes to the same destination and give each of those routes the same distance and priority.

However, if multiple routes to the same destination have the same priority but different distances, the route with the lowest distance is used. If multiple routes to the same destination have the same distance but different priorities, the route with the lowest priority is used. Distance takes precedence over priority. If multiple routes to the same destination have the different distances and different priorities, the route with the lowest distance is always used even if it has the highest priority.

By using ECMP, if more than one ECMP route is available you can configure how the unit selects the route to be used for a communication session. If only one ECMP route is available (for example, because an interface cannot process traffic because interface status detection does not receive a reply from the configured server) then all traffic uses this route.

Previous versions of FortiOS provided source IP-based load balancing for ECMP routes. FortiOS 4.0 MR1 includes three configuration options for ECMP route failover and load balancing:
You can configure only one of these ECMP route failover and load balancing methods in a single VDOM. If your unit is configured for multiple VDOM operation, each VDOM can have its own ECMP route failover and load balancing configuration.

To configure the ECMP route failover and load balancing method from the web-based manager

1. Go to **Router > Static > Static Route**.
2. Set **ECMP Route failover & Load Balance Method** to source based, weighted, or spill-over.
3. Select Apply.

To configure the ECMP route failover and load balancing method from the CLI

Enter the following command:
```
config system settings
  set v4-ecmp-mode {source-ip-based | usage-based | weight-based}
end
```

ECMP routing of simultaneous sessions to the same destination IP address

When the unit selects an ECMP route for a session, a route cache is created that matches the route with the destination IP address of the session. All new sessions to the same destination IP address use the same route until the route is flushed from the cache. Routes are flushed from the cache after a period of time when no new sessions to the destination IP address are received.

The route cache improves FortiGate routing performance by reducing how often the unit looks up routes in the routing table.

If the unit receives a large number of sessions with the same destination IP address, because all of these sessions will be processed by the same route, it may appear that sessions are not distributed according to the ECMP route failover and load balancing configuration.

Configuring spill-over or usage-based ECMP

The spill-over or usage-based ECMP method routes new sessions to interfaces that have not reached a configured bandwidth limit (called the Spillover Threshold or a route-spillover threshold). To configure spill-over or usage-based ECMP routing, you enable spill-over ECMP method, add ECMP routes, and add a Spillover Threshold to the interfaces used by the ECMP routes. Set the Spillover Thresholds to limit the amount of bandwidth processed by each interface.

With spill-over ECMP routing configured, the unit routes new sessions to an interface used by an ECMP route until that interface reaches its Spillover Threshold. Then, when the threshold of that interface is reached, new sessions are routed to one of the other interfaces used by the ECMP routes.

Use the following procedure to enable usage based ECMP routing, add Spillover Thresholds to FortiGate interfaces port3 and port4, and then to configure EMCP routes with device set to port3 and port4.

To add Spillover Thresholds to interfaces from the web-based manager

1. Go to **Router > Static > Static Route**.
2 Set ECMP Route failover & Load Balance Method to usage-based.
3 Go to Router > Static > Static Route.
4 Add ECMP routes for port3 and port4.

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>Device</th>
<th>Gateway</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.0/24</td>
<td>port3</td>
<td>172.20.130.3</td>
<td>9</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>port4</td>
<td>172.20.140.4</td>
<td>9</td>
</tr>
</tbody>
</table>

5 Go to System > Network > Interface.
6 Edit port3 and port4 and add the following spillover-thresholds:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Spillover Threshold (KBps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>port3</td>
<td>100</td>
</tr>
<tr>
<td>port4</td>
<td>200</td>
</tr>
</tbody>
</table>

7 Go to Router > Monitor > Routing Monitor to view the routing table. The routes could be displayed in the order shown in Table 21.

Table 21: Example ECMP routes as listed on the routing monitor

<table>
<thead>
<tr>
<th>Type</th>
<th>Network</th>
<th>Distance</th>
<th>Metric</th>
<th>Gateway</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>192.168.20.0/24</td>
<td>9</td>
<td>0</td>
<td>172.20.130.3</td>
<td>port3</td>
</tr>
<tr>
<td>Static</td>
<td>192.168.20.0/24</td>
<td>9</td>
<td>0</td>
<td>172.20.140.4</td>
<td>port4</td>
</tr>
</tbody>
</table>

In this example, the unit sends all sessions to the 192.168.20.0 network through port3. When port3 exceeds its spillover threshold of 100 KBps the unit sends all new sessions to the 192.168.20.0 network through port4.

To add route-spillover thresholds to interfaces from the CLI

1 Enter the following command to set the ECMP route failover and load balance method to usage-based.

```
cfg  system settings
    set v4-ecmp-mode usage-based
end
```

2 Enter the following commands to add three route-spillover thresholds to three interfaces.

```
cfg  system interface
    edit port1
        set spillover-threshold 400
    next
    edit port2
        set spillover-threshold 200
    next
    edit port3
```
set spillover-threshold 100
end

3  Enter the following commands to add three ECMP default routes, one for each interface.

config router static
edit 1
set dst 0.0.0.0/0.0.0.0
set gwy 172.20.110.1
set dev port1
next
edit 2
set dst 0.0.0.0/0.0.0.0
set gwy 172.20.120.2
set dev port2
next
edit 3
set dst 0.0.0.0/0.0.0.0
set gwy 172.20.130.3
set dev port3
end

4  Enter the following command to display static routes in the routing table:

get router info routing-table static
S  0.0.0.0/0 [10/0] via 172.20.110.1, port1
   [10/0] via 172.20.120.2, port2
   [10/0] via 172.20.130.3, port3

In this example, the unit sends all sessions to the Internet through port1. When port1 exceeds its spillover threshold of 400 KBps the unit sends all new sessions to the Internet through port2. If both port1 and port2 exceed their spillover thresholds the unit would send all new sessions to the Internet through port3.

Detailed description of how spill-over ECMP selects routes

When you add ECMP routes they are added to the routing table in the order displayed by the routing monitor or by the get router info routing-table static command. This order is independent of the configured bandwidth limit.

The unit selects an ECMP route for a new session by finding the first route in the routing table then sends the session out on a FortiGate interface that is not processing more traffic that its configured route spill-over limit.

For example, consider a unit with interfaces port3 and port4 both connected to the Internet through different ISPs. ECMP routing is set to usage-based and route spillover for to 100 KBps for port3 and 200 KBps for port4. Two ECMP default routes are added, one for port3 and one for port4.

If the route to port3 is higher in the routing table than the route to port4, the unit sends all default route sessions out port3 until port3 is processing 100 KBps of data. When port3 reaches its configured bandwidth limit, the unit sends all default route sessions out port4. When the bandwidth usage of port3 falls below 100 KBps, the unit again sends all default route sessions out port3.
New sessions to designating IP addresses that are already in the routing cache; however, use the cached routes. This means that even of port3 is exceeding its bandwidth limit, new sessions can continue to be sent out port3 if their destination addresses are already in the routing cache. As a result, new sessions are sent out port4 only if port3 exceeds its bandwidth limit and if the routing cache does not contain a route for the destination IP address of the new session. The limit on port4 is important only if there are additional interfaces for spillover.

Also, the switchover to port4 does not occur as soon as port3 exceeds its bandwidth limit. Bandwidth usage has to exceed the limit for a period of time before the switchover takes place. If port3 bandwidth usage drops below the bandwidth limit during this time period, sessions are not switched over to port4. This delay reduces route flapping. Route flapping occurs when routes change their status frequently, forcing routers to continually change their routing tables and broadcast the new information.

FortiGate usage-based ECMP routing is not actually load balancing, since routes are not distributed evenly among FortiGate interfaces. Depending on traffic volumes, most traffic would usually be processed by the first interface with only spillover traffic being processed by other interfaces.

If you are configuring usage-based ECMP, in most cases, you should add spillover thresholds to all of the interfaces with ECMP routes. The default spillover threshold is 0 which means no bandwidth limiting. If any interface has a spillover threshold of 0, no sessions will be routed to interfaces lower in the list unless the interface goes down or is disconnected. An interface can go down if Detect interface status for Gateway Load Balancing does not receive a response from the configured server.

**Note:** A new session to a destination IP address that already has an entry in the routing cache is routed using the route already added to the cache for that destination address. For more information, see “ECMP routing of simultaneous sessions to the same destination IP address” on page 178.

### Determining of a interface has exceeded its Spillover Threshold

You can use the `diagnose netlink dstmac list` CLI command to determine if an interface is exceeding its Spillover Threshold. If the command displays `over_bps=1` the interface is exceeding its threshold. If `over_bps=0` the interface has not exceeded its threshold.

### Configuring weighted static route load balancing

Configure weighted load balancing to control how the unit distributes sessions among ECMP routes by adding weights for each route. Add higher weights to routes that you want to load balance more sessions to. If no weight has been assigned to a route, its weight is set to zero by default.

With the ECMP load balancing method set to weighted, the unit distributes sessions with different destination IPs by generating a random value to determine the route to select. The probability of selecting one route over another is based on the weight value of each route. Routes with higher weights are more likely to be selected.
Large numbers of sessions are evenly distributed among ECMP routes according to the route weight values. If all weights are the same, sessions are distributed evenly. The distribution of a small number of sessions however, may not be even. For example, it's possible that if there are two ECMP routes with the same weight, two sessions to different IP addresses could use the same route. On the other hand 10,000 sessions with different destination IPs should be load balanced evenly between two routes with equal rates. The distribution could be 5000:5000 or 5001:4999. Also, 10,000 sessions with different destination IP addresses should be load balanced in the following way if the weights for the two routes are 100 and 200: 3333:6667.

Weights only affect how routes are selected for sessions to new destination IP addresses. New sessions to IP addresses already in the routing cache are routed using the route for the session already in the cache. So in practice sessions will not always be distributed according to the routing weight distribution.

To add weights to static routes from the web-based manager
1. Go to **Router > Static > Static Route**.
2. Set **ECMP Route failover & Load Balance Method** to **weighted**.
3. Go to **Router > Static > Static Route**.
4. Add new or edit static routes and add weights to them.

The following example shows two ECMP routes with weights added.

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>Device</th>
<th>Gateway</th>
<th>Distance</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.0/24</td>
<td>port1</td>
<td>172.20.110.1</td>
<td>10</td>
<td>100</td>
</tr>
<tr>
<td>192.168.20.0/24</td>
<td>port2</td>
<td>172.20.120.2</td>
<td>10</td>
<td>200</td>
</tr>
</tbody>
</table>

In this example:
- one third of the sessions to the 192.168.20.0 network will use the first route and be sent out port1 to the gateway with IP address 172.20.110.1.
- the other two thirds of the sessions to the 192.168.20.0 network will use the second route and be sent out port2 to the gateway with IP address 172.20.120.2.

To add weights to static routes from the CLI
1. Enter the following command to set the ECMP route failover and load balance method to weighted.
   ```
   config system settings
   set v4-ecmp-mode weight-based
   end
   ```
2. Enter the following commands to add three ECMP static routes and add weights to each route.
   ```
   config router static
   edit 1
   ```
set dst 192.168.20.0/24
set gwy 172.20.110.1
set dev port1
set weight 100
next
edit 2
set dst 192.168.20.0/24
set gwy 172.20.120.2
set dev port2
set weight 200
next
edit 3
set dst 192.168.20.0/24
set gwy 172.20.130.3
set dev port3
set weight 300
end

Note: In this example the priority remains set to 0 and the distance remains set to 10 for all three routes. Any other routes with a distance set to 10 will not have their weight set, so will have a weight of 0 and will not be part of the load balancing.

In this example:

- one sixth of the sessions to the 192.168.20.0 network will use the first route and be sent out port1 to the gateway with IP address 172.20.110.1.
- one third of the sessions to the 192.168.20.0 network will use the second route and be sent out port2 to the gateway with IP address 172.20.120.2.
- one half of the sessions to the 192.168.20.0 network will use the third route and be sent out port3 to the gateway with IP address 172.20.130.3.

Policy Route

A routing policy allows you to redirect traffic away from a static route. This can be useful if you want to route certain types of network traffic differently. You can use incoming traffic’s protocol, source address or interface, destination address, or port number to determine where to send the traffic. For example, generally network traffic would go to the router of a subnet, but you might want to direct SMTP or POP3 traffic addressed to that subnet directly to the mail server.

If you have configured the unit with routing policies and a packet arrives at the unit, the 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 (a minimum of the IP address of the next-hop router and the FortiGate interface for forwarding packets to it), the unit routes the packet using the information in the policy. If no policy route matches the packet, the unit routes the packet using the routing table.

Most policy settings are optional, so a matching policy alone might not provide enough information for forwarding the packet. The 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 in the policy, the unit looks up the IP address of the next-hop router in the routing table. This situation could happen when the interfaces are dynamic (such as DHCP or PPPoE) and you do not want or are unable to specify the IP address of the next-hop router.
Policy route options define which attributes of a incoming packet cause policy routing to occur. If the attributes of a packet match all the specified conditions, the unit routes the packet through the specified interface to the specified gateway.

Policy routes are configured in **Router > Static > Policy Route**. Use the following table when configuring policy routes.

### Policy Route page

Lists all policy routes that you have created. On this page, you can edit, delete or create a new policy route.

<table>
<thead>
<tr>
<th>Create New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a new policy route. When you select <strong>Create New</strong>, you are automatically redirected to the New Routing Policy page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ID numbers of configured route policies. These numbers are sequential unless policies have been moved within the table.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incoming</th>
</tr>
</thead>
<tbody>
<tr>
<td>The interfaces on which packets subjected to route policies are received.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>The interfaces through which policy routed packets are routed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP source addresses and network masks that cause policy routing to occur.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP destination addresses and network masks that cause policy routing to occur.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes a policy route from within the list on the Policy Route page. To remove multiple policy routes in the list, on the Policy Route page, in each of the rows of the routes you want removed, select the check box and then select <strong>Delete</strong>. To remove all policy routes in the list, on the Policy Route page, select the check box in the check box column, and then select <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modifies settings within a static route. When you select <strong>Edit</strong>, you are automatically redirected to the Edit Routing Policy page.</td>
</tr>
</tbody>
</table>

### New Routing Policy page

Provides settings for configuring how to redirect traffic away from the static route.

If incoming traffic matches:

<table>
<thead>
<tr>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>To perform policy routing based on the value in the protocol field of the packet, enter the protocol number to match. The Internet Protocol Number is found in the IP packet header. RFC 5237 describes protocol numbers and you can find a list of the assigned protocol numbers. The range is from 0 to 255. A value of 0 disables the feature. <strong>Tip:</strong> Commonly used Protocol settings include 6 to route TCP sessions, 17 for UDP sessions, 1 for ICMP sessions, 47 for GRE sessions, and 92 for multicast sessions. For protocols other than 6 and 17, the port number is ignored.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incoming interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the name of the interface through which incoming packets subjected to the policy are received.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source address/mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination address/mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>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. To apply policy routing to a range of ports, type the starting port number in the From field and the ending port number in the To field. A value of 0 disables this feature. The Destination Ports fields are only used for TCP and UDP protocols. The ports are skipped over for all other protocols.</td>
</tr>
</tbody>
</table>
Example policy route

Configure the following policy route to send all FTP traffic received at port1 out the port10 interface and to a next hop router at IP address 172.20.120.23. To route FTP traffic set protocol to 6 (for TCP) and set both of the destination ports to 21, the FTP port.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming interface</td>
<td>port1</td>
</tr>
<tr>
<td>Source address / mask</td>
<td>0.0.0.0/0.0.0.0</td>
</tr>
<tr>
<td>Destination address / mask</td>
<td>0.0.0.0/0.0.0.0</td>
</tr>
<tr>
<td>Destination Ports</td>
<td>From 21 to 21</td>
</tr>
<tr>
<td>Type of Service</td>
<td>bit pattern: 00 (hex) bit mask: 00 (hex)</td>
</tr>
<tr>
<td>Outgoing interface</td>
<td>port10</td>
</tr>
<tr>
<td>Gateway Address</td>
<td>172.20.120.23</td>
</tr>
</tbody>
</table>

Type of Service

Type of service (TOS) is an 8-bit field in the IP header that enables you to determine how the IP datagram should be delivered, with such qualities as delay, priority, reliability, and minimum cost.

Each quality helps gateways determine the best way to route datagrams. A router maintains a ToS value for each route in its routing table. The lowest priority TOS is 0, the highest is 7 - when bits 3, 4, and 5 are all set to 1. The router tries to match the TOS of the datagram to the TOS on one of the possible routes to the destination. If there is no match, the datagram is sent over a zero TOS route.

Using increased quality may increase the cost of delivery because better performance may consume limited network resources. For more information, see RFC 791 and RFC 1349.
For example, if you want to assign low delay, and high reliability, say for a VoIP application where delays are unacceptable, you would use a bit pattern of xxx1x1xx where an ‘x’ indicates that bit can be any value. Since all bits are not set, this is a good use for the bit mask; if the mask is set to 0x14, it will match any TOS packets that are set to low delay and high reliability.

Dynamic

Table 22: The role of each bit in the IP header TOS 8-bit field

| bits 0, 1, 2 | Precedence | Some networks treat high precedence traffic as more important traffic. Precedence should only be used within a network, and can be used differently in each network. Typically you do not care about these bits. |
| bit 3       | Delay      | When set to 1, this bit indicates low delay is a priority. This is useful for such services as VoIP where delays degrade the quality of the sound. |
| bit 4       | Throughput | When set to 1, this bit indicates high throughput is a priority. This is useful for services that require lots of bandwidth such as video conferencing. |
| bit 5       | Reliability| When set to 1, this bit indicates high reliability is a priority. This is useful when a service must always be available such as with DNS servers. |
| bit 6       | Cost       | When set to 1, this bit indicates low cost is a priority. Generally there is a higher delivery cost associated with enabling bits 3, 4, or 5, and bit 6 indicates to use the lowest cost route. |
| bit 7       | Reserved for future use | Not used at this time. |

For example, if you want to assign low delay, and high reliability, say for a VoIP application where delays are unacceptable, you would use a bit pattern of xxx1x1xx where an ‘x’ indicates that bit can be any value. Since all bits are not set, this is a good use for the bit mask; if the mask is set to 0x14, it will match any TOS packets that are set to low delay and high reliability.

Dynamic

The Dynamic menu provides settings for configuring dynamic routing. Dynamic routing protocols allow the unit to automatically share information about routes with neighboring routers and learn about routes and networks advertised by them.

The unit supports these dynamic routing protocols:
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)

This topic contains the following:
- RIP
- OSPF
- BGP
- Multicast
- Bi-directional Forwarding Detection (BFD)

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.
RIP

Routing Information Protocol (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).

RIP is configured in Routing > Dynamic > RIP. Use the following table when configuring RIP.

**RIP page**
Lists all the networks and interfaces that you have created. This page also allows you to configure basic RIP settings, including creating interfaces and networks.

**RIP Version**
Select the level of RIP compatibility needed at the unit. You can enable global RIP settings on all FortiGate interfaces connected to RIP-enabled networks:

- **1** – send and receive RIP version 1 packets.
- **2** – send and receive RIP version 2 packets.

You can override the global settings for a specific FortiGate interface if required. For more information, see “RIP-enabled interface” on page 189.

**Advanced Options**
Select the Expand Arrow to view or hide advanced RIP options. For more information, see “Advanced RIP options” on page 188.

**Networks section of the RIP page**
The IP addresses and network masks of the major networks (connected to the 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**
Adds a new network IP address and netmask to the Networks section of the RIP page.
When you select Add, the IP address and netmask is automatically added to the list.

**Delete**
Removes an IP address and netmask from within the Networks section of the RIP page.
To remove multiple IP addresses and netmasks in the list, within the Networks section, in each of the rows of the networks you want removed, select the check box and then select Delete.
To remove all IP addresses and netmasks in the list, within the Networks section, select the check box in the check box column, and then select Delete.

**Interfaces section of the RIP page**
Any additional settings needed to adjust RIP operation on a FortiGate interface.

**Create New**
Creates a new RIP interface. These parameters will override the global RIP settings for that interface.
When you select Create New in the Interfaces section of the RIP page, you are automatically redirected to the New/Edit RIP Interface. See “RIP-enabled interface” on page 189.

**Interface**
The name of the unit RIP interface.

**Send Version**
The version of RIP used to send updates through each interface: 1, 2, or both.

**Receive Version**
The versions of RIP used to listen for updates on each interface: 1, 2, or both.

**Authentication**
The type of authentication used on this interface: None, Text or MD5.

**Passive**
Permissions for RIP broadcasts on this interface. A green checkmark means the RIP broadcasts are blocked.
Advanced RIP options

With advanced RIP options, you can specify settings for RIP timers and define metrics for redistributing routes that the unit learns through some means other than RIP updates. For example, if the 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 unit to advertise those routes on RIP-enabled interfaces.

You can configure additional advanced options through customizable GUI widgets, and the CLI. For example, you can filter incoming or outgoing updates by using a route map, an access list, or a prefix list. The unit also supports offset lists, which add the specified offset to the metric of a route.

Advanced RIP options are configured in Router > Dynamic > RIP, in the Advanced Options are of the page. You must expand Advanced Options to reveal the hidden settings so that you can configure these advanced options. Use the following table when configuring advanced RIP options.

<table>
<thead>
<tr>
<th>Advanced Options section of the RIP page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Options</td>
<td>Select the Expand Arrow to view or hide advanced options.</td>
</tr>
<tr>
<td>Default Metric</td>
<td>Enter the default hop count that the unit should assign to routes that are added to the FortiGate routing table. The range is from 1 to 16. This metric is the hop count, with 1 being best or shortest. This value also applies to Redistribute unless otherwise specified.</td>
</tr>
<tr>
<td>Default-information-originate</td>
<td>Select to generate and advertise a default route into the 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.</td>
</tr>
<tr>
<td>RIP Timers</td>
<td>Enter new values to override the default RIP timer settings. The default settings are effective in most configurations — if you change these settings, ensure that the new settings are compatible with local routers and access servers. If the Update timer is smaller than Timeout or Garbage timers, you will get an error.</td>
</tr>
<tr>
<td>Update</td>
<td>Enter the amount of time (in seconds) that the unit will wait between sending RIP updates.</td>
</tr>
<tr>
<td>Timeout</td>
<td>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 unit will keep a reachable route in the routing table while no updates for that route are received. If the 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.</td>
</tr>
<tr>
<td>Garbage</td>
<td>Enter the amount of time (in seconds) that the unit will advertise a route as being unreachable before deleting the route from the routing table. The value determines how long an unreachable route is kept in the routing table.</td>
</tr>
<tr>
<td>Redistribute</td>
<td>Select one or more of the options to redistribute RIP updates about routes that were not learned through RIP. The unit can use RIP to redistribute routes learned from directly connected networks, static routes, OSPF, and BGP.</td>
</tr>
</tbody>
</table>
RIP-enabled interface

You can use RIP interface options to override the global RIP settings that apply to all unit 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 set 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 unit authenticates a neighboring router before accepting updates from that router. The 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.

RIP-enabled interfaces are configured in Router > Dynamic > RIP.

Note: Additional options such as split-horizon and key-chains can be configured per interface through the CLI.

### New/Edit RIP Interface page

Provides settings for configuring a RIP Interface. When you select Create New in the Interfaces section of the RIP page, you are automatically redirected to the New/Edit RIP Interface page.

**Interface**
Select the name of the FortiGate interface to which these settings apply. The interface must be connected to a RIP-enabled network. The interface can be a virtual IPSec or GRE interface.

**Send Version, Receive Version**
Select to override the default RIP-compatibility setting for sending and receiving updates through the interface: RIP version 1, version 2 or Both.

**Authentication**
Select an authentication method for RIP exchanges on the specified interface:
- None — Disable authentication.
- Text — Select if the interface is connected to a network that runs RIP version 2. Type a password (up to 35 characters) in the Password field. The unit and the RIP updates router must both be configured with the same password. The password is sent in clear text over the network.
- MD5 — Authenticate the exchange using MD5.

**Password**
Enter the password for authentication.

**Passive Interface**
Select to suppress the advertising of unit routing information over the specified interface. Clear the check box to allow the interface to respond normally to RIP requests.

### 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).
The main benefit of OSPF is that it advertises routes only when neighbors change state instead of at timed intervals, so routing overhead is reduced.

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.

OSPF settings are configured in Router > Dynamic > OSPF. Use the following table when configuring OSPF settings.

<table>
<thead>
<tr>
<th>OSPF page</th>
<th>Lists all areas, networks and interfaces that you created for OSPF.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>Enter a unique router ID to identify the 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. If you change the router ID while OSPF is configured on an interface, all connections to OSPF neighbors will be broken temporarily. The connections will re-establish themselves. If Router ID is not explicitly set, the highest IP address of the VDOM or unit will be used.</td>
</tr>
<tr>
<td>Advanced Options</td>
<td>Expand to view or hide advanced OSPF settings.</td>
</tr>
<tr>
<td>Areas section of the OSPF page</td>
<td>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.</td>
</tr>
<tr>
<td>Create New</td>
<td>Creates a new OSPF area. When you select Create New, you are automatically redirected to the New/Edit OSPF Area page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies settings within the OSPF area. When you select Edit, you are automatically redirected to the New/Edit OSPF Area page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes an OSPF area from within the Areas section on the OSPF page. To remove multiple areas in the list, within the Areas section, in each of the rows of the OSPF areas you want removed, select the check box and then select Delete. To remove all areas in the list, within the Areas section, select the check box in the check box column, and then select Delete.</td>
</tr>
<tr>
<td>Area</td>
<td>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.</td>
</tr>
<tr>
<td>Type</td>
<td>The types of areas in the AS:</td>
</tr>
<tr>
<td>Authentication</td>
<td>The methods for authenticating OSPF packets sent and received through all FortiGate interfaces linked to each area:</td>
</tr>
<tr>
<td>None — authentication is disabled</td>
<td></td>
</tr>
<tr>
<td>Text — text-based authentication is enabled</td>
<td></td>
</tr>
<tr>
<td>MD5 — MD5 authentication is enabled</td>
<td></td>
</tr>
</tbody>
</table>
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.
Advanced OSPF options

By selecting advanced OSPF options, you can specify metrics for redistributing routes that the unit learns through some means other than OSPF link-state advertisements. For example, if the 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 unit to advertise those routes on OSPF-enabled interfaces.

You can configure additional advanced options through customizable GUI widgets, and the CLI. For example, you can filter incoming or outgoing updates by using a route map, an access list, or a prefix list. The unit also supports offset lists, which add the specified offset to the metric of a route.

---

Networks section of the OSPF page

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. For more information, see “OSPF networks” on page 193.

- **Create New**: Creates a new OSPF network. When you select Create New, you are automatically redirected to the New/Edit OSPF Network page.
- **Edit**: Modifies settings within that OSPF network. When you select Edit, you are automatically redirected to the New/Edit OSPF Network page.
- **Delete**: Removes an OSPF network from within the Networks section on the OSPF page.
  - To remove multiple networks in the list, within the Networks section, in each of the rows of the OSPF networks you want removed, select the check box and then select Delete.
  - To remove all areas in the list, within the Networks section, select the check box in the check box column, and then select Delete.

Network

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.

Area

The area IDs that have been assigned to the OSPF network address space.

Interfaces section of the OSPF page

Any additional settings needed to adjust OSPF operation on a FortiGate interface. For more information, see “Operating parameters for an OSPF interface” on page 194.

- **Create New**: Create additional/different OSPF operating parameters for a unit’s interface and add the configuration to the Interfaces list. When you select Create New, you are automatically redirected to the New/Edit OSPF Interface page.
- **Edit**: Modifies settings within that OSPF interface. When you select Edit, you are automatically redirected to the New/Edit OSPF Interface page.
- **Delete**: Removes an OSPF interfaces from within the Interfaces section on the OSPF page.
  - To remove multiple networks in the list, within the Interface section, in each of the rows of the OSPF interfaces you want removed, select the check box and then select Delete.
  - To remove all areas in the list, within the Interfaces section, select the check box in the check box column, and then select Delete.

Name

The names of OSPF interface definitions.

Interface

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.

IP

The IP addresses of the OSPF-enabled interfaces having additional/different settings.

Authentication

The methods for authenticating LSA exchanges sent and received on specific OSPF-enabled interfaces. These settings override the area Authentication settings.
Advanced OSPF options are located in Router > Dynamic > RIP. You must expand the Advanced Options on the page to access these options. Use the following table when configuring advanced OSPF options.

### Advanced Options on the OSPF page

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Router ID</strong></td>
<td>Enter a unique router ID to identify the unit to other OSPF routers.</td>
</tr>
<tr>
<td><strong>Expand Arrow</strong></td>
<td>Select to view or hide Advanced Options.</td>
</tr>
<tr>
<td><strong>Default Information</strong></td>
<td>Generate and advertise a default (external) route to the OSPF AS. You may base the generated route on routes learned through a dynamic routing protocol, routes in the routing table, or both.</td>
</tr>
<tr>
<td><strong>None</strong></td>
<td>Prevent the generation of a default route.</td>
</tr>
<tr>
<td><strong>Regular</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Always</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Redistribute</strong></td>
<td>Select one or more of the options listed to redistribute OSPF link-state advertisements about routes that were not learned through OSPF. The unit can use OSPF to redistribute routes learned from directly connected networks, static routes, RIP, and BGP.</td>
</tr>
<tr>
<td><strong>Connected</strong></td>
<td>Select to redistribute routes learned from directly connected networks. Enter a cost for those routes in the Metric field. The range is from 1 to 16 777 214.</td>
</tr>
<tr>
<td><strong>Static</strong></td>
<td>Select to redistribute routes learned from static routes. Enter a cost for those routes in the Metric field. The range is from 1 to 16 777 214.</td>
</tr>
<tr>
<td><strong>RIP</strong></td>
<td>Select to redistribute routes learned through RIP. Enter a cost for those routes in the Metric field. The range is from 1 to 16 777 214.</td>
</tr>
<tr>
<td><strong>BGP</strong></td>
<td>Select to redistribute routes learned through BGP. Enter a cost for those routes in the Metric field. The range is from 1 to 16 777 214.</td>
</tr>
</tbody>
</table>

### Defining OSPF areas

An area logically defines part of the OSPF AS. Each area is identified by a 32-bit area ID expressed in dotted-decimal notation, for example 192.168.0.1. Area ID 0.0.0.0 is reserved for the OSPF network backbone. You can classify the remaining areas of an AS as regular, stub, or 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.
Defining an OSPF is configured in *Router > Dynamic > OSPF*. Use the following table to configure the OSPF.

**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 be set up only between two units that act as area border routers.

### New/Edit OSPF Area page
Provides settings for defining an OSPF area. When you select Create New in the Areas section of the OSPF page, you are automatically redirected to the New/Edit OSPF Area page.

- **Area**: Type a 32-bit identifier for the area. The value must resemble an IP address in dotted-decimal notation. Once you have created the OSPF area, the area IP value cannot be changed; you must delete the area and restart.

- **Type**: Select an area type to classify the characteristics of the network that will be assigned to the area:
  - **Regular**: If the area contains more than one router, each having at least one OSPF-enabled interface to the area.
  - **NSSA**: If you want routes to external non-OSPF domains made known to OSPF AS and you want the area to be treated like a stub area by the rest of the AS.
  - **STUB**: If the routers in the area must send packets to an area border router in order to reach the backbone and you do not want routes to non-OSPF domains to be advertised to the routers in the area.

- **Authentication**: Select the method for authenticating OSPF packets sent and received through all interfaces in the area:
  - **None**: Disable authentication.
  - **Text**: Enables text-based password authentication. to authenticate LSA exchanges using a plain-text password. The password is sent in clear text over the network.
  - **MD5**: Enable MD5-based authentication using an MD5 cryptographic hash (RFC 1321).

If required, you can override this setting for one or more of the interfaces in the area. For more information, see “Operating parameters for an OSPF interface” on page 194.

### 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. Assigning an OSPF area ID to a network is configured in *Router > Dynamic > OSPF*. You must be in the Network section of the page to assign an OSPF area ID to a network. Use the following table when assigning an OSPF area ID to a network.

### New/Edit OSPF Network page
Provides settings for configuring networks that are assigned to an area ID. When you select Create New in the Network section of the OSPF page, you are automatically redirected to the New/Edit OSPF Network page.

- **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. For more information, see “Defining OSPF areas” on page 192.
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 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 can run OSPF in area 0.0.0.0. To enable all interfaces, you would create an OSPF network 0.0.0.0/0

When entering the operating parameters for MD5 keys for the interface, the following special characters are not supported:

- `<`
- `>`
- `#`
- `(`
- `)`
- `“`
- `‘`

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.

OSPF operating parameters are configured in Router > Dynamic > OSPF, in the Interfaces section of the page. Use the following table when configuring OSPF operating parameters.

<table>
<thead>
<tr>
<th>New/Edit OSPF Interface page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides settings for configuring an OSPF interface. When you select Create New in the Interface section of the OSPF page, you are automatically redirected to the New/Edit OSPF Interface page.</td>
</tr>
</tbody>
</table>

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 unit can have physical, VLAN, virtual IPSec or GRE interfaces connected to the OSPF-enabled 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:

- None — Disable authentication.
- Text — 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.
- MD5 — Use one or more keys to generate an MD5 cryptographic hash.

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 a 128-bit hash, represented by an alphanumeric string of up to 16 characters. When entering the characters, do not use < >, ( ), #, “, and ‘ because they are not supported.
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 unit waits between sending Hello packets through this 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 unit waits to receive a Hello packet from an OSPF neighbor through the interface. If the unit does not receive a Hello packet within the specified amount of time, the unit declares the neighbor inaccessible.
By convention, the Dead Interval value is usually four times greater than the Hello interval value.

---

**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, OSPF, or both to route packets within the AS. The FortiGate implementation of BGP supports BGP-4 and complies with RFC 1771 and RFC 2385.

**Note:** You can configure graceful restarting and other advanced settings only through CLI commands.

When you configure BGP settings, you need to specify the AS to which the unit belongs and enter a router ID to identify this unit to other BGP routers. You must also identify the unit’s BGP neighbors and specify which of the networks local to the unit should be advertised to BGP neighbors.

When you configure BGP settings, you need to specify the AS to which the unit belongs and enter a router ID to identify this unit to other BGP routers. You must also identify the unit’s BGP neighbors and specify which of the networks local to the unit should be advertised to BGP neighbors.

BGP settings are configured in *Router > Dynamic > BGP*. You can also configure many advanced BGP options through the CLI. Use the following table to configure BGP settings.

---

**BGP page**
Lists all neighbors and networks that you have created. This page also allows you to configure neighbors, networks and a local AS. You can also configure four-byte AS paths as well. If you want additional information about configuring four-byte AS paths, see RFC 4893.

**Local AS**
Enter the number of the local AS to which the FortiGate unit belongs.

**Router ID**
Enter a unique router ID to identify the unit to other BGP routers. The router ID is an IP address written in dotted-decimal format, for example 192.168.0.1. If you change the router ID while BGP is configured on an interface, all connections to BGP peers will be broken temporarily. The connections will re-establish themselves.
If Router ID is not explicitly set, the highest IP address of the VDOM will be used.
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.

Note: You can configure basic options through the web-based manager. Many additional options are available, but only through the CLI.

When multicast (PIM) routing is enabled, you can configure sparse mode or dense mode operation on any FortiGate interface.

PIM settings are configured in Router > Dynamic > Multicast. The web-based manager offers a simplified user interface to configure basic PIM options. You can also configure advanced PIM options through the CLI.

You use multicast (PIM) interface options 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.
Overriding the multicast settings on an interface are configured in Router > Dynamic > Multicast. Use the following table when configuring overriding multicast settings on an interface.

### Multicast page

Lists each individual multicast route that you created. This page also allows you to configure each multicast route and add RP addresses.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Multicast Routing</td>
<td>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.</td>
</tr>
<tr>
<td>Static Rendezvous Points (RPs)</td>
<td>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.</td>
</tr>
<tr>
<td>Apply</td>
<td>Save the specified static RP addresses.</td>
</tr>
<tr>
<td>Create New</td>
<td>Creates a new multicast entry for an interface. When you select Create New, you are automatically redirected to the New page. You can use the new entry to fine-tune PIM operation on a specific FortiGate interface or override the global PIM settings on a particular interface.</td>
</tr>
</tbody>
</table>

### 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 change the status of 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. Available only when RP candidacy is enabled.

### DR Priority

The priority number assigned to Designated Router (DR) candidacy on the interface. Available only when sparse mode is enabled.

### Delete

Removes a multicast route from within the Multicast page. To remove multiple routes in the list, on the Multicast Route page, in each of the rows of the routes you want removed, select the check box and then select Delete. To remove all neighbors in the list, on the Multicast Route page, select the check box in the check box column, and then select Delete.

### Edit

Modifies settings within the multicast route. When you select Edit, you are automatically redirected to the Edit page.

### New page

Provides settings for configuring a new multicast interface. When you select Create New on the Multicast page, you are automatically redirected to the New page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>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.</td>
</tr>
<tr>
<td>PIM Mode</td>
<td>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.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>Enter the priority number for advertising DR candidacy on the unit’s interface. The range is from 1 to 4 294 967 295. The unit compares this value to the DR interfaces of all other PIM routers on the same network segment, and selects the router having the highest DR priority to be the DR.</td>
</tr>
<tr>
<td>RP Candidate</td>
<td>Enable RP candidacy on the interface.</td>
</tr>
<tr>
<td>RP Candidate Priority</td>
<td>Enter the priority number for advertising RP candidacy on the FortiGate interface. The range is from 1 to 255.</td>
</tr>
</tbody>
</table>
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.
By using this feature that is available only in the CLI, you can avoid redistributing routes at
the translation boundary into their network infrastructure for Reverse Path Forwarding
(RPF) to work properly. They can also receive identical feeds from two ingress points in
the network and route them independently.
Configure multicast DNAT in the CLI using the `firewall multicast policy`
command.

Bi-directional Forwarding Detection (BFD)
The bi-directional Forwarding Detection (BFD) protocol is designed to deal with dynamic
routing protocols' lack of a fine granularity for detecting device failures on the network and
re-routing around those failures. BFD can more quickly react to these failures, since it
detects them on a millisecond timer, where other dynamic routing protocols can only
detect them on a second timer.
Your unit supports BFD as part of OSPF and BGP dynamic networking. BFD is configured
only in the CLI.

Configuring BFD
BFD is intended for networks that use BGP or OSPF routing protocols. This generally
excludes smaller networks.
BFD configuration on your unit is very flexible. You can enable BFD for the whole 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 required for your network
The timeout period determines how long the unit waits before labeling a connection as
down. The length of the timeout period is important—if it is too short connections will be
labeled down prematurely, and if it is too long time will be wasted waiting for a reply from a
connection that is down. There is no easy number, as it varies for each network and unit.
High end 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, you should try setting
a longer timeout period to allow BFD more time to discover the device on the network.
For this example, BFD is enabled on the unit using the default values. This means that
once a connection is established, your unit will wait for up to 150 milliseconds for a reply
from a BFD router before declaring that router down and rerouting traffic—a 50
millisecond minimum transmit interval multiplied by a detection multiplier of 3. The port
that BFD traffic originates from will be checked for security purposes as indicated by
disabling `bfd-dont-enforce-src-port`.
`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`
Disabling BFD for a specific interface

The previous example enables BFD for your entire unit. If an interface is not connected to any BFD enabled routers, you can reduce network traffic by disabling BFD for that interface. For this example, BFD is disabled for the internal interface using CLI commands.

```
config system interface
  edit <interface>
  set bfd disable
end
```

Monitor

The Monitor menu provides a way to view the activity of configured routes. The Routing Monitor page allows you to view specific information as well as all routes. The list displays the entries in the FortiGate routing table.

This topic includes the following:

- Viewing routing information
- Searching the routing monitor table

Viewing 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.

View the list in `Router > Monitor > Routing Monitor`.

Routing Monitor page

Lists all routes that are being monitored, including the default static route. On this page, you can also filter the information that is displayed on the page by applying a filter.

- **IP version**: Select IPv4 or IPv6 routes. Fields displayed vary depending on which IP version is selected.
- **Type**: Select one of the following route types to search the routing table and display routes of the selected type only:
  - *All* – all routes recorded in the routing table.
  - *Connected* – all routes associated with direct connections to FortiGate interfaces.
  - *Static* – the static routes that have been added to the routing table manually.
  - *RIP* – all routes learned through RIP.
  - *OSPF* – all routes learned through OSPF.
  - *BGP* – all routes learned through BGP.
  - *HA* – 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 visible only if you are viewing the router monitor from a virtual domain that is configured as a subordinate virtual domain in a virtual cluster.

Not displayed when IP version IPv6 is selected.

For more information about HA routing synchronization, see the HA chapter in the FortiOS Handbook.
### Searching the routing monitor table

You can apply a filter to search the routing table and display certain routes only. For example, you can display one or more static routes, connected routes, routes learned through RIP, OSPF, or BGP, and 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 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 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

This section provides an introduction to the Firewall menu. If you require more information about the features in the Firewall menu, see the FortiOS Handbook.

The following topics are included in this section:

• Policy
• Address
• Service
• Schedule
• Traffic Shaper
• Virtual IP
• Load Balance

Policy

A firewall policy (or policy) provides instructions to the unit on how to decide what to do with the incoming and outgoing traffic passing through the unit. When the policy receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number) and attempts to locate the policy that matches the packet.

Firewall policies control all traffic attempting to pass through the unit, between FortiGate interfaces, zones, and VLAN subinterfaces.

These policies that you configure on the unit, can contain many different instructions for the unit to follow when it receives matching packets. The instructions may be quite complicated, or simple.

Policy instructions may include network address translation (NAT), or port address translation (PAT), by using virtual IPs or IP pools to translate source and destination IP addresses and port numbers. For more information on using virtual IPs and IP pools, see “Virtual IP” on page 230.

This topic contains the following:

• Policy
• Identity-based firewall policies
• Central NAT Table
• IPv6 Policy
• DoS Policy
• Protocol Options
• Sniffer Policy

Policy

You can configure firewall policies to define which sessions will match the policy and what actions the unit will perform with packets from matching sessions.

Sessions are matched to a firewall policy by considering these features of both the packet and policy:
• Source Interface/Zone
• Source Address
• Destination Interface/Zone
• Destination Address
• schedule and time of the session’s initiation
• service and the packet’s port numbers.

If the initial packet matches the firewall policy, the unit performs the configured Action and any other configured options on all packets in the session.

Packet handling actions can be ACCEPT, DENY, IPSEC or SSL-VPN.

• **ACCEPT** policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying a protection profile to apply features such as virus scanning to packets in the session. An ACCEPT policy can also apply interface-mode IPSec VPN traffic if either the selected source or destination interface is an IPSec virtual interface. For more information, see “IPsec VPN” on page 299.

• **DENY** policy actions block communication sessions, and may optionally log the denied traffic.

• **IPSEC** and **SSL-VPN** policy actions apply a tunnel mode IPSec VPN or SSL VPN tunnel, respectively, and may optionally apply NAT and allow traffic for one or both directions. If permitted by the firewall encryption policy, a tunnel may be initiated automatically whenever a packet matching the policy arrives on the specified network interface, destined for the local private network. For more information, see “IPSec identity-based firewall policies” on page 210 and “SSL VPN identity-based firewall policies” on page 210.

Firewall policy order affects policy matching. Each time that you create or edit a policy, make sure that you position it in the correct location in the list. You can create a new policy and position it right away before an existing one in the firewall policy list, by selecting Insert Policy before (see “Policy” on page 203).

**Note:** You can configure differentiated services (DSCP) firewall policy options through the CLI.

When you have configured firewall policies for IPv4 and IPv6, you can view them from the Policy page. The Policy page allows you to view these firewall policies in either Section View or Global View. Section View is default, and hides details about each of the firewall policies while Global View shows the details.

You can also remove or show different columns on the Policy page as well, by selecting Column Settings.

Firewall policies are configured in Firewall > Policy > Policy.
**Policy page**
Lists each individual policy and section that you created. On this page, you can edit, delete or create a new policy or section title.

**Create New**
Creates a new policy. Select the down arrow beside Create New to add a new section to the list to visually group the policies.
When you select Create New, you are automatically redirected to the New Policy page. If you select the down arrow to add a new section title, the Section Title window appears.
For security purposes, selecting Create New adds the new policy to the bottom of the list. Once the policy is added to the list, you can use the Move To icon to move the policy to the required position in the list. You can also use the Insert Policy before icon to add a new policy above another policy in the list.

**Column Settings**
Customize the table view. You can select the columns to hide or display and specify the column displaying order in the table.

**Section View**
Select to display firewall policies organized by source and destination interfaces. **Note:** Section View is not available if any policy selects any as the source or destination interface.

**Global View**
Select to list all firewall policies in order according to a sequence number.

**Filter icons**
Edit the column filters to filter or sort the policy list according to the criteria you specify.

**ID**
The policy identifier. Policies are numbered in the order they are added to the policy list.

**From**
The source interface of the policy. Global view only.

**To**
The destination interface of the policy. Global view only.

**Source**
The source address or address group to which the policy applies.

**Destination**
The destination address or address group to which the policy applies.

**Schedule**
The schedule that controls when the policy should be active.

**Service**
The service to which the policy applies.

**Profile**
The profile that is associated with the policy.

**Action**
The response to make when the policy matches a connection attempt.

**Status**
Select the check box to enable a policy or deselect it to disable a policy.

**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.

**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.

**Count**
The unit counts the number of packets and bytes that hit the firewall policy.
For example, 5/50B means that five packets and 50 bytes in total have hit the policy.
The counter is reset when the unit is restarted or the policy is deleted and reconfigured.

**Delete**
Removes a policy from the list on the Policy page.
To remove multiple firewall policies from within the list, on the Policy page, in each of the rows of the policies you want removed, select the check box and then select Delete.
To remove all firewall policies from the list, on the Policy page, select the check box in the check box column, and then select Delete.

**Edit**
Modifies settings within a firewall policy. When you select Edit, you are automatically redirected to the Edit Policy page.
When you are ready to configure a firewall policy, you will be redirected to the New Policy page, where you can apply UTM features to the firewall policy.

If you have a FortiGate-224B unit and it is in switch mode, you can create a policy governing traffic between switch ports on a switch GLAN. There must be at least one secure port available. This option is Intra-VLAN Policy.

Use the following table when configuring policies in Firewall > Policy > Policy.

### New Policy page
Provides settings for configuring a new firewall policy.

#### Source Interface/Zone
Select the name of the FortiGate network interface, virtual domain (VDOM) link, or zone on which IP packets are received. Interfaces and zones are configured on the System Network page. For more information, see "Interface configuration and settings" on page 58 and "Configuring zones" on page 74.

If you select any as the source interface, the policy matches all interfaces as source. By selecting Any as the source interface, the policy matches all interfaces as source. When you select any as the source interface, that firewall policy list is displayed only in Global View. This occurs because the unit understands any as potentially applying to all firewall policies within the policy list and, as such, automatically changes the page's view to Global View only.

**Note:** Fortinet does not recommend this option because it can have unexpected results, and should be used rarely and only by a knowledgeable administrator.

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 firewall address to associate with the Source Interface/Zone. Only packets whose header contains an IP address matching the selected firewall address will be subject to this policy.

You can also create firewall addresses by selecting Create New from this list.

If you want to associate multiple firewall addresses or address groups with the Source Interface/Zone, from Source Address, select Multiple. In the dialog box, move the firewall addresses or address groups from the Available Addresses section to the Members section, then select OK.

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.

#### Destination Interface/Zone
Select the name of the FortiGate network interface, virtual domain (VDOM) link, or zone to which IP packets are forwarded. Interfaces and zones are configured on the System Network page. For more information, see "Interface configuration and settings" on page 58 and "Configuring zones" on page 74.

If you select Any as the destination interface, the policy matches all interfaces as destination.

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 firewall address to associate with the Destination Interface/Zone. Only packets whose header contains an IP address matching the selected firewall address will be subject to this policy.
You can also create firewall addresses by selecting Create New from this list.
If you want to associate multiple firewall addresses or address groups with the Destination Interface/Zone, from Destination Address, select Multiple. In the dialog box, move the firewall addresses or address groups from the Available Addresses section to the Members section, then select OK.
If you select a virtual IP, the unit applies NAT or PAT. The applied translation varies by the settings specified in the virtual IP, and whether you select NAT (below). For more information on using virtual IPs, see “Virtual IP” on page 231.
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 unit.

Schedule
Select a one-time or recurring schedule or a schedule group that controls when the policy is in effect.
You can also create schedules by selecting Create New from this list. For more information, see “Schedule” on page 226.

Service
Select the name of a firewall service or service group that packets must match to trigger this policy.
You can select from a wide range of predefined firewall services, or you can create a custom service or service group by selecting Create New from this list. For more information, see “Custom services” on page 224 and “Custom service groups” on page 225.
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. The options available will vary widely depending on this selection.

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 Log Violation Traffic to log the connections denied by this policy and adding a Comment.

IPSEC
You can configure an IPSec firewall encryption policy to process IPSec VPN packets, as well as configure protection profiles, log traffic, shape traffic or add a comment to the policy. See “IPSec identity-based firewall policies” on page 210.

SSL-VPN
You can configure an SSL-VPN firewall encryption policy to accept SSL VPN traffic. This option is available only after you have added a SSL-VPN user group. You can also configure NAT and protection profiles, log traffic, shape traffic or add a comment to the policy. See “SSL VPN identity-based firewall policies” on page 210.

NAT
Available only if Action is set to ACCEPT or SSL-VPN. Enable or disable Network Address Translation (NAT) of the source address and port of packets accepted by the policy. When NAT is enabled, you can also configure Dynamic IP Pool and Fixed Port.
If you select a virtual IP as the Destination Address, but do not select the NAT option, the unit performs destination NAT (DNAT) rather than full NAT. Source NAT (SNAT) is not performed.

Dynamic IP Pool
Select the check box, then select an IP pool to translate the source address to an IP address randomly selected from addresses in the IP Pool.
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.
For more information, see “IP pools” on page 233.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fixed Port</strong></td>
<td>Select <em>Fixed Port</em> to prevent NAT from translating the source port. Some applications do not function correctly if the source port is translated. In most cases, if <em>Fixed Port</em> is selected, <em>Dynamic IP pool</em> is also selected. If <em>Dynamic IP pool</em> is not selected, a policy with <em>Fixed Port</em> selected can allow only one connection to that service at a time. <strong>Note:</strong> <em>Fixed Port</em> is only visible if enabled from the CLI.</td>
</tr>
<tr>
<td><strong>Enable Identity Based Policy</strong></td>
<td>Select to configure firewall policies that require authentication. For more information, see &quot;Identity-based firewall policies&quot; on page 209. The &quot;Identity-based firewall policies&quot; on page 209 also describes the Firewall, Directory Service (FSAE), NTLM Authentication, and Enable Disclaimer and Redirect URL to options.</td>
</tr>
<tr>
<td><strong>UTM</strong></td>
<td>Select an UTM option to apply to the firewall policy. You must enable UTM before you can select the available UTM options.</td>
</tr>
<tr>
<td><strong>Protocol options</strong></td>
<td>Select a protocol item from the drop-down list. The default protocol item is called default. The protocol item contains multiple settings, including NNTP and logging invalid certificates. Select <em>Create New</em> in the drop-down list to create a new protocol option list item.</td>
</tr>
<tr>
<td><strong>Enable Antivirus</strong></td>
<td>Select an antivirus profile from the drop-down list. Select <em>Create New</em> in the drop-down list to create a new antivirus profile.</td>
</tr>
<tr>
<td><strong>Enable Web Filter</strong></td>
<td>Select a web filtering profile from the drop-down list. Select <em>Create New</em> in the drop-down list to create a new web filtering profile.</td>
</tr>
<tr>
<td><strong>Enable Email Filter</strong></td>
<td>Select an email filter profile from the drop-down list. Select <em>Create New</em> in the drop-down list to create a new email filter profile.</td>
</tr>
<tr>
<td><strong>Enable DLP Sensor</strong></td>
<td>Select a DLP sensor from the drop-down list. Select <em>Create New</em> in the drop-down list to create a new DLP sensor.</td>
</tr>
<tr>
<td><strong>Enable Application Control</strong></td>
<td>Select an application control black/white list from the drop-down list. Select <em>Create New</em> in the drop-down list to create a new application control black/white list.</td>
</tr>
<tr>
<td><strong>Enable VoIP</strong></td>
<td>Select a VoIP profile from the drop-down list. Select <em>Create New</em> in the drop-down list to create a new VoIP profile.</td>
</tr>
<tr>
<td><strong>Traffic Shaping</strong></td>
<td>Select a shared traffic shaper for the policy. You can also create a new shared traffic shaper. Shared traffic shapers control the bandwidth available to and set the priority of the traffic as its processed by, the policy.</td>
</tr>
<tr>
<td><strong>Reverse Direction Traffic Shaping</strong></td>
<td>Select to enable reverse traffic shaping and select a shared traffic shaper. For example, if the traffic direction that a policy controls is from port1 to port2, select this option will also apply the policy shaping configuration to traffic from port2 to port1.</td>
</tr>
<tr>
<td><strong>Per-IP Traffic Shaping</strong></td>
<td>Select a Per-IP traffic shaper for the policy. Per-IP traffic shaping applies traffic shaping to the traffic generated from the IP addresses added to the Per-IP traffic shaper added to the firewall policy.</td>
</tr>
<tr>
<td><strong>Log Allowed Traffic</strong></td>
<td>Select to record messages to the traffic log whenever the policy processes a connection. You must also enable traffic log for a logging location (syslog, WebTrends, local disk if available, memory, or FortiAnalyzer) and set the logging severity level to <em>Notification</em> or lower using the Log&amp;Report menu.</td>
</tr>
<tr>
<td><strong>No NAT</strong></td>
<td>Selected by default. When it is selected, NAT is not used for that firewall policy.</td>
</tr>
<tr>
<td><strong>Enable NAT</strong></td>
<td>Select to enable logging of NAT traffic. The Dynamic IP Pool option is then available. You must configure the dynamic IP pool before enabling this option.</td>
</tr>
<tr>
<td><strong>Use Central NAT Table</strong></td>
<td>Select to enabling logging using the Central NAT table that you configured in the Central NAT Table menu.</td>
</tr>
<tr>
<td><strong>Dynamic IP Pool</strong></td>
<td>Available only when Enable NAT is selected.</td>
</tr>
</tbody>
</table>
Identity-based firewall policies

For network users to use non-SSL-VPN identity-based policies, you need to add user groups to the policy. For information about configuring user groups, see “User Group” on page 324.

Identity-based firewall policies are configured within each firewall policy, in Firewall > Policy. Use the following table when configuring identity-based policies.

<table>
<thead>
<tr>
<th>Enable Endpoint NAC</th>
<th>Select to enable the Endpoint NAC feature and select the Endpoint NAC profile to apply.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• You cannot enable Endpoint in firewall policies if Redirect HTTP Challenge to a Secure Channel (HTTPS) is enabled in User &gt; Options &gt; Authentication.</td>
</tr>
<tr>
<td></td>
<td>• If the firewall policy involves a load balancing virtual IP, the Endpoint check is not performed.</td>
</tr>
</tbody>
</table>

| Comments | Add information about the policy. The maximum length is 63 characters. |

| Add | Adds user groups to the list, located below Add. The selected user groups that must authenticate to be allowed to use this policy. When you select Add, the Edit Authentication Rule appears. |

| Display Implicit Policies | Select to display all implicit policies that are currently available. The policies appear in the list, which is located under Add. |

| Rule ID | The rule’s name or identification. |
| User Group | The selected user groups that must authenticate to be allowed to use this policy. |
| Service | The firewall service or service group that packets must match to trigger this policy. |
| Schedule | The one-time or recurring schedule that controls when the policy is in effect. You can also create schedules by selecting Create New from this list. For more information, see “Schedule” on page 226. |
| UTM | Indicates whether a UTM feature was selected for the policy. |
| Traffic Shaping | The traffic shaping configuration for this policy. For more information, see “Schedule” on page 226. |
| Logging | Indicates whether logging was selected for that policy. |
| Delete | Removes an identity-based policy from the list, which is in the Enable Identity Based Policy section. You must remove each identity-based policy individual. |
| Edit | Modifies settings within the identity-based policy. When you select Edit, the Edit Authentication Rule window appears. |
| Move To | Moves an identity-based policy to another position in the list. When you select Move To, the Move Authentication Rule window appears. |
| Firewall | Include firewall user groups defined locally on the unit, as well as on any connected LDAP and RADIUS servers. This option is selected by default. |
| Directory Service (FSAE) | Include Directory Service groups defined in User > User Group. The groups are authenticated through a domain controller using Fortinet Server Authentication Extensions (FSAE). If you select this option, you must install the FSAE on the Directory Service domain controller. For information about FSAE, see the Fortinet Server Authentication Extension Administration Guide. For information about configuring user groups, see “User Group” on page 324. |
| NTLM Authentication | Include Directory Service groups defined in User > User Group. If you select this option, you must use Directory Service groups as the members of the authentication group for NTLM. For information about configuring user groups, see “User Group” on page 324. |
IPSec identity-based firewall policies

In a firewall policy (see “Policy” on page 203), the following encryption options are available for IPSec. For more information, see the “Defining firewall policies” chapter of the FortiGate IPSec VPN User Guide.

Identity-based firewall policies are configured within each firewall policy, in Firewall > Policy > Policy. Use the following table when configuring IPSec identity-based firewall policies.

### IPSec settings on the New Policy page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Tunnel</td>
<td>Select the VPN tunnel name defined in the phase 1 configuration. The specified tunnel will be subject to this firewall encryption policy.</td>
</tr>
<tr>
<td>Allow Inbound</td>
<td>Select to enable traffic from a dialup client or computers on the remote private network to initiate the tunnel.</td>
</tr>
<tr>
<td>Allow outbound</td>
<td>Select to enable traffic from computers on the local private network to initiate the tunnel.</td>
</tr>
<tr>
<td>Inbound NAT</td>
<td>Select to translate the source IP addresses of inbound decrypted packets into the IP address of the FortiGate interface to the local private network.</td>
</tr>
<tr>
<td>Outbound NAT</td>
<td>Select only in combination with a <code>natip</code> CLI value to translate the source addresses of outbound cleartext packets into the IP address that you specify. When a <code>natip</code> value is specified, the source addresses of outbound IP packets are replaced before the packets are sent through the tunnel.</td>
</tr>
</tbody>
</table>

**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.

SSL VPN identity-based firewall policies

For network users to use SSL-VPN identity-based policies, you must configure SSL VPN users, add them to user groups, and then configure the policy. For more information, see “Policy” on page 203.

Identity-based firewall policies are configured within each firewall policy, in Firewall > Policy > Policy. Use the following table when configuring SSL VPN identity-based policies.

**Note:** The SSL-VPN option is only available from the Action list after you have added SSL VPN user groups. To add SSL VPN user groups, see “SSL VPN user groups” on page 326.
SSL-VPN settings on the New Policy page

Source Interface/Zone
Select the name of the FortiGate network interface, virtual domain (VDOM) link, or zone on which IP packets are received.

Source Address
Select the name of a firewall address to associate with the Source Interface/Zone. Only packets whose header contains an IP address matching the selected firewall address will be subject to this policy. You can also create firewall addresses by selecting Create New from this list. For more information, see “Address list” on page 218.
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.

Destination Interface/Zone
Select the name of the FortiGate network interface, virtual domain (VDOM) link, or zone to which IP packets are forwarded. If Action is set to SSL-VPN, the interface is associated with the local private network.

Destination Address
Select the name of a firewall address to associate with the Destination Interface/Zone. Only packets whose header contains an IP address matching the selected firewall address will be subject to this policy. You can also create firewall addresses by selecting Create New from this list. For more information, see “Address list” on page 218.
If you want to associate multiple firewall addresses or address groups with the Destination Interface/Zone, from Destination Address, select Multiple. In the dialog box, move the firewall addresses or address groups from the Available Addresses section to the Members section, then select OK.
If you select a virtual IP, the unit applies NAT or PAT. The applied translation varies by the settings specified in the virtual IP, and whether you select NAT (below). For more information on using virtual IPs, see “Virtual IP” on page 230.
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 unit.

Action
Select SSL-VPN to configure the firewall encryption policy to accept SSL VPN traffic. This option is available only after you have added a SSL-VPN user group.

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 the bit level of SSL encryption. The web browser on the remote client must be capable of matching the level that you select: Any, High >> 164, or Medium >> 128.

User Authentication Method
Select the authentication server type by which the user will be authenticated:
- **Any** – For all the above authentication methods. Local is attempted first, then RADIUS, and then LDAP.
- **Local** – For a local user group that will be bound to this firewall policy.
- **RADIUS** – For remote clients that will be authenticated by an external LDAP server.
- **LDAP** – For remote clients that will be authenticated by an external LDAP server.
- **TACACS+** – For remote clients that will be authenticated by an external TACACS+ server.

No NAT
Selected by default. When it is selected, NAT is not used for that firewall policy.

Dynamic IP Pool
Select to enable dynamic IP pools.
Central NAT Table

The Central NAT Table allows users to create NAT rules, as well as view NAT mappings that are set up by the global firewall table. You can use these NAT rules on firewall policies by selecting Use Central NAT Table option within the policy. This menu is not available in Transparent mode.

Configure NAT rules from Firewall > Policy > Central NAT Table, using the following table.

**Central NAT Table page**
Lists each individual NAT rules that you created. On this page, you can edit, delete or create a new NAT rule.

- **Create New**
  Creates a new NAT rule set. When you select Create New, you are automatically redirected to the New Nat page.

- **Edit**
  Modifies settings to a NAT rule set. When you select Edit, you are automatically redirected to the Edit Nat page.

- **Delete**
  Removes a NAT rule set from the list on the Central NAT Table page. To remove multiple NAT rule sets from within the list, on the Central NAT Table page, in each of the rows of the rule sets you want removed, select the check box and then select Delete. To remove all NAT rule sets from the list, on the Central NAT Table page, select the check box in the check box column and then select Delete.

- **Enable**
  Enables a NAT rule set that is currently disabled.

- **Disable**
  Disables a NAT rule set that is currently enabled.

- **Insert**
  Inserts a new NAT rule.

- **Move To**
  Moves the NAT rule to another position within the list. When you select Move To, the Move Policy window appears.

**New NAT page**
Provides settings for configuring a NAT rule.

- **Source Address**
  Select the source IP address from the drop-down list. You can optionally create a group of source IP addresses when you select Multiple in the drop-down list. You can also create a new source IP address when you select Create New in the drop-down list.

- **Translated Address**
  Select the dynamic IP pool from the drop-down list.
**Original Port**
Enter the port that the address is originating from.

**Translated Port**
Enter the translated port number. The number in the From field must be greater than the lower port number that is entered in the To field.

---

**IPv6 Policy**

Configuration of IPv6 policies is only available when IPv6 is enabled. By default, the unit is not enabled to use IPv6 addressing. The IPv6 Policy menu appears after the IPv6 is enabled in System > Admin > Settings.

The IPv6 menu is the same as the Policy menu. For more information about the available icons and settings, see “Policy” on page 203.

---

**DoS Policy**

The DoS policy list displays the DoS policies in their order of matching precedence for each interface, source/destination address pair, and service.

If virtual domains are enabled on the unit, DoS policies are configured separately for each virtual domain; you must access the VDOM before you can configure its policies.

You can add, delete, edit, and re-order policies in the DoS policy list. DoS policy order affects policy matching. As with firewall policies, DoS policies are checked against traffic in the order in which they appear in the DoS policy list, one at a time, from top to bottom. When a matching policy is discovered, it is used and further checking for DoS policy matches are stopped.

The DoS policy configuration allows you to specify the interface, a source address, a destination address, and a service. All of the specified attributes must match network traffic to trigger the policy.

You can also use the `config firewall interface-policy` CLI command to add DoS policies from the CLI. You can also use this CLI command to add an IPS sensor or an Application Control black/white list to a DoS policy.

You can use the `config firewall interface-policy6` command to add IPv6 sniffer policies.

DoS policies are configured in Firewall > Policy > DoS Policy. Use the following table when configuring DoS policies.

---

**DoS Policy page**

Lists each individual DoS policy that you created. On this page, you can edit, delete or create a new DoS policy.

**Create New**
Add a new DoS policy. Select the down arrow beside Create New to add a new section to the list to visually group the policies.

**Column Settings**
Customizes the table view. You can select the columns to hide or display and specify the column displaying order in the table. See “Using column settings to control the columns displayed” on page 26.

**Section View**
Select to display firewall policies organized by interface.

**Global View**
Select to list all firewall policies in order according to a sequence number.

**Filter icons**
Edit the column filters to filter or sort the policy list according to the criteria you specify. For more information, see “Adding filters to web-based manager lists” on page 24.

**ID**
A unique identifier for each policy. Policies are numbered in the order they are created.

**Source**
The source address or address group to which the policy applies. For more information, see “Address” on page 217.
Protocol Options

The Protocol Options menu allows you to configure settings for specific protocols, which are grouped together in a protocol group, and then applied to a firewall policy. The default groups are scan, strict, unfiltered, and web.

Protocol Options are configured in Firewall > Policy > Protocol Options. Use the following table when configuring protocol options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The destination address or address group to which the policy applies. For more information, see &quot;Address&quot; on page 217.</td>
</tr>
<tr>
<td>Service</td>
<td>The service to which the policy applies. For more information, see &quot;Service&quot; on page 220.</td>
</tr>
<tr>
<td>DoS</td>
<td>The DoS sensor selected in this policy.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface to which this policy applies.</td>
</tr>
<tr>
<td>Status</td>
<td>When selected, the DoS policy is enabled. Clear the check box to disable the policy.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a policy from the list on the DoS Policy page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies settings within the policy. When you select Edit, you are automatically redirected to the Edit DoS Policy page.</td>
</tr>
<tr>
<td>Insert</td>
<td>Inserts a new policy above the corresponding policy. When you select Insert, the New Policy window appears.</td>
</tr>
<tr>
<td>Move</td>
<td>Moves the corresponding policy before or after another policy in the list.</td>
</tr>
</tbody>
</table>

*New Policy page*

Provides settings for configuring a DoS policy. When you select Create New on the DoS Policy page, you are automatically redirected to this page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Interface/Zone</td>
<td>The interface or zone to be monitored.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Select an address, address range, or address group to limit traffic monitoring to network traffic sent from the specified address or range. Select Multiple to include multiple addresses or ranges. You can also select Create New to add a new address or address group.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Select an address, address range, or address group to limit traffic monitoring to network traffic sent to the specified address or range. Select Multiple to include multiple addresses or ranges. You can also select Create New to add a new address or address group.</td>
</tr>
<tr>
<td>Service</td>
<td>Select a firewall pre-defined service or a custom service to limit traffic monitoring to only the selected service or services. You can also select Create new to add a custom service.</td>
</tr>
<tr>
<td>DoS Sensor</td>
<td>Select and specify a DoS sensor to have the FortiGate unit apply the sensor to matching network traffic. You can also select Create new to add a new DoS Sensor. See &quot;DoS sensor&quot; on page 253.</td>
</tr>
</tbody>
</table>

Protocol Options page

Lists each individual protocol setting that you created. On this page, you can edit, delete or create a new group of protocol settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new protocol option. When you select Create New, you are automatically redirected to the Protocol Options Settings page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies settings to a protocol setting.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a protocol setting from the list on the Protocol Options page.</td>
</tr>
</tbody>
</table>
### Protocol Options Settings page

Provides settings for configuring options for each protocol which make up a protocol group.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the protocol group.</td>
</tr>
<tr>
<td><strong>Comments</strong></td>
<td>Enter a description about the protocol group. This is optional.</td>
</tr>
<tr>
<td><strong>Enable Oversized File Log</strong></td>
<td>Select to allow logging of oversized files.</td>
</tr>
<tr>
<td><strong>Enable Invalid Certificate Log</strong></td>
<td>Select to allow logging of invalid certificates.</td>
</tr>
</tbody>
</table>

#### HTTP section

Configure settings for the HTTP protocol

- **Port (i.e. 80,88, 0-auto)**: This is available for every protocol except for IM.
- **Comfort Clients**: This is available only for HTTP, FTP, and HTTPS.
  - **Interval (1-900 seconds)**: enter the interval time in seconds.
  - **Amount (1-10240 bytes)**: enter the amount in bytes.
- **Oversized File/Email**: This is available for all protocols.
  - **Threshold**: enter the threshold amount for an oversized email message or file in MB.
- **Monitor Content Information for Dashboard**: Select to view the activity of the protocol from the Dashboard menu.
- **Enable Chunked Bypass**: Select to enable the chunked bypass setting.

#### FTP section

Configure settings for the file transfer protocol. FTP and HTTP contain the same settings, except the FTP section does not contain the option Enable Chunked Bypass.

#### IMAP section

Configure settings for the IMAP protocol.

- **Allow Fragmented Messages**: Allows fragmented email messages to be passed.

#### POP3 section

Configure settings for the POP3 protocol. This section contains the same settings as are in the IMAP section.

#### SMTP section

Configure settings for the SMTP section.

- **Append Email Signature**: Select to enable the option of entering a new email signature that appears in the email message.
- **Email Signature Text**: Enter a signature for the email message, for example, Yours sincerely. Accessible only when Append Email Signature is selected.

#### IM section

Configure settings for the IM protocol.

#### NNTP section

Configure settings for the NTTP protocol.

#### HTTPS section

Configure settings for the HTTPS protocol.

- **Allow Invalid SSL Certificate**: Select to allow invalid SSL certificates.
- **Enable Deep Scanning**: Select to allow deep scanning.

#### IMAPS

Configure settings for the IMAPS protocol.

#### POP3S

Configure settings for the POP3S protocol. This section contains the same settings as IMAPS.

#### SMTPS

Configure settings for the SMTPS protocol. This section contains the same settings as IMAPS and POP3S.
Sniffer Policy

The sniffer policy list displays sniffer policies in their order of matching precedence for each interface, source/destination address pair, and service.

If virtual domains are enabled on the unit, sniffer policies are configured separately for each virtual domain; you must access the VDOM before you can configure its policies.

You can add, delete, edit, and re-order policies in the sniffer policy list. Sniffer policy order affects policy matching. As with firewall policies and DoS policies, sniffer policies are checked against traffic in the order in which they appear in the sniffer policy list, one at a time, from top to bottom. When a matching policy is discovered, it is used and further checking for sniffer policy matches are stopped. If no match is found the packet is dropped.

Use the sniffer policy configuration to specify the interface, a source address, a destination address, and a service. All of the specified attributes must match network traffic to trigger the policy.

You can also use the `config firewall sniff-interface-policy` CLI command to add sniffer policies from the CLI.

You can use the `config firewall sniff-interface-policy6` command to add IPv6 sniffer policies.

Sniffer policies are configured in **Firewall > Policy > Sniffer Policy**. Use the following table when configuring sniffer policies.

<table>
<thead>
<tr>
<th>Sniffer Policy page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists each individual sniffer policy that you created. On this page, you can edit, delete and create a new sniffer policy. You can also move a policy or insert a new policy on the page.</td>
</tr>
</tbody>
</table>

| Create New | Creates a new sniffer policy. Select the down arrow beside Create New to add a new section to the list to visually group the policies. When you select Create New (or an option from the down arrow’s drop-down list), you are automatically redirected to the New Policy page. |
| Column Settings | Customize the table view. You can select the columns to hide or display and specify the column displaying order in the table. |
| Section View | Select to display firewall policies organized by interface. |
| Global View | Select to list all firewall policies in order according to a sequence number. |
| Filter icons | Edit column filters to filter or sort the policy list according to the criteria you specify. |
| ID | A unique identifier for each policy. Policies are numbered in the order they are created. |
| Source | The source address or address group to which the policy applies. |
| Destination | The destination address or address group to which the policy applies. |
| Service | The service to which the policy applies. |
| DoS | The DoS sensor selected in this policy. |
| Sensor | The IPS sensor selected in this policy. |
| Application Black/White List | The application black/white list that is selected in this policy. |
| Status | When selected, the DoS policy is enabled. Clear the check box to disable the policy. |
Delete
Removes the policy from the list.
To remove multiple sniffer policies from within the list, on the Sniffer Policy page, in each of the rows of sniffer policies you want removed, select the check box and then select Delete.
To remove all sniffer policies from within the list, on the Sniffer Policy page, select the check box in the check box column and then select Delete.

Edit
Modifies settings within the policy. When you select Edit, you are automatically redirected to Edit Policy page.

Insert Policy Before
Add a new policy above the corresponding policy (the New Policy screen appears).

Move To
Move the corresponding policy before or after another policy in the list.

New Policy page
Provides settings for configuring a new sniffer policy. When you select Create New on the Sniffer Policy page, you are automatically redirected to this page.

Source Interface/Zone
The interface or zone to be monitored.

Source Address
Select an address, address range, or address group to limit traffic monitoring to network traffic sent from the specified address or range. Select Multiple to include multiple addresses or ranges. You can also select Create New to add a new address or address group.

Destination Address
Select an address, address range, or address group to limit traffic monitoring to network traffic sent to the specified address or range. Select Multiple to include multiple addresses or ranges. You can also select Create New to add a new address or address group.

Service
Select a firewall pre-defined service or a custom service to limit traffic monitoring to only the selected service or services. You can also select Create New to add a custom service.

DoS Sensor
Select and specify a DoS sensor to have the unit apply the sensor to matching network traffic. You can also select Create New to add a new DoS Sensor.

IPS Sensor
Select and specify an IPS sensor to have the unit apply the sensor to matching network traffic. You can also select Create New to add a new IPS Sensor.

Application Black/White List
Select and specify an Application control List sensor to have the unit apply the list to matching network traffic. You can also select Edit to add a new application control List.

Address
Firewall addresses and address groups define network addresses that you can use when configuring firewall policies’ source and destination address fields. The unit compares the IP addresses contained in packet headers with firewall policy source and destination addresses to determine if the firewall policy matches the traffic. You can add IPv4 addresses and address ranges, IPv6 addresses, and fully qualified domain names (FQDNs).

You can organize related addresses into address groups and related IPv6 addresses into IPv6 address groups to simplify your firewall policy lists.

This topic contains the following:
- Address list
- Address Group
Address list

**Caution:** Be cautious if employing FQDN firewall addresses. Using a fully qualified domain name in a firewall policy, while convenient, does present some security risks, because policy matching then relies on a trusted DNS server. Should the DNS server be compromised, firewall policies requiring domain name resolution may no longer function properly.

Firewall addresses in the list are grouped by type: IP/Netmask, FQDN, or IPv6. A unit’s default configurations include the all address, which represents any IPv4 IP address on any network. You can also add a firewall address list when configuring a firewall policy.

The IPv6 address field is restricted to around 34 characters so you cannot add full IPv6 addresses and netmasks. Instead you should use the short form netmask shown in the examples.

You cannot assign IPv6 addresses to a FortiGate interface.

Firewall addresses are configured in **Firewall > Address > Address**.

**Address page**
Lists each individual IP address group. On this page, you can edit, delete or create a new IP address group.

| Create New | Adds a firewall address. When you select Create New, you are automatically redirected to the New Address page.  
**Note:** If IPv6 Support is enabled you can select the down arrow in the Create New button and select IPv6 Address, to add an IPv6 firewall address. To enable IPv6 support on the web-based manager, see “Settings” on page 121. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the firewall address.</td>
</tr>
<tr>
<td>Address / FQDN</td>
<td>The IP address and mask, IP address range, or fully qualified domain name.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface, zone, or virtual domain (VDOM) to which you bind the IP address.</td>
</tr>
<tr>
<td>IP/Netmask</td>
<td>The list of IPv4 firewall addresses and address ranges.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The list of fully qualified domain name firewall addresses.</td>
</tr>
<tr>
<td>IPv6</td>
<td>The list of IPv6 firewall addresses.</td>
</tr>
</tbody>
</table>
| Delete | Removes an address from within the list. The Delete icon appears only if a firewall policy or address group is not currently using the address.  
To remove multiple addresses from within the list, on the Address page, in each of the rows of addresses you want removed, select the check box and then select Delete.  
To remove all addresses from within the list, on the Address page, select the check box in the check box column and then select Delete. |
| Edit | Modifies settings within the an address. When you select Edit, you are automatically redirected to the Edit Address page. |

**New Address page**
Provides settings for configuring an IP address group, which is made up of an IP address range.

| Address Name | Enter a name to identify the firewall address. Addresses, address groups, and virtual IPs must have unique names. |
| Type | Select the type of address: Subnet/IP Range or FQDN. You can enter either an IP range or an IP address with subnet mask. |
| Subnet / IP Range | Enter the firewall IP address, followed by a forward slash (/), then subnet mask, or enter an IP address range separated by a hyphen. |
| Interface | Select the interface, zone, or virtual domain (VDOM) link to which you want to bind the IP address. Select Any if you want to bind the IP address with the interface/zone when you create a firewall policy. |
| IPv6 Address | Enter the firewall IPv6 address, followed by a forward slash (/), then subnet mask. |
Address Group

**Caution:** Be cautious if employing FQDN firewall addresses. Using a fully qualified domain name in a firewall policy, while convenient, does present some security risks because policy matching then relies on a trusted DNS server. If the DNS server should ever be compromised, firewall policies requiring domain name resolution may no longer function properly.

You can organize multiple firewall addresses into an address group to simplify your firewall policy list. For example, instead of having five identical policies for five different but related firewall addresses, you might combine the five addresses into a single address group, which is used by a single firewall policy.

Because firewall policies require addresses with homogenous network interfaces, address groups should contain only addresses bound to the same network interface, or to any addresses whose selected interface is Any are bound to a network interface during creation of a firewall policy, rather than during creation of the firewall address. For example, if address A1 is associated with port1, and address A2 is associated with port2, they cannot be grouped. However, if A1 and A2 have an interface of Any, they can be grouped, even if the addresses involve different networks.

You cannot mix IPv4 firewall addresses and IPv6 firewall addresses in the same address group.

Address groups are configured in Firewall > Address > Group.

**Group page**

Lists each individual address group that you created. On this page, you can edit, delete or create a new address group.

**Create New**

Add an address group. When you select Create New, you are automatically redirected to the New Address Group page.

If IPv6 Support is enabled you can select the down arrow in the Create New button and select IPv6 Address Group, to add an IPv6 firewall address. To enable IPv6 support on the web-based manager, see “Settings” on page 121.

**Group Name**

The name of the address group.

**Members**

The addresses in the address group.

**Address Group**

The list of firewall IPv4 address groups.

**IPv6 Address Group**

The list of firewall IPv6 address groups.

**Delete**

Removes an address group. The Delete icon appears only if the address group is not currently being used by a firewall policy.

To remove multiple address groups from within the list, on the Group page, in each of the rows of the address groups you want removed, select the check box and then select Delete.

To remove all address groups from the list, on the Group page, select the check box in the check box column and then select Delete.

**Edit**

Modifies settings within the address group. When you select Edit, you are automatically redirected to the Edit Address Group page.

**New Address Group page**

Provides settings for defining the IP address that will be members of the IP address group.

**Group Name**

Enter a name to identify the address group. Addresses, address groups, and virtual IPs must have unique names.

**Available Addresses**

The list of all IPv4 or IPv6 firewall addresses. Use the arrows to move selected addresses between the lists of available and member addresses. You cannot add IPv4 and IPv6 firewall addresses to the same address group. If you are adding an IPv4 firewall address group only the IPv4 addresses and FQDN addresses appear. If you are added an IPv6 firewall address group, only the IPv6 addresses appear.
Service

Firewall services define one or more protocols and port numbers associated with each service. Firewall policies use service definitions to match session types. You can organize related services into service groups to simplify your firewall policy list.

This topic contains the following:

- Predefined service list
- Custom services
- Custom service groups

Predefined service list

Many well-known traffic types have been predefined in firewall services. These predefined services are defaults, and cannot be edited or removed. However, if you require different services, you can create custom services. For more information, see "Custom services" on page 224.

Predefined services are located in Firewall > Service > Predefined. Table 23 lists the FortiGate firewall predefined services.

**Predefined page**

Lists all the predefined services that are available. Table 23 lists and explains each firewall predefined service that is available on the unit.

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the predefined service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detail</td>
<td>The protocol (TCP, UDP, IP, ICMP) and port number or numbers of the predefined service.</td>
</tr>
</tbody>
</table>

Table 23: Predefined services

<table>
<thead>
<tr>
<th>Service name</th>
<th>Description</th>
<th>IP Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFS3</td>
<td>Advanced File Security Encrypted File, version 3, of the AFS distributed file system protocol.</td>
<td>TCP, UDP</td>
<td>7000-7009</td>
</tr>
<tr>
<td>AH</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>TCP, UDP</td>
<td>51</td>
</tr>
<tr>
<td>ANY</td>
<td>Matches connections using any protocol over IP.</td>
<td>all</td>
<td>all</td>
</tr>
<tr>
<td>AOL</td>
<td>America Online Instant Message protocol.</td>
<td>TCP</td>
<td>5190-5194</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol. BGP is an interior/exterior routing protocol.</td>
<td>TCP</td>
<td>179</td>
</tr>
<tr>
<td>CVSPSERVER</td>
<td>Concurrent Versions System Proxy Server. CVSPServer is very good for providing anonymous CVS access to a repository.</td>
<td>TCP, UDP</td>
<td>2401</td>
</tr>
<tr>
<td>DCE-RPC</td>
<td>Distributed Computing Environment / Remote Procedure Calls. Applications using DCE-RPC can call procedures from another application without having to know on which host the other application is running.</td>
<td>TCP, UDP</td>
<td>135</td>
</tr>
</tbody>
</table>
### Table 23: Predefined services (Continued)

<table>
<thead>
<tr>
<th>Service name</th>
<th>Description</th>
<th>IP Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol. DHCP allocates network addresses and delivers configuration parameters from DHCP servers to hosts.</td>
<td>UDP</td>
<td>67, 68</td>
</tr>
<tr>
<td>DHCP6</td>
<td>Dynamic Host Configuration Protocol for IPv6.</td>
<td>UDP</td>
<td>546, 547</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service. DNS resolves domain names into IP addresses.</td>
<td>TCP</td>
<td>53</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service. DNS resolves domain names into IP addresses.</td>
<td>UDP</td>
<td>53</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload. ESP is used by manual key and AutoIKE IPSec VPN tunnels for communicating encrypted data. AutoIKE VPN tunnels use ESP after establishing the tunnel by IKE.</td>
<td></td>
<td>50</td>
</tr>
<tr>
<td>FINGER</td>
<td>A network service providing information about users.</td>
<td>TCP</td>
<td>79</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol.</td>
<td>TCP</td>
<td>21</td>
</tr>
<tr>
<td>FTP_GET</td>
<td>File Transfer Protocol. FTP GET sessions transfer remote files from an FTP server to an FTP client computer.</td>
<td>TCP</td>
<td>21</td>
</tr>
<tr>
<td>FTP_PUT</td>
<td>File Transfer Protocol. FTP PUT sessions transfer local files from an FTP client to an FTP server.</td>
<td>TCP</td>
<td>21</td>
</tr>
<tr>
<td>GOPHER</td>
<td>Gopher organizes and displays Internet server contents as a hierarchically structured list of files.</td>
<td>TCP</td>
<td>70</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation. GRE allows 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>TCP</td>
<td>47</td>
</tr>
<tr>
<td>H323</td>
<td>H.323 multimedia protocol. H.323 is a standard approved by the International Telecommunication Union (ITU) defining how audiovisual conferencing data can be 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>H323</td>
<td>H.323 multimedia protocol. H.323 is a standard approved by the International Telecommunication Union (ITU) defining how audiovisual conferencing data can be transmitted across networks. For more information, see the FortiGate Support for H.323 Technical Note.</td>
<td>UDP</td>
<td>1719</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol. HTTP is used to browse web pages on the World Wide Web.</td>
<td>TCP</td>
<td>80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HTTP with secure socket layer (SSL). HTTPS is used for secure communication with web servers.</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>ICMP_ANY</td>
<td>Internet Control Message Protocol. ICMP allows control messages and error reporting between a host and gateway (Internet).</td>
<td>ICMP</td>
<td>Any</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange. IKE obtains authenticated keying material for use with the Internet Security Association and Key Management Protocol (ISAKMP) for IPSEC.</td>
<td>UDP</td>
<td>500, 4500</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol. IMAP is used by email clients to retrieves email messages from email servers.</td>
<td>TCP</td>
<td>143</td>
</tr>
<tr>
<td>IMAPS</td>
<td>IMAP with SSL. IMAPS is used for secure IMAP communication between email clients and servers. IMAPS is only available on FortiGate units that support SSL content scanning and inspection. For more information, see the UTM chapter of the FortiOS Handbook.</td>
<td>TCP</td>
<td>993</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>
</tbody>
</table>
### Table 23: Predefined services (Continued)

<table>
<thead>
<tr>
<th>Service name</th>
<th>Description</th>
<th>IP Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRC</td>
<td>Internet Relay Chat. IRC allows users to join chat channels.</td>
<td>TCP</td>
<td>6660-6669</td>
</tr>
<tr>
<td>Internet-Locator-Service</td>
<td>Internet Locator Service. ILS includes LDAP, User Locator Service, and LDAP over TLS/SSL.</td>
<td>TCP</td>
<td>389</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol. L2TP is a PPP-based tunnel protocol for remote access.</td>
<td>TCP</td>
<td>1701</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>1701</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol. LDAP is used to access information directories.</td>
<td>TCP</td>
<td>389</td>
</tr>
<tr>
<td>MGCP</td>
<td>Media Gateway Control Protocol. MGCP is used by call agents and media gateways in distributed Voice over IP (VoIP) systems.</td>
<td>UDP</td>
<td>2427, 2727</td>
</tr>
<tr>
<td>MS-SQL</td>
<td>Microsoft SQL Server is a relational database management system (RDBMS) produced by Microsoft. Its primary query languages are MS-SQL and T-SQL.</td>
<td>TCP</td>
<td>1433, 1434</td>
</tr>
<tr>
<td>MYSQL</td>
<td>MySQL is a relational database management system (RDBMS) which runs as a server providing multi-user access to a number of databases.</td>
<td>TCP</td>
<td>3306</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System. NFS allows network users to mount shared files.</td>
<td>TCP</td>
<td>111, 2049</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>111, 2049</td>
</tr>
<tr>
<td>NNTP</td>
<td>Network News Transport Protocol. NNTP is used to post, distribute, and retrieve Usenet messages.</td>
<td>TCP</td>
<td>119</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol. NTP synchronizes a host’s time with a time server.</td>
<td>TCP</td>
<td>123</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</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>ONC-RPC</td>
<td>Open Network Computing Remote Procedure Call. ONC-RPC is a widely deployed remote procedure call system.</td>
<td>TCP</td>
<td>111</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>111</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First. 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>TCP</td>
<td>5631</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>5632</td>
</tr>
<tr>
<td>PING</td>
<td>Ping sends ICMP echo request/replies to test connectivity to other hosts.</td>
<td>ICMP</td>
<td>8</td>
</tr>
<tr>
<td>PING6</td>
<td>Ping6 sends ICMPv6 echo request/replies to network hosts to test IPv6 connectivity to other hosts.</td>
<td></td>
<td>58</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol v3. POP retrieves email messages.</td>
<td>TCP</td>
<td>110</td>
</tr>
<tr>
<td>POP3S</td>
<td>Post Office Protocol v3 with secure socket layer (SSL). POP3S is used for secure retrieval of email messages. POP3S is only available on FortiGate units that support SSL content scanning and inspection. For more information, see the UTM chapter of the FortiOS Handbook.</td>
<td>TCP</td>
<td>995</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol. PPTP is used to tunnel connections between private network hosts over the Internet. <strong>Note:</strong> Also requires IP protocol 47.</td>
<td>TCP</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1723</td>
</tr>
</tbody>
</table>
Table 23: Predefined services (Continued)

<table>
<thead>
<tr>
<th>Service name</th>
<th>Description</th>
<th>IP Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUAKE</td>
<td>Quake multi-player computer game traffic.</td>
<td>UDP</td>
<td>26000, 27000, 27910, 27960</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service. RADIUS is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.</td>
<td>TCP</td>
<td>1812, 1813</td>
</tr>
<tr>
<td>RAUDIO</td>
<td>RealAudio multimedia traffic.</td>
<td>UDP</td>
<td>7070</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol is a multi-channel protocol that allows a user to connect to a networked computer.</td>
<td>TCP</td>
<td>3389</td>
</tr>
<tr>
<td>REXEC</td>
<td>Rexec traffic allows specified commands to be executed on a remote host running the rexecd service (daemon).</td>
<td>TCP</td>
<td>512</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol. RIP is a common distance vector routing protocol. This service matches RIP v1.</td>
<td>UDP</td>
<td>520</td>
</tr>
<tr>
<td>RLOGIN</td>
<td>Remote login traffic.</td>
<td>TCP</td>
<td>513</td>
</tr>
<tr>
<td>RSH</td>
<td>Remote Shell traffic allows specified commands to be executed on a remote host running the rshd service (daemon).</td>
<td>TCP</td>
<td>514</td>
</tr>
<tr>
<td>RTSP</td>
<td>Real Time Streaming Protocol is a protocol for use in streaming media systems which allows a client to remotely control a streaming media server, issuing VCR-like commands such as play and pause, and allowing time-based access to files on a server.</td>
<td>TCP</td>
<td>554, 7070, 8554</td>
</tr>
<tr>
<td>SAMBA</td>
<td>Server Message Block. SMB allows clients to use file and print shares from enabled hosts. This is primarily used for Microsoft Windows hosts, but may be used with operating systems running the Samba daemon.</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. SIP allows audiovisual conferencing data to be transmitted across networks. For more information, see the Voice Solutions: SIP chapter of the FortiOS Handbook.</td>
<td>UDP</td>
<td>5060</td>
</tr>
<tr>
<td>SIP-MSNmessenger</td>
<td>Session Initiation Protocol 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. SMTP is used for sending email messages between email clients and email servers, and between email servers.</td>
<td>TCP</td>
<td>25</td>
</tr>
<tr>
<td>SMTPS</td>
<td>SMTP with SSL. Used for sending email messages between email clients and email servers, and between email servers securely. SMTPS is only available on FortiGate units that support SSL content scanning and inspection. For more information, see the UTM chapter of the FortiOS Handbook.</td>
<td>TCP</td>
<td>465</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol. SNMP can be used to monitor and manage complex networks.</td>
<td>TCP</td>
<td>161-162</td>
</tr>
</tbody>
</table>
### Custom services

If you need to create a firewall policy for a service that is not in the predefined service list, you can add a custom service. Custom services are configured in **Firewall > Service Custom**. You can view all custom services from the Service Custom page as well.

<table>
<thead>
<tr>
<th>Service name</th>
<th>Description</th>
<th>IP Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOCKS</td>
<td>SOCKetS. SOCKS is an Internet protocol that allows client-server applications to transparently use the services of a network firewall.</td>
<td>TCP, UDP</td>
<td>1080</td>
</tr>
<tr>
<td>SQUID</td>
<td>A proxy server and web cache daemon that has a wide variety of uses that includes speeding up a web server by caching repeated requests; caching web, DNS and other computer network lookups for a group of people sharing network resources; aiding security by filtering traffic.</td>
<td>TCP</td>
<td>3128</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell. SSH allows secure remote management and tunneling.</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>Talk allows conversations between two or more users.</td>
<td>UDP</td>
<td>517-518</td>
</tr>
<tr>
<td>TCP</td>
<td>Matches connections using any TCP port.</td>
<td>TCP</td>
<td>0-65535</td>
</tr>
<tr>
<td>TELNET</td>
<td>Allows plain text remote management.</td>
<td>TCP</td>
<td>23</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol. TFTP is similar to FTP, but without security features such as authentication.</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>TRACEROUTE</td>
<td>A computer network tool used to determine the route taken by packets across an IP network.</td>
<td>TCP</td>
<td>33434</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>33434</td>
</tr>
<tr>
<td>UDP</td>
<td>Matches connections using any UDP port.</td>
<td>UDP</td>
<td>0-65535</td>
</tr>
<tr>
<td>UUCP</td>
<td>Unix to Unix Copy Protocol. UUCP provides simple file copying.</td>
<td>UDP</td>
<td>540</td>
</tr>
<tr>
<td>VDOLIVE</td>
<td>VDO Live streaming multimedia traffic.</td>
<td>TCP</td>
<td>7000-7010</td>
</tr>
<tr>
<td>VNC</td>
<td>Virtual Network Computing. VNC is a graphical desktop sharing system which uses the RFB protocol to remotely control another computer.</td>
<td>TCP</td>
<td>5900</td>
</tr>
<tr>
<td>WAIS</td>
<td>Wide Area Information Server. WAIS is an Internet search protocol which may be used in conjunction with Gopher.</td>
<td>TCP</td>
<td>210</td>
</tr>
<tr>
<td>WINFRAME</td>
<td>WinFrame provides communications between computers running Windows NT, or Citrix WinFrame/MetaFrame.</td>
<td>TCP</td>
<td>1494</td>
</tr>
<tr>
<td>WINS</td>
<td>Windows Internet Name Service is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names.</td>
<td>TCP</td>
<td>1512</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP</td>
<td>1512</td>
</tr>
<tr>
<td>X-WINDOWS</td>
<td>X Window System (also known as X11) can forward the graphical shell from an X Window server to X Window client.</td>
<td>TCP</td>
<td>6000-6063</td>
</tr>
</tbody>
</table>
You can organize multiple firewall services into a service group to simplify your firewall policy list. For example, instead of having five identical policies for five different but related firewall services, you might combine the five services into a single address group that is used by a single firewall policy.

Service groups can contain both predefined and custom services. Service groups cannot contain other service groups.

You can organize multiple firewall services into a service group to simplify your firewall policy list. For example, instead of having five identical policies for five different but related firewall services, you might combine the five services into a single service group that is used by a single firewall policy.

Service groups can contain both predefined and custom services. Service groups cannot contain other service groups.
Custom service groups are configured in Firewall > Service > Group.

**Group page**
Lists each individual service group that you created. On this page, you can edit, delete or create a new service group.

<table>
<thead>
<tr>
<th>Create New</th>
<th>Adds a service group. When you select Create New, you are automatically redirected to the New Service Group page. Tip: You can also create custom services when you are configuring a firewall policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td>Modifies settings within a group. When you select Edit, you are automatically redirected to the Edit Service Group page.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Removes the entry from the list. The Delete icon appears only if the service group is not selected in a firewall policy. To remove multiple custom service groups from within the list, on the Group page, in each of the rows of the groups you want removed, select the check box and then select Delete. To remove all custom service groups from the list, on the Group page, select the check box in the check box column and then select Delete.</td>
</tr>
</tbody>
</table>

| **Group Name** | The name to identify the service group. |
| **Members**    | The services added to the service group. |

**New Service Group page**
Provides settings for defining the services that will be members within a service group.

| **Group Name** | Enter a name to identify the service group. |
| **Available Services** | The list of configured and predefined services available for your group, with custom services at the bottom. Use the arrows to move selected services between this list and Members. |
| **Members**    | The list of services in the group. Use the arrows to move selected services between this list and Available Services. |

**Schedule**
Firewall schedules control when policies are in effect. You can create one-time schedules or recurring schedules. One-time schedules are in effect only once for the period of time specified in the schedule. Recurring schedules are in effect repeatedly at specified times of specified days of the week.

This topic contains the following:
- Recurring schedule list
- One-time schedule list

**Recurring schedule list**
You can create a recurring schedule that activates a policy during a specified period of time. For example, you might prevent game playing during office hours by creating a recurring schedule that covers office hours.

If a recurring schedule has a stop time that is earlier than the start time, the schedule will take effect at the start time but end at the stop time on the next day. You can use this technique to create recurring schedules that run from one day to the next. For example, to prevent game playing except at lunchtime, you might set the start time for a recurring schedule at 1:00 p.m. and the stop time at 12:00 noon. To create a recurring schedule that runs for 24 hours, set the start and stop times to 00. To put a policy into effect for an entire day, set schedule start and stop times to 00.

Recurring schedules are configured in Firewall > Schedule > Recurring.
Recurring page
Lists each individual recurring schedule that you created. On this page, you can edit, delete or create a new recurring schedule.

Create New
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.

Stop
The stop time of the recurring schedule.

Delete
Removes the schedule from the list. The Delete icon appears only if the schedule is not being used in a firewall policy.

Edit
Modifies settings within the schedule.

New Recurring Schedule page
Provides settings for configuring a schedule that is active on a regular basis.

Name
Enter a name to identify the recurring schedule.

Select
Select the days of the week for the schedule to be active.

Start
Select the start time for the recurring schedule.

Stop
Select the stop time for the recurring schedule.

Tip: You can also create recurring schedules when you configure a firewall policy.

One-time schedule list

You can create a one-time schedule that activates a policy during 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, but you could add a one-time schedule to block access to the Internet during a holiday.

One-time schedules are configured in Firewall > Schedule > One-time.

One-time page
Lists each individual schedule that only occurs once. On this page, you can edit, delete or create a new one-time schedule. To put a policy into effect for an entire day, set schedule start and stop times to 00.

Create New
Add a one-time schedule. When you select Create New, you are automatically redirected to the New One-time Schedule page.

Tip: You can also create custom services when you are configuring a firewall policy.

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
Removes the schedule from the list. The Delete icon appears only if the schedule is not being used in a firewall policy.

To remove multiple one-time schedules from within the list, on the One-time Schedule page, in each of the rows of schedules you want removed, select the check box and then select Delete.

To remove all one-time schedules from the list, on the One-time Schedule page, select the check box in the check box column and then select Delete.

Edit
Modifies settings within the schedule. When you select Edit, you are automatically redirected to the Edit One-time Schedule page.
Schedule groups

You can organize multiple firewall schedules into a schedule group to simplify your firewall policy list. For example, instead of having five identical policies for five different but related firewall schedules, you might combine the five schedules into a single schedule group that is used by a single firewall policy.

Schedule groups can contain both recurring and on-time schedules. Schedule groups cannot contain other schedule groups.

Scheduled groups are configured in Firewall > Schedule > Group.

Traffic Shaper

Traffic shaping, when included in a firewall policy, 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 unit. 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 extra high speed Internet access could have a special outgoing policy set up with higher bandwidth.

Traffic shaping is available for firewall policies whose Action is ACCEPT, IPSEC, or SSL-VPN. 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 you can use it to improve the quality of bandwidth-intensive and sensitive traffic.
This topic contains the following:

- **Shared traffic shapers**
- **Per-IP traffic shaping**

### Shared traffic shapers

By default, the unit includes pre-defined shared traffic shapers. You can add these shapers to firewall policies as is, custom them, or add new shared traffic shapers.

After creating or editing shared traffic shapers, you add them to firewall policies by going to **Firewall > Policy > Policy** and adding a new or editing a firewall policy. You can also go to **Firewall > Policy > IPv6 Policy** and add a new or edit an IPv6 firewall policy to apply traffic shaping to IPv6 traffic.

To enable shared traffic shaping in a firewall policy, select **Traffic Shaping** and select a shared traffic shaper. You can also select **Reverse Direction Traffic Shaping** and select a shared traffic shaper to apply shared traffic shaping to return traffic.

When you want to ensure that traffic shaping is working at its best, verify that the interface Ethernet statistics show no errors, collisions, or bugger overruns. If any of these problems appear, the FortiGate and switch settings may require adjusting.

Shared traffic shapers are configured in **Firewall > Traffic Shaper > Shared**.

#### Shared page

Lists each individual shared traffic shaper that you created. On this page, you can edit, delete or create a new shared traffic shaper.

- **Create New**: Select to add a new shared traffic shaper.
- **Name**: Type a name for this traffic shaper.
- **Delete**: Select to remove a traffic shaper.
- **Edit**: Select to modify a traffic shaper.

#### New Shared Traffic Shaper page

Provides settings for configuring a new shared traffic shaper.

- **Apply Shaping**: Select **Per Policy** to apply this traffic shaper to a single firewall policy that uses it. Select **For all policies using this shaper** to apply this traffic shaper to all firewall policies that use it.

#### Shaping Methods

Configure the traffic shaping methods used by the shared traffic shaper.

- **Guaranteed Bandwidth**: Select a value 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**: Select to limit bandwidth in order to keep less important services from using bandwidth needed for more important ones. Do not set both Guaranteed Bandwidth and Maximum Bandwidth to 0 (zero), or the firewall policy that the shared traffic shaper is added to will not allow any traffic.

- **Traffic Priority**: Select **High**, **Medium**, or **Low**. Select Traffic Priority so the 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.
Per-IP traffic shaping

Per-IP traffic shaping is applied per IP address, instead of per policy or per shaper. As with the shared traffic shaper, you select the per-IP traffic shaper in firewall policies. Per-IP traffic shaping is configured in Firewall > Traffic Shaper > Per-IP.

Per-IP page

Lists each individual Per-IP traffic shaper that you created. On this page, you can edit, delete or create a new Per-IP traffic shaper.

**Create New**

Creates a new per-IP traffic shaper. When you select Create New, you are automatically redirected to the New Per-IP Traffic Shaper page.

**Delete**

Removes a per-IP traffic shaper. To remove multiple per-traffic shapers from within the list, on the Per-IP page, in each of the rows of the shapers you want removed, select the check box and then select Delete. To remove all per-traffic shapers from the list, on the Per-IP page, select the check box in the check box column and then select Delete.

**Edit**

Modifies settings within a per-IP traffic shaper. When you select Edit, you are automatically redirected to the Edit Per-IP Traffic Shaper page.

**Name**

The name of this per-IP traffic shaper.

**Maximum Bandwidth**

The maximum bandwidth allowed.

**Maximum Concurrent Connections**

The maximum number of concurrent connections.

**New Per-IP Traffic Shaper page**

Provides settings for configuring a per-IP traffic shaper. These per-IP traffic shapers are each made up of an IP address, and this per-IP traffic shaper is applied to a firewall policy.

**Name**

Enter a name for the per-IP traffic shaper.

**Maximum Bandwidth**

Select the check box beside Maximum Bandwidth to enable this setting. Enter the maximum allowed bandwidth in Kbps. This limit applies to each IP address. Range 1 to 2,097,000. Enter 0 to disable bandwidth limit.

**Maximum Concurrent Connections**

Select the check box beside Maximum Concurrent Connection to enable this setting. Enter the maximum allowed concurrent connection.

Virtual IP

Virtual IPs can specify translations of packets' port numbers and/or IP addresses for both inbound and outbound connections. In Transparent mode, virtual IPs are available from the CLI.

This topic contains the following:

- Virtual IP, load balance virtual server and load balance real server limitations
- VIP group
- IP pools
Virtual IP, load balance virtual server and load balance real server limitations

The following limitations apply when adding virtual IPs, Load balancing virtual servers, and load balancing real servers. Load balancing virtual servers are actually server load balancing virtual IPs. You can add server load balance virtual IPs from the CLI.

- Virtual IP External IP Address/Range entries or ranges cannot overlap with each other or with load balancing virtual server Virtual Server IP entries.
- A virtual IP Mapped IP Address/Range cannot be 0.0.0.0 or 255.255.255.255.
- A real server IP cannot be 0.0.0.0 or 255.255.255.255.
- If a static NAT virtual IP External IP Address/Range is 0.0.0.0, the Mapped IP Address/Range must be a single IP address.
- If a load balance virtual IP External IP Address/Range is 0.0.0.0, the Mapped IP Address/Range can be an address range.
- When port forwarding, the count of mapped port numbers and external port numbers must be the same. The web-based manager does this automatically but the CLI does not.
- Virtual IP and virtual server names must be different from firewall address or address group names.

Virtual IP

A virtual IP’s external IP address can be a single IP address or an IP address range, and is bound to a FortiGate interface. When you bind the virtual IP’s external IP address to a FortiGate interface, by default, the network interface responds to ARP requests for the bound IP address or IP address range. Virtual IPs use proxy ARP, as defined in RFC 1027, so that the unit can respond to ARP requests on a network for a server that is actually installed on another network.

A virtual IP’s mapped IP address can be a single IP address, or an IP address range.

When the unit receives packets matching a firewall policy whose Destination Address field is a virtual IP, the unit applies NAT, replacing the packet’s destination IP address with the virtual IP’s mapped IP address.

To implement the translation configured in the virtual IP or IP pool, you must add it to a NAT firewall policy. For example, to add a firewall policy that maps public network addresses to a private network, add an external to internal firewall policy whose Destination Address field is a virtual IP.

For limitations on creating virtual IPs, see “Virtual IP, load balance virtual server and load balance real server limitations” on page 231.

Virtual IP’s are configured in Firewall > Virtual IP > Virtual IP. Use the following table when configuring virtual IPs.

**Virtual IP page**

Lists each individual virtual IP that you created. On this page, you can edit, delete or create a new virtual IP.

- **Create New**
  Creates a new virtual IP. When you select Create New, you are automatically redirected to the Add New Virtual IP Mapping page.

- **Name**
  The name of the virtual IP.

- **IP**
  The bound network interface and external IP address or IP address, separated by a slash (/).

- **Service Port**
  The external port number or port number range. This field is empty if the virtual IP does not specify port forwarding.
VIP group

You can organize multiple virtual IPs into a virtual IP group to simplify your firewall policy list. For example, instead of having five identical policies for five different but related virtual IPs located on the same network interface, you might combine the five virtual IPs into a single virtual IP group, which is used by a single firewall policy.
Firewall policies using VIP Groups are matched by comparing both the member VIP IP address(es) and port number(s).

VIP groups are configured in Firewall > Virtual IP > VIP Group. Use the following table when configuring VIP groups.

**VIP Group page**
Lists each individual VIP group that you created. On this page, you can edit, delete or create a new VIP group.

- **Create New**: Adds a new VIP group. See "VIP group" on page 232. When you select Create New, you are automatically redirected to the New VIP Group page.
- **Group Name**: The name of the virtual IP group.
- **Members**: Lists the group members.
- **Interface**: Displays the interface that the VIP group belongs to.
- **Delete**: Remove the VIP group from the list. The Delete icon only appears if the VIP group is not being used in a firewall policy. To remove multiple VIP groups from within the list, on the VIP Group page, in each of the rows of the groups you want removed, select the check box and then select Delete. To remove all groups from the list, on the VIP Group page, select the check box in the check box column, and then select Delete.
- **Edit**: Modifies the settings within the VIP group. When you select Edit, you are automatically redirected to the Edit VIP Group page.

**New VIP Group page**
Provides settings for defining VIPs in a group.

- **Group Name**: Enter or modify the group name.
- **Interface**: Select the interface for which you want to create the VIP group. If you are editing the group, the Interface box is grayed out.
- **Available VIPs and Members**: Select the up or down arrow to move virtual IPs between Available VIPs and Members. Members contains virtual IPs that are a part of this virtual IP group.

**IP pools**
Use IP pools to add NAT policies that translate source addresses to addresses randomly selected from the IP pool, rather than the IP address assigned to that unit interface. In Transparent mode, IP pools are available only from the CLI. ARP replies are disabled in the CLI.

An IP pool defines a single IP address or a range of IP addresses. A single IP address in an IP pool becomes a range of one IP address. For example, if you enter an IP pool as 1.1.1.1 the IP pool is actually the address range 1.1.1.1 to 1.1.1.1.

If a FortiGate interface IP address overlaps with one or more IP pool address ranges, the interface responds to ARP requests for all of the IP addresses in the overlapping IP pools.

IP pools are configured in Firewall > Virtual IP > IP Pools. Use the following table when configuring IP pools.

**IP Pool page**
Lists each individual IP pool that you created. On this page, you can edit, delete or create a new IP pool.

- **Create New**: Adds an IP pool. When you select Create New, you are automatically redirected to the New Dynamic IP Pool page.
- **Name**: The name of the IP pool. Select this name in a firewall policy.
- **Start IP**: Enter the start IP address. This address defines the start of the IP pool address range.
When you use the load balancing function on the unit to intercept the incoming traffic and share it across the available servers, the unit allows multiple servers to respond as if they were a single device or server. This, in turn, means that more simultaneous requests can be handled.

There are additional benefits to server load balancing. Firstly, because the load is distributed across multiple servers, the service being provided can be highly available. If one of the servers breaks down, the load can still be handled by the other servers. Secondly, this increases scalability. If the load increases substantially, more servers can be added behind the unit in order to cope with the increased load.

The following topics are included in this section:

- Virtual servers
- Real servers
- Health check monitors

**Virtual servers**

When you bind the virtual server’s external IP address to a FortiGate interface, by default, the network interface responds to ARP requests for the bound IP address. Virtual servers use proxy ARP, as defined in RFC 1027, so that the unit can respond to ARP requests on a network for a real server that is actually installed on another network. ARP replies are disabled in the CLI.

For limitations on creating virtual servers, see “Virtual IP, load balance virtual server and load balance real server limitations” on page 231.

Virtual servers are configured in Firewall > Load Balance > Virtual Server. Use the following table when configuring virtual servers.

| End IP | Enter the end IP address. This address defines the end of the IP pool address range. |
| Delete | Removes the entry from the list. The Delete icon only appears if the IP pool is not being used in a firewall policy. |
|        | To remove multiple entries from within the list, on the IP Pool page, in each of the rows of the IP pools you want removed, select the check box and then select Delete. |
|        | To remove all entries from within the list, on the IP Pool page, select the check box in the check box column and then select Delete. |
| Edit   | Modifies settings within the IP pool. When you select Edit, you are automatically redirected to the Edit IP Pool page. |

**New Dynamic IP Pool page**

Provides settings for configuring the IP address range and subnet for the IP pool. You can also enter a single IP address for the IP pool.

| Name | Enter the name of the IP pool. |
| IP Range/Subnet | 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 start and end of the IP range does not have to be on the same subnet as the IP address of the interface to which you are adding the IP pool. |

**Load Balance**

When you use the load balancing function on the unit to intercept the incoming traffic and share it across the available servers, the unit allows multiple servers to respond as if they were a single device or server. This, in turn, means that more simultaneous requests can be handled.

There are additional benefits to server load balancing. Firstly, because the load is distributed across multiple servers, the service being provided can be highly available. If one of the servers breaks down, the load can still be handled by the other servers. Secondly, this increases scalability. If the load increases substantially, more servers can be added behind the unit in order to cope with the increased load.

The following topics are included in this section:

- Virtual servers
- Real servers
- Health check monitors

| Edit | Modifies settings within the IP pool. When you select Edit, you are automatically redirected to the Edit IP Pool page. |
| Name | Enter the name of the IP pool. |
| IP Range/Subnet | 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 start and end of the IP range does not have to be on the same subnet as the IP address of the interface to which you are adding the IP pool. |

**Virtual Service page**

Lists each individual virtual server that you created. On this page, you can edit, delete or create a new virtual server.

| Create New | Select to add virtual servers. For more information, see “Virtual servers” on page 234. |
Name         Name of the virtual server.
Type         The protocol load balanced by the virtual server.
Comments     A description of the virtual server.
Virtual Server IP The IP address of the virtual server. This is an IP address on the external interface that you want to map to an address on the destination network.
Virtual server Port The external port number that you want to map to a port number on the destination network. Sessions with this destination port are load balanced by this virtual server.
Load Balance Method The load balancing method for this virtual server.
Health Check  The health check monitor selected for this virtual server. For more information, see “Health Check” on page 237.
Persistence   The type of persistence applied to this virtual server.
Delete       Removes the virtual server from the list. The Delete icon only appears if the virtual server is not bound to a real server.
             To remove multiple virtual servers from within the list, on the Virtual Service page, in each of the rows of virtual servers you want removed, select the check box and then select Delete.
             To remove all virtual servers from the list, on the Virtual Service page, select the check box in the check box column and then select Delete.
Edit         Modifies the virtual server to change any virtual server option including the virtual server name. When you select Edit, you are automatically redirected to the Edit Virtual Server page.

New Virtual Server page
Provides settings for configuring a virtual server.
Name         Enter the name for the virtual server. This name is not the hostname for the unit.
Type         Select the protocol to be load balanced by the virtual server. If you select a general protocol such as IP, TCP, or UDP the virtual server load balances all IP, TCP, or UDP sessions. If you select specific protocols such as HTTP, HTTPS, or SSL you can apply additional server load balancing features such as Persistence and HTTP Multiplexing.

- Select HTTP to load balance only HTTP sessions with destination port number that matches the Virtual Server Port setting. Change Virtual Server Port to match the destination port of the sessions to be load balanced (usually port 80 for HTTP sessions). You can also select HTTP Multiplex. You can also set Persistence to HTTP Cookie to select cookie-based persistence.

- Select HTTPS to load balance only HTTPS sessions with destination port number that matches the Virtual Server Port setting. Change Virtual Server Port to match the destination port of the sessions to be load balanced (usually port 443 for HTTPS sessions). You can also select HTTP Multiplex. You can also set Persistence to HTTP Cookie to select cookie-based persistence. You can also set Persistence to SSL Session ID.

- Select IP to load balance all sessions accepted by the firewall policy that contains this virtual server.

- Select SSL to load balance only SSL sessions with destination port number that matches the Virtual Server Port setting. Change Virtual Server Port to match the destination port of the sessions to be load balanced.

- Select TCP to load balance only TCP sessions with destination port number that matches the Virtual Server Port setting. Change Virtual Server Port to match the destination port of the sessions to be load balanced.

- Select UDP to load balance only UDP sessions with destination port number that matches the Virtual Server Port setting. Change Virtual Server Port to match the destination port of the sessions to be load balanced.
### Interface
Select the virtual server 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.

### Virtual Server IP
The IP address of the virtual server. This is an IP address on the external interface that you want to map to an address on the destination network.

### Virtual server Port
Enter the external port number that you want to map to a port number on the destination network. Sessions with this destination port are load balanced by this virtual server.

### Load Balance Method
Load balancing methods include:

- **Static**: The traffic load is spread evenly across all servers, no additional server is required. This load balancing method provides some persistence because all sessions from the same source address always go to the same server. However, the distribution is stateless, so if a real server is added or removed (or goes up or down) the distribution is changed so persistence will be lost. Separate real servers are not 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.

- **First Alive**: Always directs requests to the first alive real server. In this case “first” refers to the order of the real servers in the virtual server configuration. For example, if you add real servers A, B and C in that order, then traffic always goes to A as long as it is alive. If A goes down then traffic goes to B and if B goes down the traffic goes to C. If A comes back up traffic goes to A. Real servers are ordered in the virtual server configuration in the order in which you add them, with the most recently added real server last. If you want to change the order you must delete and re-add real servers as required.

- **Least RTT**: Directs requests to the server with the least round trip time. The round trip time is determined by a Ping health check monitor and is defaulted to 0 if no Ping health check monitors are added to the virtual server.

- **Least Session**: Directs requests to the server that has the least number of current connections. This method works best in environments where the servers or other equipment you are load balancing have similar capabilities.

### Persistence
Configure persistence to make sure that a user is connected to the same server every time they make a request that is part of the same session. When you configure persistence, the unit load balances a new session to a real server according to the Load Balance Method. If the session has an HTTP cookie or an SSL session ID, the FortiGate unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server.

You can configure persistence if Type is set to HTTP, HTTPS, or SSL.

- **Select None** for no persistence. Sessions are distributed solely according to the Load Balance Method. Setting Load Balance Method to Static (the default) results in behavior equivalent to persistence. See the description of Load Balance Method for more information.

- **Select HTTP Cookie** so that all HTTP or HTTPS sessions with the same HTTP session cookie are sent to the same real server. HTTP Cookie is available if Type is set to HTTP or HTTPS.

- **Select SSL Session ID** so that all sessions with the same SSL session ID are sent to the same real server. SSL Session ID is available if Type is set to HTTPS or SSL.
A real server is configured to bind it to a virtual server. For limitations on creating real servers, see "Virtual IP, load balance virtual server and load balance real server limitations" on page 231.

Real servers are configured in Firewall > Load Balance > Real Server. Use the following table when configuring real servers.
Health check monitors

You can specify which health check monitor configuration to use when polling to determine a virtual server’s connectivity status.

Health check monitor configurations can specify TCP, HTTP or ICMP PING. A health check occurs every number of seconds indicated by the interval. If a reply is not received within the timeout period, and you have configured the health check to retry, it will attempt a health check again; otherwise, the virtual server is deemed unresponsive, and load balancing will compensate by disabling traffic to that server until it becomes responsive again.
Health check monitors are configured in Firewall > Load Balance > Health Check Monitor. Use the following table when configuring health check monitors.

### Health Check Monitor page
Lists each individual health check monitor that you created. On this page, you can edit, delete and create a new health check monitor.

- **Create New**: Creates a new health check monitor. When you select Create New, you are automatically redirected to the Add New Health Check Monitor page.
- **Name**: The name of the health check monitor configuration. The names are grouped by the health check monitor types.
- **Details**: The details of the health check monitor configuration, which vary by the type of the health check monitor, and do not include the interval, timeout, or retry, which are settings common to all types.
  - This field is empty if the type of the health check monitor is PING.
- **Delete**: Removes a health check monitor from the list on the Health Check Monitor page. This option appears only if the health check monitor configuration is not currently being used by a virtual server configuration.
  - To remove multiple health check monitors, on the Health Check Monitor page, in each of the rows of the monitors you want removed, select the check box and then select Delete.
  - To remove all health check monitors, on the Health Check Monitor page, select the check box in the check box column, and then select Delete.
- **Edit**: Modifies settings within the health check monitor configuration. When you select Edit, you are automatically redirected to the Edit Health Check Monitor page.

### Add New Health Check Monitor
Provides settings for configuring a health check monitor.

- **Name**: Enter the name of the health check monitor configuration.
- **Type**: Select the protocol used to perform the health check.
  - TCP
  - HTTP
  - PING
- **Port**: Enter the port number used to perform the health check. If you set the Port to 0, the health check monitor uses the port defined in the real server. This way you can use a single health check monitor for different real servers.
  - This option does not appear if the Type is PING.
- **Interval**: Enter the number of seconds between each server health check.
- **URL**: For HTTP health check monitors, add a URL that the unit uses when sending a get request to check the health of a HTTP server. The URL should match an actual URL for the real HTTP servers. The URL is optional.
  - The URL would not usually include an IP address or domain name. Instead it should start with a “/” and be followed by the address of an actual web page on the real server. For example, if the IP address of the real server is 10.10.10.1, the URL “/test_page.htm” causes the unit to send an HTTP get request to “http://10.10.10.1/test_page.htm”.
  - This option appears only if Type is HTTP.
- **Matched Content**: For HTTP health check monitors, add a phrase that a real HTTP server should include in response to the get request sent by the unit using the content of the URL option. You can use the URL and Matched Content options to verify that an HTTP server is actually operating correctly by responding to get requests with expected web pages. Matched content is only required if you add a URL.
  - For example, you can set Matched Content to “server test page” if the real HTTP server page defined by the URL option contains the phrase "server test page". When the FortiGate unit receives the web page in response to the URL get request, the system searches the content of the web page for the Matched Content phrase.
  - This option appears only if Type is HTTP.
You can monitor the status of each virtual server and real server and start or stop the real servers. The monitored servers can be viewed from Firewall > Load Balance > Monitor.

**Monitor page**
Lists each individual server and real server that is currently being monitored by the unit.

**Virtual Server**
The IP addresses of the existing virtual servers.

**Real Server**
The IP addresses of the existing real servers.

**Health Status**
Display the health status according to the health check results for each real server. A green arrow means the server is up. A red arrow means the server is down.

**Monitor Events**
Display each real server's up and down times.

**Active Sessions**
Display each real server's active sessions.

**RTT (ms)**
Display the Round Trip Time of each real server. By default, the RTT is "<1". This value will change only when ping monitoring is enabled on a real server.

**Bytes Processed**
Display the traffic processed by each real server.

**Graceful Stop/Start**
Select to start or stop real servers. When stopping a server, the unit will not accept new sessions but will wait for the active sessions to finish.
UTM

This section provides an introduction to the UTM menu. If you require more information about the features in the UTM menu, see the FortiOS Handbook.

The following topics are included in this section:

- UTM overview
- AntiVirus
- Intrusion Protection
- Web Filter
- Email Filter
- Data Leak Prevention
- Application Control
- VoIP

UTM overview

The UTM menu provides a number of security features, such as antivirus or DoS sensors. This menu also includes profiles, which are applied to firewall policies. A profile is specific information that defines how the traffic within a policy is examined and what action is taken based on the examination.

The UTM menu contains the following seven features, and some of these features contain profiles which you can then apply to firewall policies:

- Antivirus – provides settings for configuring filtering and scanning of viruses, as well as quarantine settings. This feature also contains settings for choosing an antivirus database that is suited to your network requirements. Profiles are available.

- Intrusion Protection – provides settings for configuring IPS sensors and DoS sensors, including creating customized signatures. You can also view detailed information about the predefined signatures. Default protocol decoders are available to view as well.

- Web filter – provides settings for filtering web content, as well as enabling FortiGuard web filter and FortiGuard web filtering overrides. This feature also includes URL filter, override, local categories, and local ratings configuration settings. Profiles are available.

- Email filtering – also known as anti-spam, provides settings for configuring filtering and scanning banned words, IP addresses, and email addresses. Profiles are available.

- Data Leak Prevention (DLP) – provides settings for creating DLP sensors, compound rules and rules. Instead of profiles, DLP sensors are applied to firewall policies.

- Application Control – provides settings for creating application control black/white lists. You can also view detailed information about applications from the list of applications on the Application List page.

- VoIP – provides settings for creating a VoIP profile, which you can then apply to a firewall policy. This profile also includes enabling logging of SIP and SCCP traffic as well as traffic violations.
AntiVirus

The following explains the antivirus options that you can configure in the Antivirus menu. When configuring a profile, you can apply an antivirus profile to a firewall policy for HTTP, FTP, IMAP, POP3, SMTP, IM, and NNTP sessions. If your unit supports SSL content scanning and inspection you can also configure antivirus protection for HTTPS, IMAPS, POP3S, and SMTPS sessions.

This topic includes the following:

- Profile
- File Filter
- Quarantine
- Quarantine configuration
- Virus Database

Note: If you are currently running FortiOS 4.0 MR2 and have configured the unit to perform a deep inspection using explicit web proxy (HTTPS AV scanning), it will not work properly.

Profile

The Profile page allows you to configure antivirus profiles for applying to firewall policies. A profile is specific information that defines how the traffic within a policy is examined and what action may be taken based on the examination.

You can create multiple antivirus profiles for different antivirus scanning requirements. For example, you create an antivirus profile that specifies only virus scanning for POP3 which you then apply to the out-going firewall policy.

Configure antivirus profiles in UTM > Antivirus > Profile using the following table.

Profile page
Lists each individual antivirus profile that you created. On this page, you can edit, delete or create a new antivirus profile.

Create New
Creates a new antivirus profile. When you select Create New, you are automatically redirected to the New Antivirus Profile page.

Edit
Modifies settings within the antivirus profile. When you select Edit, you are automatically redirected to the Edit Antivirus Profile page.

Delete
Removes an antivirus profile from the list on the Profile page.
To remove multiple antivirus profiles from within the list, on the Antivirus Profile page, in each of the rows of the profiles you want to remove, select the check box and then select Delete.
To remove all antivirus profiles in the list, on the Antivirus Profile page, select the check box in the check box column, and then select Delete.

Name
The name of the antivirus profile.

Comments
A description for the antivirus profile.

New Antivirus Profile page
Provides settings for configuring a new antivirus profile. This page also allows you to configure quarantine settings for including a virus sender to the Banned User List. If you are editing an existing antivirus profile, you are redirected to the Edit Antivirus Profile page, which contains the same settings as in the New Antivirus Profile page.

Name
Enter a name for the profile. If you are editing an existing antivirus profile and want to change the name, enter a new name in this field. You must select OK to save these changes.
The Filter menu allows you to configure filtering options that block specific file patterns and file types. Files are compared to the enabled file patterns and then the file types from top to bottom. If a file does not match any specified patterns or types, it is passed along to antivirus scanning (if enabled). In effect, files are passed if not explicitly blocked. The unit also writes a message to the virus log and sends an alert email message if configured to do so.

The unit can take either of these actions toward files that match a configured file pattern or type:

- Allow: the file is allowed to pass.
- Block: the file is blocked and a replacement messages will be sent to the user. If both file filter and virus scan are enabled, the unit blocks files that match the enabled file filter and does not scan these files for viruses.
Using the allow action, this behavior can be reversed with all files being blocked unless explicitly passed. Simply enter all the file patterns or types 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. For standard operation, you can choose to disable file filter in the profile, and enable it temporarily to block specific threats as they occur.

The unit 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, *.xls?)
- Microsoft Works files (*.wps)
- Visual Basic files (*.vb?)
- screen saver files (*.scr)
- program information files (*.pif)
- control panel files (*.cpl)

The unit can detect the following file types:

### Table 24: Supported file types

<table>
<thead>
<tr>
<th>arj</th>
<th>activemime</th>
<th>aspack</th>
<th>base64</th>
<th>bat</th>
<th>binhex</th>
<th>bzip</th>
<th>bzip2</th>
</tr>
</thead>
<tbody>
<tr>
<td>cab</td>
<td>class</td>
<td>cod</td>
<td>elf</td>
<td>exe</td>
<td>fsg</td>
<td>gzip</td>
<td>hlp</td>
</tr>
<tr>
<td>hta</td>
<td>html</td>
<td>jad</td>
<td>javascript</td>
<td>lzh</td>
<td>mime</td>
<td>msc</td>
<td>msoffice</td>
</tr>
<tr>
<td>petite</td>
<td>prc</td>
<td>rar</td>
<td>sis</td>
<td>tar</td>
<td>upx</td>
<td>uue</td>
<td>zip</td>
</tr>
<tr>
<td>unknown</td>
<td>ignored</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The "unknown" type is any file type that is not listed in the table. The "ignored" type is the traffic the unit typically does not scan. This includes primarily streaming audio and video.

### File filter configuration

You can add multiple file filter lists to the antivirus profile. For file patterns, you can add a maximum of 5000 patterns to a list. For file types, you can select only from the supported types.

File filters are configured in **UTM > Antivirus > File Filter**. Use the following table when configuring file filters.

#### File Filter page

Lists each individual file filter that you created. On this page, you can edit, delete or create a new file filter.

- **Create New**
  - Creates a new file filter. When you select Create New, you are automatically redirected to the File Filter Settings page.

- **Name**
  - The available file filter lists.

- **# Entries**
  - The number of file patterns or file types in each file filter list.

- **DLP Rule**
  - The DLP rules in which each filter is used.

- **Comments**
  - An optional description of each file filter list.
Delete

Removes the file filter list from the list on the File Filter page.

To remove multiple file filter lists from within the list, on the File Filter page, in each of the rows of the file filter lists you want removed, select the check box and then select Delete.

To remove all file filter lists from the list, on the File Filter page, select the check box in the check box column and then select Delete.

Edit

Modifies the settings within a file filter list. When you select Edit, you are redirected to the File Filter Settings page.

File Filter Settings page

Provides settings for configuring multiple file patterns and file types that make up a file filter. This page also lists the file patterns and file types that were created for the file filter. If you are editing a file filter, you are redirected to this page.

Name

File filter name. To change the name, edit the text in the name field and select OK.

Comment

Optional comment. To add or edit comment, enter text in comment field and select OK.

OK

If you make changes to the list name or comments, select OK to save the changes.

Create New

Creates a new file filter pattern or type within the list on the File Filter Settings page. When you select Create New, you are automatically redirected to the New File Filter page.

Disable

Select to disable a file pattern or type.

Delete

Removes the file pattern or type from the list on the File Filter Settings page.

To remove multiple file filter lists from within the list, on the File Filter page, in each of the rows of the file filter lists you want removed, select the check box and then select Delete.

To remove all file filter lists from the list, on the File Filter page, select the check box in the check box column and then select Delete.

Edit

Modifies settings within the file pattern/type and action. When you select Edit, you are automatically redirected to the Edit File Filter page.

Move To

Moves the file pattern or type to any position in the list. When you select Move To, the Move AV File Filter Entry window appears.

To move a file pattern or type, select the new position Before or After, which will place the current entry before or after the entry you enter in (Entry). Enter the entry’s name in the (Entry) field.

Filter

The current list of file patterns and types.

Action

Files matching the file patterns and types can be set to Block or Allow. For information about actions, see “File Filter” on page 243.

Enable

Clear the checkbox to disable the file pattern or type.

New File Filter page

Filter Type

Select File Name Pattern or File Type.

File Type

Select a file type from the list. Appears only when File Type is selected in Filter Type.

Pattern

Enter the file pattern. The file pattern can be an exact file name or can include wildcards. The file pattern can be 80 characters long.

Action

Select an action from the drop down list: Block or Allow. For more information about actions, see “File Filter” on page 243.

Enable

Select to enable or disable the filter.

Note: The default file pattern list catalog is called builtin-patterns.
Quarantine

FortiGate units with a local disk can quarantine blocked and infected files. Detailed information about the file is found in the log file, which is available for viewing in Log&Report > Archive Access > Quarantine. Submit specific files and add file patterns to the AutoSubmit list so they will automatically be uploaded to Fortinet for analysis.

FortiGate units can also quarantine blocked and infected files to a FortiAnalyzer unit, which are also available to view in Log&Report > Archive Access > Quarantine.

Quarantine configuration

You can configure quarantine options for HTTP, FTP, IMAP, POP3, SMTP, IM, and NNTP traffic. If your FortiGate unit supports SSL content scanning and inspection, you can also quarantine blocked and infected files from HTTPS, IMAPS, POP3S, and SMTPS traffic.

Quarantine configuration is located in UTM > Antivirus > Quarantine. Use the following table when configuring quarantine settings.

<table>
<thead>
<tr>
<th>Quarantine Configuration page</th>
<th>Provides settings for configuring the actions the unit takes when infected, suspicious, and blocked files are scanned for viruses. These settings are for the local disk or FortiAnalyzer unit. You can view these settings or modify them from the Quarantine Configuration page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine Infected Files</td>
<td>Select the protocols that you want the unit to look at.</td>
</tr>
<tr>
<td>Quarantine Suspicious Files</td>
<td>Select the protocols that you want the unit to look at.</td>
</tr>
<tr>
<td>Quarantine Blocked Files</td>
<td>Select the check boxes within the protocol columns that you want the FortiGate unit to look at.</td>
</tr>
<tr>
<td>Quarantine To</td>
<td>Select to enable storage of blocked, suspicious and infected files to a FortiAnalyzer unit or local disk. By default, the setting is set to None; you must select FortiAnalyzer if you want to store quarantine files.</td>
</tr>
<tr>
<td>Max Filesize to Quarantine</td>
<td>Appears only when either the FortiAnalyzer unit or local disk is selected as the storage location for quarantine files. The maximum size of quarantined files in MB. Setting the size too large may affect performance.</td>
</tr>
<tr>
<td>Disk Age Limit (only on FortiGate models with local disks)</td>
<td>The time limit in hours which keeps files in quarantine. The age limit is used to formulate the value in the TTL column of the quarantined files list, located in Log&amp;Report &gt; Archive Access &gt; Quarantine. When the limit is reached, the TTL column displays EXP and the file is deleted (although the entry in the quarantined files list is maintained). Entering an age limit of 0 (zero) means files are stored on the local disk indefinitely, depending on what action was chosen in Log Disk space.</td>
</tr>
<tr>
<td>Low Disk space</td>
<td>Select the action to take when the local disk is full: overwrite the oldest file or drop the newest file.</td>
</tr>
<tr>
<td>Enable AutoSubmit (appears only on FortiGate models with local disks)</td>
<td>Select to enable the automatic submission feature.</td>
</tr>
</tbody>
</table>

Use File Pattern Select to enable the automatic upload of the files matching the file patterns in

Use File Status Select to enable the automatic upload of files matching the file patterns in the AutoSubmit list.

Heuristics Select to base the automatic upload of files on their heuristic status.

Block Pattern Select to base the automatic upload of files on their block pattern status.
Virus Database

The unit contains multiple antivirus databases for you to choose from, so that you can get the maximum protection that you need for your network environment. The Virus Database, located in UTM > Antivirus > Virus Database, is used to detect viruses in network traffic. The databases are available on the Virus Database page:

- Regular Virus Database
- Extended Virus Database
- Extreme Virus Database
- Flow-based Virus Database

On the Virus Database page, you can also enable grayware detection. This grayware detection includes adware, dial, downloader, hacker tool, keylogger, RAT, and spyware.

The extended database provides “in the wild” viruses as well as a large collection of zoo viruses that have not yet been seen in current virus studies. An enhanced security environment is best suited for this type of database. The flow-based database provides “in the wild” viruses as well as some commonly seen viruses on the network. Flow-based virus scanning is an alternative to the file-based virus scanning, providing better performance but lower coverage rates than the file-based virus scan.

The extreme antivirus database allows scanning for both “in the wild” and “zoo” viruses that are no longer seen in recent studies as well as all available signatures that are currently supported. The extreme database provides flexibility, providing the maximum protection without sacrificing performance and is suited to an enhanced security environment. The extreme antivirus database is available only on models that have AMC-enabled platforms and large capacity hard drives.

The flow-based antivirus database helps to detect malware using IPS. This database includes “in the wild” viruses along with some commonly seen viruses on the network. The flow-based antivirus database provides an alternative to the file-based virus scan while also providing better performance.

The FortiGuard virus definitions are updated when the unit receives a new version of FortiGuard antivirus definitions from the FDN.

The FortiGuard Center Virus Encyclopedia contains detailed descriptions of the viruses, worms, trojans, and other threats that can be detected and removed by your unit using the information in the FortiGuard virus definitions.

The FortiGuard AV definitions are updated automatically from the FortiGuard Distribution Network (FDN). Automatic antivirus definition updates are configured from the FDN by going to System > Maintenance > FortiGuard. You can also update the antivirus definitions manually from the system dashboard by going to System > Dashboard > Status.

**Note:** If virtual domains are enabled, you must configure antivirus file filtering and antivirus settings in antivirus profiles separately for each virtual domain.

Grayware settings can only be enabled or disabled when running FortiOS 4.0 MR2 or higher on the unit.
Intrusion Protection

The Intrusion Protection system combines signature and anomaly detection and prevention with low latency and excellent reliability. With Intrusion Protection, you can create multiple IPS sensors, each containing a complete configuration based on signatures. Then, you can apply any IPS sensor to a firewall policy. You can also create DoS sensors to examine traffic for anomaly-based attacks.

This topic contains the following:

- IPS Sensor
- DoS sensor
- Predefined
- Custom
- Protocol Decoder

IPS Sensor

You can group signatures into IPS sensors for easy selection when applying to firewall policies. You can define signatures for specific types of traffic in separate IPS sensors, and then select those sensors in profiles designed to handle that type of traffic. For example, you can specify all of the web-server related signatures in an IPS sensor, and that sensor can then be applied to a firewall policy that controls all of the traffic to and from a web server protected by the unit.

The FortiGuard Service periodically updates the pre-defined signatures, with signatures added to counter new threats. Since the signatures included in filters are defined by specifying signature attributes, new signatures matching existing filter specifications will automatically be included in those filters. For example, if you have a filter that includes all signatures for the Windows operating system, your filter will automatically incorporate new Windows signatures as they are added.

Each IPS sensor consists of two parts: filters and overrides. Overrides are always checked before filters.

Each filter consists of a number of signatures attributes. All of the signatures with those attributes, and only those attributes, are checked against traffic when the filter is run. If multiple filters are defined in an IPS Sensor, they are checked against the traffic one at a time, from top to bottom. If a match is found, the unit takes the appropriate action and stops further checking.

A signature override can modify the behavior of a signature specified in a filter. A signature override can also add a signature not specified in the sensor’s filters. Custom signatures are included in an IPS sensor using overrides.

The signatures in the overrides are first compared to network traffic. If the IPS sensor does not find any matches, it then compares the signatures in each filter to network traffic, one filter at a time, from top to bottom. If no signature matches are found, the IPS sensor allows the network traffic.

The signatures included in the filter are only those matching every attribute specified. When created, a new filter has every attribute set to all which causes every signature to be included in the filter. If the severity is changed to high, and the target is changed to server, the filter includes only signatures checking for high priority attacks targeted at servers.

IPS sensors are configured in UTM > Intrusion Protection > IPS Sensor.
**IPS Sensor page**

Lists each individual IPS sensor, either default or ones that you created. On this page you can edit, delete or create a new IPS sensor.

**Create New**

Creates a new IPS sensor. When you select Create New, you are automatically redirected to the New IPS Sensor page. This page provides a name field and comment field. You must enter a name to go the IPS Sensor Settings page.

**Name**

The name of each IPS sensor.

**Comments**

An optional description of the IPS sensor.

**all_defaults (default)**

Includes all signatures. The sensor is set to use the default enable status and action of each signature.

**all_default_pass (default)**

Includes all signatures. The sensor is set to use the default enable status of each signature, but the action is set to pass.

**protect_client (default)**

Includes only the signatures designed to detect attacks against clients and uses the default enable status and action of each signature.

**protect_email_server (default)**

Includes only the signatures designed to detect attacks against servers and the SMTP, POP3, or IMAP protocols and uses the default enable status and action of each signature.

**protect_http_server (default)**

Includes only the signatures designed to detect attacks against servers and the HTTP protocol and uses the default enable status and action of each signature.

**Delete**

Removes the IPS sensor from the list.

To remove multiple IPS sensors from within the list, on the IPS Sensor page, in each of the rows of the sensors you want removed, select the check box and then select Delete.

To remove all IPS sensors from the list, on the IPS Sensor page, select the check box in the check box column and then select Delete.

**Edit**

Modifies settings within an IPS sensor. When you select Edit, you are automatically redirected to the Edit IPS Sensor page.

**IPS Sensor Settings page**

Provides settings for configuring multiple filters and overrides that make up an IPS sensor. The IPS Sensor Settings page also lists filters in the Filters section of the page, and overrides in the Override section of the page. You must select Add Pre-defined Override to add a pre-defined override to the sensor, and you need to select Add Custom Override to add a custom override to the sensor.

**Name**

If you are editing an existing IPS sensor and you want to change the name, enter a new name in the field. You must select OK to save the change.

**Comments**

If you are editing an existing IPS sensor and you want to change the description, enter the changes in the field. You must select OK to save the changes.

**OK**

Select to save changes that you have made to the list.

**Enable Logging**

Select to log the IPS filters and patterns. You can view these logs in Log&Report > Log Access.

**Filters**

This is the Filters section of the IPS Sensor Settings page. This section lists all the filters you have currently configured for the IPS sensor. You can also modify each filter from this area as well as create additional filters.

**Create New**

Creates a new filter. You can also use the Insert icon to create a new filter for an IPS sensor. When you select Create New, you are automatically redirected to the Edit IPS Filter page.

**Edit**

Modifies settings within a filter. When you select Edit, you are automatically redirected to the Edit IPS Filter page.
Delete
Removes a filter from the list within the Filters section of the IPS Sensor Settings page.
To remove multiple filter lists from within the list, in the Filters section, in each of the rows of the filters you want removed, select the check box and then select Delete.

To remove all filters from the list, in the Filters section, select the check box in the check box column and then select Delete.

Insert
Inserts a new filter in filter list in the list in the Filters section. When you select Insert, you are automatically redirected to the Edit IPS Filter page.

Move To
Moves a filter to any position within the list in the Filters section. You must select the check box in the row of the filter you want moved so that filter will be moved within the list.

When you select Move To, the following appears:
Please enter the destination filter position.
Enter the number for the filter's new position within the list, for example, 5 to place the first entry in the fifth position Select OK.

View Rules
View the rules of a filter. When you select View Rules, the Matched Rules window appears. Scroll through the list to see all the rules within that filter.

Name
The name of the filter that you created.

Severity
The severity level of the filter.

Target
The target specified for that filter.

Protocol
The type of protocol for that filter.

OS
The type of operating system.

Application
The software application, such as Adobe.

Enable
A green checkmark appears if you select Enable all within the filter's settings. If you select Disable all, a gray x appears.

Logging
A green checkmark appears if you select Enable all within the filter's settings. A gray x appears if you select Disable all.

Action
The type of action the unit will take. This action can be Block, Pass, or Reset.

Count
The number of signatures included in the filter. Overrides are not included in the total.

Overrides section of the page
This is the Overrides section for the IPS Sensor Settings page. This section lists all the overrides you have currently configured for the IPS sensor.

Edit
Modifies either a custom override or pre-defined override. When you select Edit, you are automatically redirected to Configure IPS Override page.

Delete
Removes a custom override or pre-defined override within the list in the Overrides section of the IPS Sensor Settings page.

To remove multiple overrides from within the list, in the Overrides section, in each of the rows of the overrides you want removed, select the check box and then select Delete.

To remove all overrides from the list, in the Overrides section, select the check box in the check box column and then select Delete.

Add Pre-defined Override
Select to add a pre-defined override. When you select Add Pre-defined Override, you are automatically redirected to the Configure IPS Override page. See "Pre-defined overrides and custom overrides" on page 252.

Add Custom Override
Select to add a custom override. When you select Add Custom Overrides, you are automatically redirected to Configure IPS Override page. See "Pre-defined overrides and custom overrides" on page 252.
Filters

A filter is a collection of signature attributes that you specify. The signatures that have all of the attributes specified in a filter are included in the IPS signature. An IPS sensor can contain multiple IPS filters. The following are the available options when configuring filters.
Filters are configured in the IPS sensor itself, located in UTM > Intrusion Protection > IPS Sensors.

Edit IPS Filter page

Provides settings for configuring a filter. You are automatically redirected to this page when you select Create New in the Filters section of the IPS Sensor Settings page.

Name
Enter a name for the filter.

Severity
Select a severity level. You must specify a severity level if you do not want to allow severity levels.

Target
Select the type of system targeted by the attack.

OS
Select to specify the type of operating system, or select All to include all operating systems. The operating system available include BSD and Solaris. Signatures with an OS attack attribute of All affect all operating system and these signatures are automatically included in any filter regardless of whether a single, multiple, or all operating systems are specified.

Protocol
Select to choose multiple protocols or all available protocols.
To select specific protocols, select Specify, and then move each protocol that you want from the Available column to the Selected column using the -> arrow.
To remove a protocol from the Selected column, select the protocol and then use the <- arrow to move the protocol back to the Available column.

Application
Select to choose multiple applications or all available applications.
To select specific applications, select Specify, and then move each application that you want from the Available column to the Selected column using the -> arrow.
To remove an application from the Selected column, select the protocol and then use the <- arrow to move the application back to the Available column.

Quarantine Attackers (to Banned Users List)

Method
Select Attacker’s IP Address to block all traffic sent from the attacker’s IP address. Traffic from the attacker’s IP address is blocked because the attacker’s IP address is in the Banned Users List.
Select Attacker and Victim IP Addresses to block all traffic sent from the attacker IP address to the target (victim) IP address. Traffic from the attacker IP address to addresses other than the victim IP address is allowed. The attacker and target IP addresses are added to the banned user list as one entry.
Select Attack’s Incoming Interface to block all traffic from connecting to the FortiGate interface that received the attack. The interface is added to the banned user list.

Logging
Select if you want to log the quarantined attacker’s information.

Expires
You can select whether the attacker is banned indefinitely or for a specified number of days, hours, or minutes.

Signature Settings
Configure whether the filter overrules the following signature settings or uses the default settings in the signatures.

Enable
Select from the options to specify what the unit will do with the signatures included in the filter: enable all, disable all, or enable or disable each according to the individual default values as shown in the signature list.
Pre-defined overrides and custom overrides

Pre-defined and custom overrides are configured and work mainly in the same way as filters. Unlike filters, each override defines the behavior of one signature.

Overrides can be used in two ways:

- Change the behavior of a signature already included in a filter. For example, to protect a web server, you could create a filter that includes and enables all signatures related to servers. If you wanted to disable one of those signatures, the simplest way would be to create an override and mark the signature as disabled.

- Add an individual signature that is not included in any filters to an IPS sensor. This is the only way to add custom signatures to IPS sensors.

When a pre-defined signature is specified in an override, the default status and action attributes have no effect. These settings must be explicitly set when creating the override.

When configuring either a pre-defined override or a custom override, the following options are available regardless which override you are configuring.

Predefined and custom overrides are configured in the IPS Sensor itself, located in **UTM > Intrusion Protection > IPS Sensors**. Use the following table when you are configuring predefined and custom overrides within an IPS sensor.

Note: Before an override can affect network traffic, you must add it to a filter, and you must select the IPS sensor and then apply it to a policy. An override does not have the ability to affect network traffic until these steps are taken.

### Configure IPS Override

Provides settings for configuring predefined overrides and custom overrides. You are automatically redirected to this page after selecting either Add Pre-defined Override or Add Custom Override in the Override section of the IPS Sensor Settings page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>Select the browse icon to view the list of available signatures. From this list, select a signature the override will apply to and then select OK.</td>
</tr>
<tr>
<td>Enable</td>
<td>Select to enable the signature override.</td>
</tr>
<tr>
<td>Action</td>
<td>Select Pass, Block or Reset. When the override is enabled, the action determines what the unit will do with traffic containing the specified signature.</td>
</tr>
<tr>
<td>Logging</td>
<td>Select to enable creation of a log entry if the signature is discovered in network traffic.</td>
</tr>
<tr>
<td>Packet Log</td>
<td>Select to save packets that trigger the override to the unit’s hard drive for later examination. For more information, see &quot;Packet logging&quot; on page 258.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Select to enable NAC quarantine for this override. For more information about NAC quarantine, see &quot;The Banned User list&quot; on page 336.</td>
</tr>
<tr>
<td>Attackers (to Banned Users List)</td>
<td>The unit deals with the attack according to the IPS sensor or DoS sensor configuration regardless of this setting.</td>
</tr>
</tbody>
</table>
DoS sensor

IPS uses a traffic anomaly detection feature to identify network traffic that does not fit known or common traffic patterns and behavior. For example, one type of flooding is the denial of service (DoS) attack that occurs when an attacking system starts an abnormally large number of sessions with a target system. The large number of sessions slows down or disables the target system so legitimate users can no longer use it. This type of attack gives the DoS sensor its name, although it is capable of detecting and protecting against a number of anomaly attacks.

You can enable or disable logging for each traffic anomaly, and configure the detection threshold and action to take when the detection threshold is exceeded.

You can create multiple DoS sensors. Each sensor consists of 12 anomaly types that you can configure. When a sensor detects an anomaly, it applies the configured action. One sensor can be selected for use in each DoS policy, allowing you to configure the anomaly thresholds separately for each interface. Multiple sensors allow great granularity in detecting anomalies because each sensor can be configured for the specific needs of the interface it is attached to by the DoS policy.

The traffic anomaly detection list can be updated only when the firmware image is upgraded on the unit.

Since an improperly configured DoS sensor can interfere with network traffic, no DoS sensors are present on a factory default unit. You must create your own and then select them in a DoS policy before they will take effect. Thresholds for newly created sensors are preset with recommended values that you can adjust to meet the needs of your network.
Intrusion Protection UTM

FortiGate Version 4.0 MR2 Administration Guide

01-420-89802-201126

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 allow otherwise avoidable attacks.

Note: If virtual domains are enabled on the unit, the Intrusion Protection settings must be configured separately in each VDOM. All sensors and custom signatures will appear only in the VDOM in which they were created.

DoS Sensor page
Lists each default DoS sensor and each DoS sensor that you created. On this page, you can create, edit or delete a DoS sensor.

Create New
Creates a new DoS sensor. When you select Create New, you are automatically redirected to the New DoS Sensor page. The New DoS Sensor page provides a name field and a comment file; you must enter a name to go to the Edit DoS Sensor page.

Name
The DoS sensor name.

Comments

Delete
Removes a DoS sensor from the list on the DoS Sensor page.
To remove multiple DoS sensors from within the list, on the DoS Sensor page, in each of the rows of the sensors you want removed, select the check box and then select Delete.
To remove all DoS sensors from the list, on the DoS Sensor page, select the check box in the check box column and then select Delete.

Edit
Modifies the settings within a DoS sensor. You can modify the following information: Action, Severity, and Threshold.
When you select Edit, you are automatically redirected to the Edit DoS Sensor page.

Edit DoS Sensor page
Provides settings for configuring the action type, threshold amount, and if logging should be enabled for the anomaly. There are twelve default anomalies to configure settings for. If you are editing a DoS Sensor, you are redirected to this page.

Name
Enter or change the DoS sensor name.

Comments
Enter or change an optional description of the DoS sensor. This description will appear in the DoS sensor list.

Anomalies Configuration

Name
The name of the anomaly.

Enable
Select the check box to enable the DoS sensor to detect when the specified anomaly occurs. Selecting the check box in the header row will enable all anomalies.

Logging
Select the check box to enable the DoS sensor to log when the anomaly occurs. Selecting the check box in the header row will enable logging for all anomalies. Anomalies that are not enabled are not logged.

Action
Select Pass to allow anomalous traffic to pass when the unit detects it, or set Block to prevent the traffic from passing.

Threshold
Displays the number of sessions/packets that must show the anomalous behavior before the FortiGate unit triggers the anomaly action (pass or block). If required, change the number. Range 1 to 2,147,483,647. For more information about how these settings affect specific anomalies, see Table 25 on page 255 and "SYN threshold (preventing SYN floods using a DoS sensor)" on page 255.
SYN proxy

FortiGate units with Fortinet security processing modules installed offer a third action for the tcp_syn_flood threshold when a module is installed. Instead of Block and Pass, you can choose to Proxy the incomplete connections that exceed the threshold value.

When the tcp_syn_flood threshold action is set to proxy, incomplete TCP connections are allowed as normal as long as the configured threshold is not exceeded. If the threshold is exceeded, the unit will intercept incoming SYN packets from clients and respond with a SYN+ACK packet. If the unit receives an ACK response as expected, it will “replay” this exchange to the server to establish a communication session between the client and the server, and allow the communication to proceed.

SYN threshold (preventing SYN floods using a DoS sensor)

The preferred primary defines against any type of SYN flood is the DoS sensor tcp_syn_flood threshold. The threshold value sets an upper limit on the number of new incomplete TCP connections allowed per second. If the number of incomplete connections exceeds the threshold value, and the action is set to Pass, the unit will allow the SYN packets that exceed the threshold. If the action is set to Block, the unit will block the SYN packets that exceed the threshold, but it will allow SYN packets from clients that send another SYN packet.

The tools attackers use to generate network traffic will not send a second SYN packet with a SYN+ACK response is not received from the server. These tools will not “retry”. Legitimate clients will retry when no response is received, and these retries are allowed even if they exceed the threshold with the action set to Block.

Understanding the anomalies

For each of the TCP, UDP, and ICMP protocols, DoS sensors offer four statistical anomaly types. The result is twelve configurable anomalies, which are shown in Table 25.

Table 25: The twelve individually configurable anomalies

<table>
<thead>
<tr>
<th>Anomaly</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp_syn_flood</td>
<td>If the SYN packet rate, including retransmission, to one destination IP</td>
</tr>
<tr>
<td></td>
<td>address exceeds the configured threshold value, the action is executed.</td>
</tr>
<tr>
<td></td>
<td>The threshold is expressed in packets per second.</td>
</tr>
<tr>
<td>tcp_port_scan</td>
<td>If the SYN packets rate, including retransmission, from one source IP</td>
</tr>
<tr>
<td></td>
<td>address exceeds the configured threshold value, the action is executed.</td>
</tr>
<tr>
<td></td>
<td>The threshold is expressed in packets per second.</td>
</tr>
<tr>
<td>tcp_src_session</td>
<td>If the number of concurrent TCP connections from one source IP address</td>
</tr>
<tr>
<td></td>
<td>exceeds the configured threshold value, the action is executed.</td>
</tr>
<tr>
<td>tcp_dst_session</td>
<td>If the number of concurrent TCP connections to one destination IP address</td>
</tr>
<tr>
<td></td>
<td>exceeds the configured threshold value, the action is executed.</td>
</tr>
<tr>
<td>udp_flood</td>
<td>If the UDP traffic to one destination IP address exceeds the configured</td>
</tr>
<tr>
<td></td>
<td>threshold value, the action is executed.</td>
</tr>
<tr>
<td></td>
<td>The threshold is expressed in packets per second.</td>
</tr>
<tr>
<td>udp_scan</td>
<td>If the number of UDP sessions originating from one source IP address</td>
</tr>
<tr>
<td></td>
<td>exceeds the configured threshold value, the action is executed.</td>
</tr>
<tr>
<td></td>
<td>The threshold is expressed in packets per second.</td>
</tr>
<tr>
<td>udp_src_session</td>
<td>If the number of concurrent UDP connections from one source IP address</td>
</tr>
<tr>
<td></td>
<td>exceeds the configured threshold value, the action is executed.</td>
</tr>
<tr>
<td>udp_dst_session</td>
<td>If the number of concurrent UDP connections to one destination IP address</td>
</tr>
<tr>
<td></td>
<td>exceeds the configured threshold value, the action is executed.</td>
</tr>
<tr>
<td>icmp_flood</td>
<td>If the number of ICMP packets sent to one destination IP address</td>
</tr>
<tr>
<td></td>
<td>exceeds the configured threshold value, the action is executed.</td>
</tr>
<tr>
<td></td>
<td>The threshold is expressed in packets per second.</td>
</tr>
</tbody>
</table>
The Intrusion Protection system can use signatures once you have grouped the required signatures in an IPS sensor. If required, you can override the default settings of the signatures specified in an IPS sensor. The unit provides a number of pre-built IPS sensors, but you should check their settings before using them, to ensure they meet your network requirements.

By using only the signatures you require, you can improve system performance and reduce the number of log messages and alert email messages that the IPS sensor generates. For example, if the unit is not protecting a web server, web server signatures are not included.

The predefined signature list, located in UTM > Intrusion Protection > Predefined, includes signatures that are currently in the FortiGuard Center Vulnerability Encyclopedia. This encyclopedia also includes additional signatures not found in the Predefined menu. Each signature name is a link to the vulnerability encyclopedia entry for the signature. The vulnerability encyclopedia describes the attack detected by the signature and provides recommended actions and links for more information.

The predefined signature list also includes characteristics such as severity of the attack, protocol, and applications affected for each signature. These characteristics give you a quick reference to what the signature is for. You can also use these characteristics to sort the signature list, grouping signatures by common characteristics. The signature list also displays the default action, the default logging status, and whether the signature is enabled by default. The signatures are sorted by name, which is default.

You can view predefined signatures in UTM > Intrusion Protection > Predefined. Use the following table when viewing the predefined signatures.

### Table 25: The twelve individually configurable anomalies (Continued)

<table>
<thead>
<tr>
<th>Anomaly</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp_sweep</td>
<td>If the number of ICMP packets originating from one source IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.</td>
</tr>
<tr>
<td>icmp_src_session</td>
<td>If the number of concurrent ICMP connections from one source IP address exceeds the configured threshold value, the action is executed.</td>
</tr>
<tr>
<td>icmp_dst_session</td>
<td>If the number of concurrent ICMP connections to one destination IP address exceeds the configured threshold value, the action is executed.</td>
</tr>
</tbody>
</table>

**Predefined**

The Intrusion Protection system can use signatures once you have grouped the required signatures in an IPS sensor. If required, you can override the default settings of the signatures specified in an IPS sensor. The unit provides a number of pre-built IPS sensors, but you should check their settings before using them, to ensure they meet your network requirements.

By using only the signatures you require, you can improve system performance and reduce the number of log messages and alert email messages that the IPS sensor generates. For example, if the unit is not protecting a web server, web server signatures are not included.

The predefined signature list, located in UTM > Intrusion Protection > Predefined, includes signatures that are currently in the FortiGuard Center Vulnerability Encyclopedia. This encyclopedia also includes additional signatures not found in the Predefined menu. Each signature name is a link to the vulnerability encyclopedia entry for the signature. The vulnerability encyclopedia describes the attack detected by the signature and provides recommended actions and links for more information.

The predefined signature list also includes characteristics such as severity of the attack, protocol, and applications affected for each signature. These characteristics give you a quick reference to what the signature is for. You can also use these characteristics to sort the signature list, grouping signatures by common characteristics. The signature list also displays the default action, the default logging status, and whether the signature is enabled by default. The signatures are sorted by name, which is default.

You can view predefined signatures in UTM > Intrusion Protection > Predefined. Use the following table when viewing the predefined signatures.

**Note:** If virtual domains are enabled on the unit, the Intrusion Protection settings are configured separately in each VDOM. All sensors and custom signatures will appear only in the VDOM in which they were created.

**Predefined page**

Lists each predefined signature that is currently on your unit. When you select the name of the signature, you are automatically redirected to that signature’s detailed definition in the FortiGuard Center Vulnerability Encyclopedia. This page also indicates which signatures are enabled and which are disabled.

**Column Settings**

Select to customize the signature information displayed in the table. You can also readjust the column order. For more information, see “Using column settings to control the columns displayed” on page 26 and “Using filters with column settings” on page 27.

**Clear All Filters**

If you have applied filtering to the predefined signature list display, select this option to clear all filters and display all the signatures.
Custom signatures provide the power and flexibility to customize the Intrusion Protection system for diverse network environments. The predefined signatures represent common attacks. If you use an unusual or specialized application or an uncommon platform, you can 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.

After creating custom signatures, you need to specify them in IPS sensors that were created to scan traffic.

Use custom signatures to block or allow specific traffic. For example, to block traffic containing profanity, add custom signatures similar to the following:

```
set signature 'F-SBID (--protocol tcp; --flow bi_direction; --pattern "bad words"; --no_case)'
```

Custom signatures must be added to a signature override in an IPS filter to have any effect. Creating a custom signature is a necessary step, but a custom signature does not affect traffic simply by being created.

Custom signatures are configured in UTM > Intrusion Protection > Custom. Use the following table when configuring custom signatures.

### Tip:
To determine what effect IPS protection will have on your network traffic, enable the required signatures, set the action to pass, and enable logging. Traffic will not be interrupted, but you will be able to examine, in detail, which signatures were detected.

### Caution:
Custom signatures are an advanced feature. This document assumes the user has previous experience creating intrusion detection signatures.

### Note:
If virtual domains are enabled on the unit, the Intrusion Protection settings are configured separately in each VDOM. All sensors and custom signatures will appear only in the VDOM in which they were created.
Protocol Decoder

The Intrusion Protection system uses protocol decoders to identify the abnormal traffic patterns that do not meet the protocol requirements and standards. For example, the HTTP decoder monitors traffic to identify any HTTP packets that do not meet the HTTP protocol standards.

The decoder list is provided for your reference and can be configured using the CLI. You can view protocol decoders in UTM > Intrusion Protection > Protocol Decoder.

Upgrading the IPS protocol decoder list

The Intrusion Protection system protocol decoders are upgraded automatically through the FortiGuard Distribution Network (FDN) if existing decoders are modified or new decoders added. The FDN keeps the protocol decoder list up-to-date with protection against new threats such as the latest versions of existing IM/P2P as well as against new applications.

Packet logging

Packet logging is a way you can debug custom signatures or how any signature is functioning in your network environment.

If a signature is selected in a custom override, and packet logging is enabled, the unit will save any network packet triggering the signature to memory, the internal hard drive (if so equipped), a FortiAnalyzer, or the FortiGuard Analysis and Management Service. These saved packets can later be viewed and saved in PCAP format for closer examination.
Packet logs are enabled in either a pre-defined override or a custom override, within an IPS sensor. IPS sensors are located in UTM > Intrusion Protection > IPS Sensor.

Packet logging configuration

Packet logging saves the network packets matching an IPS signature to the attack log. This log type is for use as a type of diagnostic tool. The unit saves the logged packets to wherever logs are configured to be stored, such as a FortiAnalyzer unit.

Packet logging is available only in signature overrides. It is not an available option in IPS sensors or filters because enabling packet logging on a large number of signatures could produce an unusable large amount of data.

There are a number of CLI commands available to further configure packet logging. When logging to memory, the packet-log-memory command defines the maximum amount of memory is used to store logged packets. This command only takes effect when logging to memory.

Since only the packet containing the signature is sometimes not sufficient to troubleshoot a problem, the packet-log-history command allows you to specify how many packets are captured when an IPS signature is found in a packet. If the value is set to larger than 1, the packet containing the signature is saved in the packet log, as well as those preceding it, with the total number of logged packets equaling the value. For example, if packet-log-history is set to 7, the unit will save the packet containing the IPS signature and the six before it.

After the unit logs packets, you can view or save them. You can save logged packets as PCAP files. PCAP files can be opened and examined in network analysis software such as Wireshark.

Note: Setting packet-log-history to a value larger than 1 can affect the maximum performance of the unit because network traffic must be buffered. The performance penalty depends on the model, the setting, and the traffic load.

Web Filter

The following explains the web filtering options in the Web Filtering menu. If your unit supports SSL content scanning and inspection you can also configure web filtering for HTTPS traffic.

This topic includes the following:

- Profile
- Web Content Filter
- URL Filter
- Override
- Local Categories
- Local Ratings
- FortiGuard Quota

Profile

The Profile menu allows you to configure a web filter profile to apply to a firewall policy. A profile is specific information that defines how the traffic within a policy is examined and what action may be taken based on the examination.
If you want to use the SSL Proxy exemption by FortiGuard category feature, you must enable this feature in the FortiGuard Web Filtering section of the New Web Filter Profile page. The SSL Proxy exemption feature allows a FortiGuard category to bypass proxy setup for connection to certain destinations that are based on a FortiGuard category. This web filtering check does not check if the connection should be exempted and blocking or logging of traffic occurs in the HTTP proxy as normal.

Web filter profiles are configured in **UTM > Web Filter > Profile**. Use the following table when configuring web filter profiles.

<table>
<thead>
<tr>
<th><strong>Profile page</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists each web filter profile that you created. On this page, you can edit, delete or create a new web filter profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Create New</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a new web filter profile. When you select <strong>Create New</strong>, you are automatically redirected to the New Web Filter Profile page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Edit</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Modifies settings within a web filter profile. When you select <strong>Edit</strong>, you are automatically redirected to the Edit Web Filter Profile page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Delete</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes a web filter profile from within the list on the Profile page. To remove multiple web filter profiles from within the list, on the Profile page, in each of the rows of the file filter lists you want removed, select the check box and then select <strong>Delete</strong>. To remove all web filter profiles from the list, on the Profile page, select the check box in the check box column and then select <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the web filter profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Comments</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A description given to the web filter profile. This is an optional setting.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>New Web Filter Profile page</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides settings for configuring a web filter profile. If you want to enable Web Content Filter, you also need to have a web content filter; and if you want to enable Web URL Filter you must have a URL filter. When editing a web filter profile, you are redirected to the Edit Web Filter Profile page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a name for the web filter profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Comments</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a description for the web filter profile. This is optional.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Web Content Filter</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the protocols to apply web content filtering to. In the Options column, select the web content filter list from the drop-down list. To log web content filtering, select the check box in the Logging column. To apply a threshold, enter a number in the Threshold field.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Web URL Filter</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the protocols to apply web URL filtering to. In the Options column, select a URL filter list from the drop-down list. To log URL filtering, select the check box in the Logging column.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Safe Search</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>When enabled, the supported search engines exclude offensive material from search results. The search engines that you can enable this for are Google, Yahoo! and Bing.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Google</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the check box in the Options column to enforce strict filtering levels of the safe search protection for Google searches. Strict filtering filters both explicit text and images.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Yahoo!</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the check box in the Options column to enforce strict filtering levels of the safe search protection for Yahoo! searches.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Bing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the check box in the Options column to enforce strict filtering levels of the safe search protection for Bing searches.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>FortiGuard Web Filtering</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable and apply FortiGuard Web Filtering options to the profile. Select the check boxes for the protocols that you want to apply FortiGuard web filtering settings to. To enable SSL exempt proxy exemption by FortiGuard category, select the SSL Exempt check box in the row of the category that you want to enable this for. You can apply FortiGuard Quota settings as well. Within <strong>Classification</strong>, you can also apply FortiGuard Quota settings.</td>
</tr>
</tbody>
</table>
Web Content Filter

Web Content Filter allows you to configure lists containing specific words or patterns that control access to web pages. For example, no one can access any web pages with the word Example in it. You can also enter wildcards or Perl regular expressions to filter web content. For more information about wildcards and Perl regular expressions, see “Using wildcards and Perl regular expressions” on page 279.

Note: Perl regular expression patterns are case sensitive for the Web content filter. 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. For more information, see “Using wildcards and Perl regular expressions” on page 279.

With web content filter enabled, in a firewall policy every requested web page is checked against the content filter 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 web filter profile, the page is blocked. The score for a pattern is applied only once even if it appears on the page multiple times.

For each pattern you can select Block or Exempt. Block, blocks access to a web page that matches with the pattern. Exempt allows access to the web page even if other entries in the list that would block access to the page. Web content patterns can be one word or a text string up to 80 characters long. The maximum number of patterns in the list is 5000.
Web content filters are configured in UTM > Web Filter > Web Content Filter.

**Web Content Filter page**
Lists each individual web content filter that you created. On this page, you can edit, delete or create a new web content filters.

- **Create New**: Creates a new web content filter list. When you select Create New, you are automatically redirected to the New List page. The New List page provides a name field and comment field; you must enter a name to go to the Web Content Filter List page.

- **Name**: The name of the web content filter list.

- **# Entries**: The number of content patterns in each web content filter list.

- **Comments**: Optional description of each web content filter list. The comment text must be less than 63 characters long. Otherwise, it will be truncated.

- **Delete**: Removes a web content filter from the page. To remove multiple web content filter lists from within the list, on the Web Content Filter page, in each of the rows of the web content filter lists you want removed, select the check box and then select Delete. To remove all web content filter lists from the list, on the Profile page, select the check box in the check box column and then select Delete.

- **Edit**: Modifies a web content filter. When you select Edit, you are automatically redirected to the Web Content Filter Settings page.

---

**Web Content Filter Settings page**
Provides settings for configuring multiple patterns which make up a web content filter, and also lists the patterns you created for that web content filter. You are automatically redirected to this page from the New List page. If you are editing a web content filter, you are redirected to this page.

- **Name**: If you are editing an existing web content filter and want to change the name, enter a new name in this field. You must select OK to save the change.

- **Comments**: If you are editing an existing web content filter and want to change the description, enter a new description in this field. If you want to change the description, enter the changes here as well. You must select OK to save these changes.

- **Create New**: Creates a new pattern for the web content filter. When you select Create New, you are automatically redirected to the New Pattern page.

- **Enable**: Indicates whether the pattern is enabled or disabled.

- **Pattern**: The current list of patterns that were created for the web content filter.

- **Pattern Type**: The pattern type used in the pattern list entry. Pattern type can be wildcard or regular expression.

- **Language**: The character set to which the pattern belongs: Simplified Chinese, Traditional Chinese, Cyrillic, French, Japanese, Korean, Spanish, Thai, or Western.

- **Action**: Action can be either block or exempt.

- **Score**: A numerical weighting applied to the pattern. The score values of all the matching patterns appearing on a page are added, and if the total is greater than the threshold value set in the web filter profile, the page is blocked. The score value is not applied when Action is set to Exempt.

- **Page Controls**: Use the page controls to view all web content filters within Web Content Filter Settings page.

- **Edit**: Modifies the pattern in the list. When you select Edit, you are automatically redirected to the Edit Pattern page.
### Delete
Removes the pattern in the list.
To remove multiple filters from within the list, on the Web Content Filter Settings page, in each of the rows of the filters you want removed, select the check box and then select Delete.
To remove all filters from the list, on the Web Content Filter Settings page, select the check box in the check box column and then select Delete.

### Enable
Enables the pattern so that it will be used in the list.

### Disable
Disables the pattern so that it will not be used in the list.

### Remove All Entries
Removes all patterns within the list on the Web Content Filter Settings page.

---

#### New Pattern page

<table>
<thead>
<tr>
<th><strong>Action</strong></th>
<th>Select one of:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Block</strong> — If the pattern matches, the Score is added to the total for the web page. The page is blocked if the total score of the web page exceeds the web content block threshold defined in the web filter profile.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Exempt</strong> — If the pattern matches, the web page will not be blocked even if there are matching Block entries.</td>
</tr>
</tbody>
</table>

**Pattern**
Enter the content pattern. Web content patterns can be one word or a text string up to 80 characters long.
For a single word, the unit checks all web pages for that word. For a phrase, the unit checks all web pages for any word in the phrase. For a phrase in quotation marks, the unit checks all web pages for the entire phrase.

**Pattern Type**
Select a pattern type from the dropdown list: Wildcard or Regular Expression.

**Language**
The character set to which the pattern belongs: Simplified Chinese, Traditional Chinese, Cyrillic, French, Japanese, Korean, Spanish, Thai, or Western.

**Score**
Enter a score for the pattern.
When you add a web content list to a web filter profile you configure a web content filter threshold for the profile. When a web page is matched with an entry in the content block list, the score is recorded. If a web page matches more than one entry the score for the web page increases. When the total score for a web page equals or exceeds the threshold, the page is blocked.
The default score for a content list entry is 10 and the default threshold is 10. This means that by default a web page is blocked by a single match. You can change the scores and threshold so that web pages are blocked only if there are multiple matches. For more information, see "Web Filter" on page 259.

**Enable**
Select to enable the entry.
HTTP and FTP client comforting

**Caution:** Client comforting can send unscanned and therefore potentially infected content to the client. You should only enable client comforting if you are prepared to accept this risk. Keeping the client comforting interval high and the amount low will reduce the amount of potentially infected data that is downloaded.

In general, client comforting provides a visual display of progress for web page loading or HTTP or FTP file downloads. Client comforting does this by sending the first few packets of the file or web page being downloaded to the client at configured time intervals so that the client is not aware that the download has been delayed. The client is the web browser or FTP client. Without client comforting, clients and their users have no indication that the download has started until the FortiGate unit has completely buffered and scanned the download. During this delay users may cancel or repeatedly retry the transfer, thinking it has failed.

The appearance of a client comforting message (for example, a progress bar) is client-dependent. In some instances, there will be no visual client comforting cue.

During client comforting, if the file being downloaded is found to be infected, then the unit caches the URL and drops the connection. The client does not receive any notification of what happened because the download to the client had already started. Instead the download stops, and the user is left with a partially downloaded file.

If the user tries to download the same file again within a short period of time, then the cached URL is matched and the download is blocked. The client receives the Infection cache message replacement message as a notification that the download has been blocked. The number of URLs in the cache is limited by the size of the cache.

**FTP and HTTP client comforting steps**

The following steps show how client comforting works for an FTP or HTTP download of a 10 Mbyte file with the client comforting interval set to 20 seconds and the client comforting amount set to 512 bytes.

1. The FTP or HTTP client requests the file.
2. The unit buffers the file from the server. The connection is slow, so after 20 seconds about one half of the file has been buffered.
3. The unit continues buffering the file from the server, and also sends 512 bytes to the client.
4. After 20 more seconds, the unit sends the next 512 bytes of the buffered file to the client.
5. When the file has been completely buffered, the client has received the following amount of data:
   \[ ca \times \left( \frac{T}{ci} \right) \text{ bytes} = 512 \times \left( \frac{40}{20} \right) = 512 \times 2 = 1024 \text{ bytes}, \]
   where \( ca \) is the client comforting amount, \( T \) is the buffering time and \( ci \) is the client comforting interval.
6. **FTP client:** If the file does not contain a virus, the unit sends the rest of the file to the client. If the file is infected, the unit closes the data connection and sends the FTP Virus replacement message to the client.
   **HTTP client:** If the file does not contain a virus, the unit sends the rest of the file to the client. If the file is infected, the unit closes the data connection but cannot send a message to the client.

Caution: Client comforting can send unscanned and therefore potentially infected content to the client. You should only enable client comforting if you are prepared to accept this risk. Keeping the client comforting interval high and the amount low will reduce the amount of potentially infected data that is downloaded.
Character sets and Web content filtering, Email filtering banned word, and DLP scanning

Caution: Specifying multiple character sets reduces web filtering and DLP performance.

The unit converts HTTP, HTTPS, and email content to the UTF-8 character set before applying email filtering banned word checking, web filtering and DLP content scanning as specified in the web filter profile.

For email messages, while parsing the MIME content, the unit converts the content to UTF-8 encoding according to the email message charset field before applying Email filtering banned word checking and DLP scanning.

For HTTP get pages, the unit converts the content to UTF-8 encoding according to the character set specified for the page before applying web content filtering and DLP scanning.

For HTTP post pages, because character sets are not always accurately indicated in HTTP posts, you can use the following CLI command to specify up to five character set encodings.

```
config firewall profile
edit <profile_name>
   set http-post-lang <charset1> [<charset2> ... <charset5>]
end
```

The unit performs a forced conversion of HTTP post pages to UTF-8 for each specified character set. After each conversion the unit applies web content filtering and DLP scanning to the content of the converted page.

To view the list of available character sets, enter `set http-post-lang ?` from within the edit shell for the web filter profile. Separate multiple character set names with a space. You can add up to 5 character set names.

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 unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message.

You can add multiple URL filter lists and then select the best URL filter list for each profile.

You can add the following to block or exempt URLs:

- complete URLs
- IP addresses
- partial URLs to allow or block all sub-domains

Each URL filter list can have up to 5000 entries.

URL filters are configured in `UTM > Web Filter > URL Filter`.

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.
**URL Filter page**

Lists each URL filter that you created. On this page, you can edit, delete or create a new URL filter.

- **Create New**
  Creates a new URL filter list. When you select Create New, you are automatically redirected to the New List page. This page provides a name field and comment field; you must enter a name to go to the URL Filter Settings page.

- **Name**
  The available URL filter lists.

- **# Entries**
  The number of URL patterns in each URL filter list.

- **Comment**
  Optional description of each URL filter list.

- **Delete**
  Removes the URL filter list from the list on the URL Filter page. The Delete icon is only available if the URL filter list is not selected in any profiles.
  - To remove multiple URL filter list from within the list, on the URL Filter page, in each of the rows of the file filter lists you want removed, select the check box and then select Delete.
  - To remove all URL filter list from the list, on the URL Filter page, select the check box in the check box column and then select Delete.

- **Edit**
  Modifies settings within a URL filter list. When you select Edit, you are automatically redirected to the URL Filter Settings page.

**URL Filter Settings page**

Provides settings for configuring URLs that make up the URL filter, and also lists the URLs that you created. You are automatically redirected to this page from the New List Page. If you are editing a URL filter, you are automatically redirected to this page.

- **Name**
  If you are editing an existing URL filter setting and want to change the name, enter a new name in this field. You must select OK to save the change.

- **Comments**
  If you are editing an existing URL filter setting and want to change the description, enter the changes in this field. You must select OK to save these changes.

- **OK**
  Select to save the changes you made to the list.

- **Create New**
  Adds a URL address and filter settings to the list. When you select Create New, you are automatically redirected to the New URL Filter list.

- **Edit**
  Modifies the settings within a URL filter.

- **Delete**
  Removes an entry from the list.
  - To remove multiple URL filters from within the list, on the URL Filter Settings page, in each of the rows of the filters you want removed, select the check box and then select Delete.
  - To remove all URL filters from the list, on the URL Filter Settings page, select the check box in the check box column and then select Delete.

- **Enable**
  Enables a filter in the list.

- **Disable**
  Disables a filter in the list.

- **Move**
  Moves the URL to any position in the list. When you select Move To, the Move URL Filter window appears.
  - To move a URL, select the new position Before or After, which will place the current URL entry before or after the entry you enter in the (URL) field. For example, 1example.com is being moved after 3example.com, so 3example.com is entered in the (URL) field.

- **Remove All Entries**
  Removes all filter entries within the list on the URL Filter Settings page.

**New URL Filter page**

- **URL**
  Enter the URL. Do not include http://. For details about URL formats, see “URL formats” on page 267.

- **Type**
  Select a type from the drop-down list: Simple, Regex (regular expression), or Wildcard.
URL formats

When adding a URL to the URL filter list, follow these rules:

How URL formats are detected when using HTTPS

If your unit does not support SSL content scanning and inspection or if you have selected the URL filtering option in web content profile for HTTPS content filtering mode under Protocol Recognition, filter HTTPS traffic by entering a top level domain name, for example, www.example.com. HTTPS URL filtering of encrypted sessions works by extracting the CN from the server certificate during the SSL negotiation. Since the CN only contains the domain name of the site being accessed, web filtering of encrypted HTTPS sessions can only filter by domain names.

If your unit supports SSL content scanning and inspection and if you have selected Deep Scan, you can filter HTTPS traffic in the same way as HTTP traffic.

How URL formats are detected when using HTTP

URLs with an action set to exempt are not scanned for viruses. If users on the network download files through the unit from trusted web site, 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.

- 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 URL filtering supports standard regular expressions.

Tip: Type a top-level domain suffix (for example, "com" without the leading period) to block access to all URLs with this suffix.
Override

You can modify FortiGuard web filtering overrides for users who may require access to web sites that are blocked by FortiGuard web filtering.

When a user attempts to access a blocked site, if override is enabled in the user's user group, a link appears on the block page directing the user to an authentication form. The user can enter a user name and password to override the FortiGuard web filtering for the the web site.

Overrides are modified in UTM > Web Filter > Override.

Override page

Lists the two default overrides, Administration Overrides and User Overrides. You can modify and add new overrides to each default override. Creating new overrides is not supported.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Modifies an override’s settings.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the override setting.</td>
</tr>
<tr>
<td>Administrative Overrides</td>
<td>The administrative overrides that you can either modify or add administrative overrides to. See “Administrative overrides” on page 268.</td>
</tr>
<tr>
<td>User Overrides</td>
<td>The user overrides that you can modify. See “User overrides” on page 269.</td>
</tr>
</tbody>
</table>

Administrative overrides

Administrative override rules can be modified to allow access to blocked web sites based on directory, domain name, or category. You can also create new overrides within the Administrative Overrides group.

Administrative are backed up with the main configuration and managed by the system. The administrative overrides are not cleaned up when they expire and you can reuse these override entries by extending their expiry dates. You can create administrative overrides using both the CLI and the web-based manager.

Administrative overrides are modified in UTM > Web Filter > Override. Use the following table to modify the existing administrative override settings.

Administrative Overrides page

Lists each individual rule that you created for the Administrative Override. On this page, you can edit, delete or create a new override. You can also disable individual overrides within the list, or delete all overrides within the list.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Adds a a new override rule to the list. When you select Create New, you are automatically redirected to the New Override Rule page. This is not available for User Overrides.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies the settings of an administrative override. When you select Edit, you are automatically redirected to the Edit Override Rule page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes an administrative rule from the list on the Administrative Overrides page. To remove multiple administrative overrides from within the list, on the Administrative Overrides page, in each of the rows of the overrides you want removed, select the check box and then select Delete. To remove all administrative overrides from the list, on the Administrative Overrides page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enables an administrative rule.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables an administrative rule.</td>
</tr>
<tr>
<td>Remove All Entries</td>
<td>Removes all administrative override entries within the list.</td>
</tr>
<tr>
<td>#</td>
<td>The number that displays which order the override is listed in the list.</td>
</tr>
<tr>
<td>Enable</td>
<td>The number identifying the order of the rule in the list.</td>
</tr>
</tbody>
</table>
User overrides

Entries are added to the User Overrides list when a user authenticates to enable a user override. User overrides are not backed up as part of the FortiGate configuration. These overrides are also purged when they expire. Administrators can view and delete user overrides.

Use the following when accessing user overrides from the Override page, in UTM > Web Filter > Override. You cannot modify the entries in the list on the Override page.
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 web filter profile. Users can rate URLs based on the local categories.

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”.

Use the following table when configuring local categories in UTM > Web Filter > Local Categories.

<table>
<thead>
<tr>
<th>Local Categories page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists the individual local categories that you created. Local categories are created when you enter the local category in the Create New field. You cannot modify a local category, only remove it from the list.</td>
</tr>
</tbody>
</table>

| Create New | Enter a local category name in the field and then select Create New. |
| Delete | Select to remove the local category from the list. |
| Local categories | The category or classification in which the URL has been placed. If the URL is rated in more than one category or classification, trailing dots appear. Select the gray funnel to open the Category Filter dialog box. When the list has been filtered, the funnel changes to green. |

Note: If virtual domains are enabled on the unit, web filtering features are configured globally. To access these features, select Global Configuration on the main menu.
Local Ratings

You can configure user-defined categories and then specify the URLs that belong to the category. This allows users to block groups of websites 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.

Local ratings are configured in UTM > Web Filter > Local Ratings.

Local Ratings page

Lists each individual local rating that you created. On this page, you can edit, delete or create a new local rating. You can also disable or enable a local rating, as well as remove all local ratings from the page.

Create New

Creates a new local rating. When you select Create New, you are automatically redirected to the New Local Rating page.

Search

Enter a word or name to search for the local rating within the list. Select Go to start the search.

Edit

Modifies settings within a local rating. When you select Edit, you are automatically redirected to the Edit Local Rating page.

Delete

Select to remove a local rating from the list.

Enable

Enables a local rating within the list on the Local Ratings page.

Disable

Disables a local rating within the list on the Local Ratings page.

Remove All Entries

Removes all local ratings within the list on the Local Ratings page.

#

The number identifying the order of the item in the list.

Enable

A green checkmark appears if the local rating is enabled. A gray x appears if the local rating is disabled.

URL

The URL address of the local rating.

Category

The category that was selected for the local rating.

Page controls

Use to navigate through the list of local ratings.

New Local Rating page

Provides settings for configuring the URL address that belongs to a category and classification rating. When editing a local rating, you are automatically redirected to the Edit Local Rating page which contains the same settings.

URL

Enter the URL address.

Category Rating

Select the ratings for the URL.

Classification Rating

Select to add classifications.

FortiGuard Quota

You can view the web quotas that are monitored in UTM > Web Filter > FortiGuard Quota. This list displays all of the users, which are sorted by user name, who have used up some of their quota time. The list also displays how much time has been used. You can view details of each individual user’s quota by selecting the View icon in the row of the user.

FortiGuard Quota page

Displays each individual users’ used quota.

Page Controls

Use the page controls to navigate through the list on the FortiGuard Quota page.

User Name

The name of the user.
If your unit supports SSL content scanning and inspection you can also configure email filtering for IMAPS, POP3S, and SMTPS email traffic.

You can configure the unit to manage unsolicited commercial email by identifying spam messages from known or suspected spam servers.

The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools, to detect and block a wide range of spam messages. Using FortiGuard Email filtering profile settings you can enable IP address checking, URL checking, E-mail checksum checking, and Spam submission. Updates to the IP reputation and spam signature databases are provided continuously from the global FortiGuard distribution network.

From the FortiGuard Antispam Service page in the FortiGuard center you can use IP and signature lookup to check whether an IP address is blacklisted in the FortiGuard antispam IP reputation database, or whether a URL or email address is in the signature database.

**Order of email filtering**

Email filtering uses various filtering techniques. The order the unit uses these filters depends on the mail protocol used.

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 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 tags as spam the email according to the settings in the email filter profile.

For SMTP and SMTPS if the action is discard the email message is discarded or dropped. 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 or SMTPS email messages are substituted with a configurable replacement message.

**Order of SMTP and SMTPS email filtering**

SMTPS email filtering is available on FortiGate units that support SSL content scanning and inspection.

1. IP address BWL check on last hop IP.
2. DNSBL & ORDBL check on last hop IP, FortiGuard Email Filtering IP address 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 email DNS check, FortiGuard Antispam email checksum check, FortiGuard Email Filtering URL check, DNSBL & ORDBL check on public IP extracted from header.

**Order of IMAP, POP3, IMAPS and POP3S email filtering**

IMAPS and POP3S email filtering is available on units the support SSL content scanning and inspection.

1. MIME headers check, Email address BWL check.
2. Banned word check on email subject.
3. IP BWL check.
4. Banned word check on email body.
5. Return email DNS check, FortiGuard Email Filtering email checksum check, FortiGuard Email Filtering URL check, DNSBL & ORDBL check.

**Profile**

The Profile menu allows you to configure email filter profiles for applying to firewall policies. A profile is specific information that defines how the traffic within a policy is examined and what action may be taken based on the examination.

Email filter profiles are configured in *UTM > Email Filter > Profile*.

<table>
<thead>
<tr>
<th>Profile page</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists each individual email filter profile that you created. On this page, you can edit, delete or create a new email filter profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Create New</strong></td>
<td>Creates a new email filter profile. When you select <em>Create New</em>, you are automatically redirected to the New Email Filter Profile page.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Modifies settings within an email filtering profile. When you select <em>Edit</em>, you are automatically redirected to the Edit Email Filter Profile page.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Removes an email filter profile from the list. To remove multiple email filter profiles from within the list, on the Profile page, in each of the rows of the email filter profiles you want removed, select the check box and then select <em>Delete</em>. To remove all email filter profiles from the list, on the Profile page, select the check box in the check box column and then select <em>Delete</em>.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The name of the email filter profile.</td>
</tr>
<tr>
<td><strong>Comments</strong></td>
<td>The description given to the email filter profile. This is an optional setting.</td>
</tr>
</tbody>
</table>

**New Email Filter Profile page**

Provides settings for configuring multiple email filter profiles. If you are editing an email filter profile, you are automatically redirected to the Edit Email Filter Profile page.

| Name | Enter a name for the email filter profile. |
| Comments | Enter a description about the email filter profile. This is optional. |
| Enable logging | Select to enable logging for the email filter profile. |
| **FortiGuard Email Filtering** | To access the options, you must select the check box beside the column name of the protocol that you want to configure settings. For example, selecting the check box beside IMAP allows you access to the options available for IMAP. |
| **IP Address Check** | Select to enable a check of the FortiGuard IP Address black list. If the IP Address Check is not enabled, the unit does not examine that type of traffic. **Note:** Disabling the traffic types that you do not want checked to save system resources. |
| **URL Check** | Select to enable a check of the FortiGuard URL black list. |
### Email Filter UTM

**Email Checksum Check**
Select to enable the FortiGuard email message checksum check.

**Spam Submission**
Select to add a spam submission message and a link to the message body of all email messages marked as spam by the FortiGuard Email Filtering. If the receiver determines that the email message is not spam, he or she can use the link in the message to inform. You can change the content of this message by going to the Replacement Messages page and customizing the Spam submission message.

**IP Address BWL Check**
Select the IP address black/white list in the Options column from the drop-down list.

**HELO DNS Lookup**
Select to look up the source domain name (from the SMTP HELO command) for SMTP email messages.

**E-mail Address DNS Check**
Select to look up the DNS of the email address.

**Return E-mail DNS Check**
Select to enable checking that the domain specified in the reply to or from address has an A or MX record.

**Banned Word Check**
Select to block email messages based on matching the content of the messages with the words or patterns in the selected email filter banned word list.

**Spam Action**
Select to either tag or discard email that the unit determines to be spam. Tagging adds the text in the Tag Format field to the subject line or header of email identified as spam.

**Tag Location**
Select to add the tag to the subject or MIME header of email identified as spam.

**Tag Format**
Enter a word or phrase with which to tag email identified as spam. When typing a tag, use the same language as the unit’s current administrator language setting. Tag text using other encodings may not be accepted. For example, when entering a spam tag that uses Japanese characters, first verify that the administrator language setting is Japanese, the unit will not accept a spam tag written in Japanese characters while the administrator language setting is English.

Tags must not exceed 64 bytes. The number of characters constituting 64 bytes of data varies by text encoding, which may vary by the FortiGate administrator language setting.

---

## Banned Word

Control spam by blocking email messages containing specific words or patterns. You can add words, phrases, wild cards and Perl regular expressions to match content in email messages. For information, about wild cards and Perl regular expressions, see “Using wildcards and Perl regular expressions” on page 279.
The unit checks each email message against the banned word list. The unit can sort email messages containing those banned 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 email filter profile, the unit processes the message according to the setting in the profile. The score for a pattern is applied only once even if the word appears in the message multiple times.

Banned words are configured in UTM > Email Filter > Banned Word.

### Banned Word page
Lists each banned word list that you created. On this page you can edit, delete or create a new banned word.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new banned word. When you select Create New, you are automatically redirected to the New List page. This page provides a name field and comment field; you must enter a name to go to the Banned Word Settings page.</td>
</tr>
<tr>
<td>Name</td>
<td>The available Email Filter banned word lists.</td>
</tr>
<tr>
<td># Entries</td>
<td>The number of entries in each banned word list.</td>
</tr>
<tr>
<td>Comments</td>
<td>Optional description of each banned word list.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the banned word list from the catalog. The Delete icon is available only if the banned word list is not selected in any email filter profiles. The location where the unit searches for the banned word: Subject, Body, or All.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies the banned word list, list name, or list comment. When you select Edit, you are automatically redirected to the Banned Word Settings page.</td>
</tr>
</tbody>
</table>

### Banned Word Settings page
Provides settings for configuring a word pattern or word that will be considered banned by the unit. These words and word patterns make up a banned word list which appears on the Banned Word page. If you are editing a banned word, you are automatically redirected to the Banned Word Settings page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>If you are editing an existing banned word list and you want to change the name, enter a new name in this field. You must select OK to save these changes.</td>
</tr>
<tr>
<td>Comments</td>
<td>If you are editing an existing banned word list and want to change the description, enter the changes in this field. You must select OK to save these changes.</td>
</tr>
<tr>
<td>OK</td>
<td>Select to save changes in the list.</td>
</tr>
<tr>
<td>Create New</td>
<td>Adds a word or phrase to the banned word list. When you select Create New, you are automatically redirected to the Add Banned Word page.</td>
</tr>
<tr>
<td>Enable</td>
<td>A green checkmark appears if the banned word is enabled.</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>
<tr>
<td>Pattern Type</td>
<td>The pattern type used in the banned word list entry. Choose from wildcard or regular expression. For more information, see “Using wildcards and Perl regular expressions” on page 279.</td>
</tr>
<tr>
<td>Language</td>
<td>The character set to which the banned word belongs.</td>
</tr>
<tr>
<td>Where</td>
<td>The location where the unit searches for the banned word: Subject, Body, or All.</td>
</tr>
</tbody>
</table>
Email Filter

You can add IP address black/white lists and email address black/white lists to filter email. When performing an IP address list check, the unit compares the IP address of the message sender to the IP address list items in sequence. When performing an email list check, the unit compares the email address of the message sender to the email address list items in sequence. If a match is found, the action associated with the IP address or email address is taken. If no match is found, the message is passed to the next enabled email filter.

You can add multiple IP address lists and then select the best one for each email filter profile.
Configure the unit to filter email from specific IP addresses. The unit compares the IP address of the sender to the check 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.

After creating an IP address list, you can add IP addresses to the list.

Enter an IP address or a pair of IP address and mask in the following formats:

- x.x.x.x, for example, 192.168.69.100.
- x.x.x.x/x.x.x.x, for example, 192.168.69.100/255.255.255.0
- x.x.x.x/x, for example, 192.168.69.100/24

IP addresses black/white lists configured in UTM > Email Filter > IP Address. Use the following table when configuring IP addresses black/white lists.

### IP Address page
Lists each individual IP address list that you created. On this page, you can edit, delete or create a new IP address list. An IP address list contains multiple IP addresses and this list is configured in the IP Address Settings page.

- **Create New** Creates a new IP address list. When you select Create New, you are automatically redirected to the New List page. This page provides a name field and comment field; you must enter a name to go to the IPS Address Settings page.

- **Name** The available name of the IP address lists.

- **# Entries** The number of entries in each IP address list.

- **Comments** Optional description of each IP address list.

- **Delete** Removes the IP address black/white list from the list. The delete icon is available only if the IP address list is not selected in any profiles. To remove multiple IP address black/white lists from within the list, on the IP Address page, in each of the rows of the black/white lists you want removed, select the check box and then select Delete. To remove all IP address lists from the list, on the IP Address page, select the check box in the check box column and then select Delete.

- **Edit** Modifies settings within an IP address list. When you select Edit, you are automatically redirected to the IP Address Settings page.

### IP Address Settings page
Provides settings for configuring multiple IP addresses that are then grouped together to form a list of IP addresses. This list is then applied within the email filter profile. You are automatically redirected to this page from the New List page. If you are editing an IP Address, you are automatically redirected to the IP Address Settings page.

- **Name** If you are editing an existing IP address list and want to change the name, enter a new name in this field. You must select OK to save the change.

- **Comments** If you are editing an existing IP address list and want to change the description, enter the changes in this field. You must select OK to save the changes.

- **OK** Select to save modification to the list.

- **Create New** Creates a new IP address with settings. When you select Create New, you are automatically redirected to the Add IP Address page.

- **Edit** Modifies the settings within an IP address. When you select Edit, you are automatically redirected to the Edit IP Address page.
Delete
Removes an IP address from the list.
To remove multiple IP addresses from within the list, on the IP Address Settings page, in each of the rows of the IP addresses you want removed, select the check box and then select Delete.
To remove all IP addresses from the list, on the IP Address Settings page, select the check box in the check box column and then select Delete.

Enable
Enables an IP address within that IP address list.

Disable
Disables an IP address within that IP address list.

Move To
Moves the entry to a different position in the list. When you select Move To, the Move IP Address window appears.
To move an IP address, select the new position Before or After, which will place the current IP address before or after the IP address you enter in the field (IP/Netmask). Enter the IP address and netmask in the (IP/Netmask) field.
The firewall policy executes the list from top to bottom. For example, if you have IP address 192.168.100.1 listed as spam and 192.168.100.2 listed as clear, you must put 192.168.100.1 above 192.168.100.2 for 192.168.100.1 to take effect.

Remove All Entries
Removes all IP addresses from within the list on the IP Address Settings page.

Add IP Address page
IP/Netmask
Enter the IP address or the IP address/mask pair.
Action
Select: Mark as Spam to apply the spam action configured in the profile, Mark as Clear to bypass this and remaining email filters, or Mark as Reject (SMTP or SMTPS) to drop the session.
Enable
Select to enable the address.

E-mail Address page
The unit can filter email from specific senders or all email from a domain (such as example.net). You can add email address lists and then select the best one for each profile.

Email address lists are configured in UTM > Email Filter > E-mail Address. Use the following table when configuring email address lists.

E-mail Address page
Lists each individual email address list that you created. On this page, you can edit, delete or create a new email address list.

Create New
Creates a new email address list. When you select Create New, you are automatically redirected to the New List page. This page provides a name field and comment field; you must enter a name to go to the E-mail Address Settings page.

Name
The name of the email address list.

# Entries
The number of entries in each email address list.

Comments
Optional description of each email address list.

Delete
Removes the email address list from the list on the E-mail Address page. The Delete icon is only available if the email address list is not selected in any profiles.
To remove multiple email address lists from within the list, on the E-mail Address page, in each of the rows of the lists you want removed, select the check box and then select Delete.
To remove all email filter lists from the list, on the E-mail Address page, select the check box in the check box column and then select Delete.

Edit
Modifies settings within an email address list. When you select Edit, you are automatically redirected to the E-mail Address Settings page.
Using wildcards and Perl regular expressions

Email address list, MIME headers list, and banned word list entries can include wildcards or Perl regular expressions.

For more information about using Perl regular expressions, see http://perldoc.perl.org/perlretut.html.
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.

**Note:** To add a question mark (?) character to a regular expression from the FortiGate CLI, enter Ctrl+V followed by ?. To add a single backslash character (\) to a regular expression from the CLI you must add precede it with another backslash character. For example, fortinet\\.com.

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 "atetest", "mytest", "testimony", "atetestb". The notation "\b" specifies the word boundary. To match exactly the word "test", the expression should be \btest\b.

Case sensitivity

Regular expression pattern matching is case sensitive in the web and Email Filter 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 26 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>^a</td>
<td>bc</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>
</tbody>
</table>
Examples of regular expressions

**Block any word in a phrase**

```
/block|any|word/
```

**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.*$/
```

**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\[\+\-\*=<\>\.,;\?!\^\$\%\&\#\@\^\*\$\€\{\}\(\)\[\]\|\_\]dit/i
```

---

Table 26: Perl regular expression formats (Continued)

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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</td>
<td>c</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;acbabcaca&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\s*mk</td>
<td>The strings “100” and “mk” optionally separated by any amount of white space (spaces, tabs, newlines)</td>
</tr>
<tr>
<td>abc\b</td>
<td>&quot;abc&quot; when followed by a word boundary (for example, in &quot;abc!&quot; but not in &quot;abcd&quot;)</td>
</tr>
<tr>
<td>perl\B</td>
<td>&quot;perl&quot; when not followed by a word boundary (for example, in &quot;perlert&quot; but not in &quot;perl stuff&quot;)</td>
</tr>
<tr>
<td>/x</td>
<td>Tells the regular expression parser to ignore white space that is neither preceded by a backslash character nor within a character class. Use this to break up a regular expression into (slightly) more readable parts.</td>
</tr>
<tr>
<td>/x</td>
<td>Used to add regular expressions within other text. If the first character in a pattern is forward slash '/', the '/' is treated as the delimiter. The pattern must contain a second '/' . The pattern between '/' will be taken as a regular expressions, and anything after the second '/' will be parsed as a list of regular expression options (&quot;i&quot;, &quot;x&quot;, etc). An error occurs if the second '/' is missing. In regular expressions, the leading and trailing space is treated as part of the regular expression.</td>
</tr>
</tbody>
</table>
Data Leak Prevention

You can use the Data Leak Prevention (DLP) system to prevent sensitive data from leaving or entering your network. You can define sensitive data patterns, and data matching these patterns will be blocked and/or logged or archived when passing through the unit. The DLP system is configured by creating individual rules, combining the rules into DLP sensors, and then assigning a sensor to a firewall policy.

Although the primary use of the DLP feature is to stop sensitive data from leaving your network, it can also be used to prevent unwanted data from entering your network and to archive some or all of the content passing through the unit.

This topic includes the following:

• Sensor
• Compound rules
• Rule
• DLP archiving

Sensor

Caution: Before use, examine the sensors and rules in the sensors closely to ensure you understand how they will affect the traffic on your network.

DLP sensors are simply collections of DLP rules and DLP compound rules. The DLP sensor also includes settings such as action, archive, and severity for each rule or compound rule. Once a DLP sensor is configured, it can be specified in a firewall policy. Any traffic handled by the policy in which the DLP sensor is specified will enforce the DLP sensor configuration.

You can create a new DLP sensor and configure it to include the DLP rules and DLP compound rules required to protect the traffic leaving your network.

A DLP sensor must be created before it can be configured by adding rules and compound rules.

Sensors are configured in UTM > Data Leak Prevention > Sensor. Use the following table when configuring DLP sensors.

<table>
<thead>
<tr>
<th>Sensor page</th>
<th>Lists each individual DLP sensor that you created, as well as the default DLP sensors. On this page, you can edit DLP sensors (default or ones that you created), delete or create new DLP sensors.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new DLP sensor. When you select Create New, you are automatically redirected to the New DLP List page. This page provides a name field and comment field; you must enter a name to go to the Sensor Settings page.</td>
</tr>
<tr>
<td>Name</td>
<td>The DLP sensor name. There are six default sensors. The following default DLP sensors are provided with your unit. You can use these as provided, or modify them as required.</td>
</tr>
</tbody>
</table>
## Content_Archive
*(default)*

DLP archive all email (POP3, IMAP, and SMTP), FTP, HTTP, and IM traffic. For each rule in the sensor, *Archive* is set to *Full*. No blocking or quarantine is performed. See “DLP archiving” on page 291.

You can add the *All-Session-Control* rule to also archive session control content.

If you have a unit that supports SSL content scanning and inspection, you can edit the *All-Email* rule to archive POP3S, IMAPS, and SMTPS traffic. You can also edit the *All-HTTP* rule to archive HTTPS traffic.

## Content_Summary
*(default)*

DLP summary archive all email (POP3, IMAP, and SMTP), FTP, HTTP, and IM traffic. For each rule in the sensor, *Archive* is set to *Summary Only*. No blocking or quarantine is performed. See “DLP archiving” on page 291.

You can add the *All-Session-Control* rule to also archive session control content.

If you have a unit that supports SSL content scanning and inspection, you can edit the *All-Email* rule to archive POP3S, IMAPS, and SMTPS traffic.

You can also edit the *All-HTTP* rule to archive HTTPS traffic.

## Credit-Card
*(default)*

The number formats used by American Express, Visa, and Mastercard credit cards are detected in HTTP and email traffic.

As provided, the sensor is configured not to archive matching traffic and an action of *None* is set. Configure the action and archive options as required.

## Large-File
*(default)*

Files larger than 5MB will be detected if attached to email messages or if sent using HTTP or FTP.

As provided, the sensor is configured not to archive matching traffic and an action of *None* is set. Configure the action and archive options as required.

## SSN-Sensor
*(default)*

The number formats used by U.S. Social Security and Canadian Social Insurance numbers are detected in email and HTTP traffic.

As provided, the sensor is configured not to archive matching traffic and an action of *None* is set. Configure the action and archive options as required.

## Comments

The optional description of the DLP sensor.

## Delete

Removes a DLP sensor from the list.

To remove multiple DLP sensors from within the list, on the Sensor page, in each of the rows of the sensors you want removed, select the check box and then select *Delete*.

To remove all DLP sensors from the list, on the Sensor page, select the check box in the check box column and then select *Delete*.

## Edit

Modifies settings within a DLP sensor. When you select *Edit*, you are automatically redirected to the Edit DLP Sensor page.

## Clone

Select to use an existing DLP sensor’s settings as the basis for a new DLP sensor’s settings.

---

### Sensor Settings page

Provides settings for configuring rules that are added to DLP sensors. When you select *Create New* to create a new sensor, you are automatically redirected to the New DLP Sensor page. You must enter a name for the sensor in the Name field to continue configuring the sensor, at which time you are redirected to the Sensor Settings page. When you select *Create New* on this page, you are redirected to the New DLP Sensor Rule page.

#### Name

If you are editing an existing sensor and want to change the name, enter a name in this field. You must select OK to save the change.

#### Comment

If you are editing an existing sensor and want to change the description, enter the changes in this field. You must select OK to save these changes.

#### Enable Logging

Select to enable logging of the sensor.

#### Enable NAC Quarantine Logging

Select to enable logging of NAC quarantine activity, if the compound rule or rule contains the action *Quarantine IP address* or *Quarantine Interface*.
Compound rules

DLP compound rules are groupings of DLP rules that also change the way they behave when added to a DLP sensor. Individual rules can be configured with only a single attribute. When this attribute is discovered in network traffic, the rule is activated.
Compound rules allow you to group individual rules to specify far more detailed activation conditions. Each included rule is configured with a single attribute, but every attribute must be present before the rule is activated.

For example, create two rules and add them to a sensor:

- Rule 1 checks SMTP traffic for a sender address of spammer@example.com
- Rule 2 checks SMTP traffic for the word “sale” in the message body

When the sensor is used, either rule could be activated its configured condition is true. If only one condition is true, only the corresponding rule would be activated. Depending on the contents of the SMTP traffic, neither, either, or both could be activated.

If you remove these rules from the sensor, add them to a compound rule, and add the compound rule to the sensor, the conditions in both rules have to be present in network traffic to activate the compound rule. If only one condition is present, the message passes without any rule or compound rule being activated.

By combining the individually configurable attributes of multiple rules, compound rules allow you to specify far more detailed and specific conditions to trigger an action.

Compound rules for DLP sensors are configured in UTM > Data Leak Prevention > Compound.

**Compound page**

Lists the compound rules that you created. On this page, you can edit, delete or create new compound rules.

**Create New**

Creates a new compound rule. When you select Create New, you are automatically redirected to the New/Edit Compound Rule page.

**Name**

The compound rule name.

**Comments**

The optional description of the compound rule.

**DLP sensors**

If the compound rule is used in any sensors, the sensor names are listed here.

**Edit**

Modifies settings within a compound rule. When you select Edit, you are automatically redirected to the New/Edit Compound Rule page.

**Delete**

Removes a compound rule from within the list on the Compound page. If a compound rule is used in a sensor, the Delete icon will not be available. Remove the compound rule from the sensor and then delete it. To remove multiple compound rules from within the list, on the Compound page, in each of the rows of the compound rules you want removed, select the check box and then select Delete. To remove all compound rules from the list, on the Compound page, select the check box in the check box column and then select Delete.

**Clone**

Select to use an existing compound rule’s settings as the basis for a new compound rule.

**New/Edit Compound Rule page**

Provides settings for configuring compound rules. When you edit an existing compound rule, you are automatically redirected to this page.

**Name**

Enter a name for the compound rule.

**Comments**

An optional description of the compound rule.

**Protocol**

Select the type of content traffic that the DLP compound rule applies to. The rules that you can add to the compound rule vary depending on the protocol that you select. You can select the following protocols: Email, HTTP, FTP, NNTP, and Instant Messaging.

**AIM, ICQ, MSN, Yahoo!**

When you select the Instant Messaging protocol, you can select the supported IM protocols for which to add rules. Only the rules that include all of the selected protocols can be added to the compound rule.
Data Leak Prevention

HTTP POST, HTTP GET
When you select the HTTP protocol, you can configure the compound rule to apply to HTTP post or HTTP get sessions or both. Only the rules that include all of the selected options can be added to the compound rule.

HTTPS POST, HTTPS GET
When you select the HTTP protocol, if your FortiGate unit supports SSL content scanning and inspection, you can configure the compound rule to apply to HTTPS post or HTTPS get sessions or both. Only the rules that include all of the selected options can be added to the compound rule.

To scan these encrypted traffic types, you must set HTTPS Content Filtering Mode to Deep Scan (Decrypt on SSL Traffic) in the Protocol Recognition section of the profile. If URL Filtering is selected, the DLP sensors will not scan HTTPS content.

FTP PUT, FTP GET
When you select the FTP protocol, you can configure the compound rule to apply to FTP put, or FTP get sessions or both. Only the rules that include all of the selected options can be added to the compound rule.

SMTP, IMAP, POP3
When you select the Email protocol, you can select the supported email protocols for which to add rules. Only the rules that include all of the selected protocols can be added to the compound rule.

Rules
Select the rule to include in the compound rule. Only the rules that include all of the selected protocols can be added to the compound rule.

Add Rule/Delete Rule
Use the add rule and delete rule icons to add and remove rules from the compound rule. Select the add rule icon and then select rule from the list.

Caution: Before use, examine the rules closely to ensure you understand how they will affect the traffic on your network.

DLP rules are the core element of the data leak prevention feature. These rules define the data to be protected so the FortiGate unit can recognize it. For example, an included rule uses regular expressions to describe Social Security number:

```
([0-6]\d{2}|7(([0-6]\d|7[0-2]))[ \-]?\d{2}[ \-]?\d{4}
```

Rather than having to list every possible Social Security number, this regular expression describes the structure of a Social Security number. The pattern is easily recognizable by the unit. For more information about regular expressions, see “Using wildcards and Perl regular expressions” on page 279.

DLP rules can be combined into compound rules and they can be included in sensors. If rules are specified directly in a sensor, traffic matching any single rule will trigger the configured action. If the rules are first combined into a compound rule and then specified in a sensor, every rule in the compound rule must match the traffic to trigger the configured action.

Individual rules in a sensor are linked with an implicit OR condition while rules within a compound rule are linked with an implicit AND condition.

Rules are configured in UTM > Data Leak Prevention > Rule. Use the following table when configuring rules.

Note: These rules affect only unencrypted traffic types. If you are using a unit able to decrypt and examine encrypted traffic, you can enable those traffic types in these rules to extend their functionality if required.
Rule page
Lists the rules that you created. On this page, you can edit, delete or create new rules.

Create New
Creates a new rule. When you select Create New, you are automatically redirected to the New/Edit Regular Rule page.

Edit
Modifies a rule’s settings. When you select Edit, you are automatically redirected to the New/Edit Regular Rule page.

Delete
Remove a rule from the list on the Rule page. If a compound rule is used in a compound rule or a sensor, the delete icon will not be available. Remove the compound rule from the compound rule or sensor first, and then delete it.
To remove multiple rules from within the list, on the Rule page, in the each of the rows of rules you want removed, select the check box and then select Delete.
To remove all rules from the list, on the Rule page, select the check box in the check box column and then select Delete.

Clone
Select to use an existing rule’s settings as the basis for a new rule.

Name
The rule name. There are many default rules to choose from that are provided with your unit. You can modify the default rules as required.
These rules will detect all traffic of the specified type.

All-Email, All-FTP, All-HTTP, All-IM, All-NNTP, All-Session-Control
These four rules detect American Express numbers, Canadian Social Insurance Numbers, U.S. Social Security Numbers, or Visa and Mastercard numbers within the message bodies of SMTP, POP3, and IMAP email traffic.

Email-AmEx, Email-Canada-SIN, Email-US-SSN, Email-Visa-Mastercard
These four rules detect American Express numbers, Canadian Social Insurance Numbers, U.S. Social Security Numbers, or Visa and Mastercard numbers within HTTP traffic. The HTTP POST is used to send information to a web server.
As written, these rules are designed to detect data the user is sending to web servers. This rule does not detect the data retrieved with the HTTP GET command, which is used to retrieve load web pages.

Email-Not-Webex, HTTP-Post-Not-Webex
These rules prevent DLP from matching email or HTTP pages that contain the string WebEx.

Large-Attachment
This rule detects files larger than 5MB attached to SMTP, POP3, and IMAP email messages.

Large-FTP-Put
This rule detects files larger than 5MB sent using the FTP PUT protocol. Files received using FTP GET are not examined.

Large-HTTP-Post
This rule detects files larger than 5MB sent using the HTTP POST protocol. Files received using HTTP GET are not examined.

Comments
The optional description of the rule.

Compound Rules
If the rule is included in any compound rules, the compound rule names are listed here.

DLP Sensors
If the rule is used in any sensors, the sensor names are listed here.

New/Edit Regular Rule
Provides settings for configuring each type of rule, for example, a rule that is for emails.

Name
The name of the rule.

Comments
An optional comment describing the rule.

Protocol
Select the type of content traffic that the DLP rule the rule will apply to.
The available rule options vary depending on the protocol that you select. You can select the following protocols: Email, HTTP, FTP, NNTP, Instant Messaging and Session Control.
AIM, ICQ, MSN, Yahoo! When you select the *Instant Messaging* protocol, you can configure the rule to apply to file transfers using any or all of the supported IM protocols (AIM, ICQ, MSN, and Yahoo!). Only file transfers using the IM protocols are subject to DLP rules. IM messages are not scanned.

HTTP POST, HTTP GET When you select the *HTTP* protocol, you can configure the rule to apply to HTTP post or HTTP get traffic or both.

HTTPS POST, HTTPS GET When you select the *HTTP* protocol, if your unit supports SSL content scanning and inspection, you can also configure the HTTP rule to apply to HTTPS get or HTTPS post sessions or both. To scan these encrypted traffic types, you must set *HTTPS Content Filtering Mode to Deep Scan (Decrypt on SSL Traffic)* in the Protocol Recognition section of the profile. If *URL Filtering* is selected, the DLP sensors will not scan HTTPS content.

FTP PUT, FTP GET When you select the *FTP* protocol, you can configure the rule to apply to FTP put, or FTP get sessions or both.

SMTP, IMAP, POP3 When you select the *Email* protocol, you can configure the rule to apply to any or all of the supported email protocols (SMTP, IMAP, and POP3).

SMTPS IMAPS POP3S When you select the *Email* protocol, if your unit supports SSL content scanning and inspection, you can also configure the rule to apply to SMTPS, IMAPS, POP3S or any combination of these protocols.

SIP, SIMPLE, SCCP When you select the *Session Control* protocol, you can configure the rule to apply to any or all of the supported session control protocols (SIP, SIMPLE, and SCCP). The only rule option for the session control protocols is *Always*. This option matches all session control traffic is used for session control DLP archiving.

**Rule**

Use the *Rule* settings to configure the content that the DLP rule matches. These settings change according to what protocol is chosen. For example, when the protocol HTTPS is selected, no *Rule* settings appear.

**Note:** For HTTPS, no settings are given because there are none.

**When the protocol type Email is selected in Protocol, the following appear:**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Always</strong></td>
<td>Match any content. This option is available for all protocols.</td>
</tr>
<tr>
<td><strong>Body</strong></td>
<td>Search for the specified string in the message or page body.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>Search for the specified string in the message subject. This option is</td>
</tr>
<tr>
<td></td>
<td>available for Email.</td>
</tr>
<tr>
<td><strong>Sender</strong></td>
<td>Search for the specified string in the message sender user ID or email</td>
</tr>
<tr>
<td></td>
<td>address. This option is available for Email and IM. For email, the sender</td>
</tr>
<tr>
<td></td>
<td>is determined by the From: address in the email header. For IM, all members</td>
</tr>
<tr>
<td></td>
<td>of an IM session are senders and the senders are determined by finding the</td>
</tr>
<tr>
<td></td>
<td>IM user IDs in the session.</td>
</tr>
<tr>
<td><strong>Receiver</strong></td>
<td>Search for the specified string in the message recipient email address.</td>
</tr>
<tr>
<td><strong>Attachment Size</strong></td>
<td>Check the attachment file size.</td>
</tr>
<tr>
<td><strong>Attachment Type</strong></td>
<td>Search email messages for file types or file patterns as specified in the selected file filter.</td>
</tr>
<tr>
<td><strong>Attachment Text</strong></td>
<td>Search for the text within the attachment that uses either UTF-8 or ASCII, and may contain wildcard or regular expression.</td>
</tr>
<tr>
<td><strong>Transfer Size</strong></td>
<td>Check the total size of the information transfer. In the case of email traffic for example, the transfer size includes the message header, body, and any encoded attachment.</td>
</tr>
<tr>
<td><strong>Binary file pattern (enter in base 64)</strong></td>
<td>Search for the specified binary string in network traffic.</td>
</tr>
<tr>
<td><strong>Authenticated User</strong></td>
<td>Search for traffic from the specified authenticated user.</td>
</tr>
<tr>
<td><strong>User group</strong></td>
<td>Search for traffic from any user in the specified user group.</td>
</tr>
</tbody>
</table>
File

Check whether the file is or is not encrypted. Encrypted files are archives and MS Word files protected with passwords. Because they are password protected, the unit cannot scan the contents of encrypted files.

When the protocol type HTTP is selected in Protocol, the following appear:

- **Always**: Match any content. This option is available for all protocols.
- **Body**: Search for the specified string in the message or page body.
- **URL**: Search for the specified URL in HTTP traffic.
- **Transfer Size**: Check the total size of the information transfer. In the case of email traffic for example, the transfer size includes the message header, body, and any encoded attachment.
- **Cookie**: Search the contents of cookies for the specified text. This option is available for HTTP.
- **CGI parameters**: Search for the specified CGI parameters in any web page with CGI code. This option is available for HTTP.
- **HTTP header**: Search for the specified string in HTTP headers.
- **Hostname**: Search for the specified host name when contacting a HTTP server.
- **File type**: Search for the specified file patterns and file types. The patterns and types configured in file filter lists and a list is selected in the DLP rule. For more information about file filter lists, see “File Filter” on page 243.
- **Binary file pattern (enter in base 64)**: Search for the specified binary string in network traffic.
- **Authenticated User**: Search for traffic from the specified authenticated user.
- **User group**: Search for traffic from any user in the specified user group.
- **File**: Check whether the file is or is not encrypted. Encrypted files are archives and MS Word files protected with passwords. Because they are password protected, the unit cannot scan the contents of encrypted files.

When the protocol type FTP is selected in Protocol, the following appear:

- **Always**: Match any content. This option is available for all protocols.
- **Transfer Size**: Check the total size of the information transfer. In the case of email traffic for example, the transfer size includes the message header, body, and any encoded attachment.
- **Server: Start/End**: Search for the server’s IP address in a specified range.
- **File type**: Search for the specified file patterns and file types. The patterns and types configured in file filter lists and a list is selected in the DLP rule. For more information about file filter lists, see “File Filter” on page 243.
- **File text**: Search for the specified text in transferred text files.
- **Binary file pattern (enter in base 64)**: Search for the specified binary string in network traffic.
- **Authenticated User**: Search for traffic from the specified authenticated user.
- **User group**: Search for traffic from any user in the specified user group.
- **File**: Check whether the file is or is not encrypted. Encrypted files are archives and MS Word files protected with passwords. Because they are password protected, the unit cannot scan the contents of encrypted files.

When the protocol type NNTP is selected in Protocol, the following appear:

- **Always**: Match any content. This option is available for all protocols.
- **Body**: Search for the specified string in the message or page body.
Rule operators that appear on the New/Edit Regular Rule page are:

### matches/does not match
This operator specifies whether the unit is searching for the presence of specified string, or for the absence of the specified string.
- **Matches**: The rule will be triggered if the specified string is found in network traffic.
- **Does not match**: The rule will be triggered if the specified string is not found in network traffic.

### ASCII/UTF-8
Select the encoding used for text files and messages.

### Regular Expression/Wildcard
Select the means by which patterns are defined.

For more information about wildcards and regular expressions, see "Using wildcards and Perl regular expressions" on page 279.
DLP archiving

You can use DLP archiving to collect and view historical logs that have been archived to a FortiAnalyzer unit or the FortiGuard Analysis and Management service. DLP archiving is available for FortiAnalyzer when you add a FortiAnalyzer unit to the FortiGate configuration (see "Remote logging to a FortiAnalyzer unit" on page 364). The FortiGuard Analysis and Management server becomes available when you subscribe to the FortiGuard Analysis and Management Service.

You can configure full DLP archiving and summary DLP archiving. Full DLP archiving includes all content, for example, full email DLP archiving includes complete email messages and attachments. Summary DLP archiving includes just the meta data about the content, for example, email message summary records include only the email header.

You can archive Email, FTP, HTTP, IM, and session control content:

- Email content includes IMAP, POP3, and SMTP sessions. Email content can also include email messages tagged as spam by Email filtering. If your unit supports SSL content scanning and inspection, Email content can also include IMAPS, POP3S, and SMTPS sessions.
- HTTP content includes HTTP sessions. If your unit supports SSL content scanning and inspection HTTP content can also include HTTPS sessions.
- IM content includes AIM, ICQ, MSN, and Yahoo! sessions.
- Session control content includes SIP, SIMPLE and SCCP sessions. Only summary DLP archiving is available for SIP and SCCP. Full and summary DLP archiving is available for SIMPLE.

You add DLP sensors to archive Email, Web, FTP, IM, and session control content. Archiving of spam email messages is configured in the DLP sensor.

DLP archiving is enabled in the DLP sensor itself. DLP sensors are located in UTM > Data Leak Prevention > Sensor. You can also use either Content_Archive or Content_Summary sensors to archive DLP logs instead of creating a new DLP sensor for archiving purposes.

You can now create a session control DLP rule that includes SIP, SIMPLE or SCCP for DLP archiving within the CLI.

Application Control

This section describes how to configure the application control options associated with firewall policies.
By using the UTM feature’s application control, the unit can detect and take action against network traffic depending on the application generating the traffic. Based on Intrusion Protection protocol decoders, application control is a more user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

The unit can recognize the network traffic generated by a large number of applications. You can create application control black/white lists that specify the action to take with the traffic of the applications you need to manage and the network on which they are active. Add application control lists to firewall policies applied to the network traffic you need to monitor.

Fortinet is constantly increasing the list of applications that application control can detect by adding applications to the FortiGuard Application Control Database. Because intrusion protection protocol decoders are used for application control, the application control database is part of the FortiGuard Intrusion Protection System Database and both of these databases have the same version number.

You can find the version of the application control database that is installed on your unit, by going to the License Information dashboard widget and find IPS Definitions version.

You can go to the FortiGuard Application Control List to see the complete list of applications supported by FortiGuard. This web page lists all of the supported applications. You can select any application name to see details about the application.

Figure 7: ISIS.Over.IPv4 application page

This topic includes the following:

- Application Control List
- Application List

**Application Control List**

Each application control list contains details about the application traffic to be monitored and the actions to be taken when it is detected. An application control list must be selected in a firewall policy to take effect.

There are no default application control lists provided.
The unit examines network traffic for the application entries in the listed order, one at a time, from top to bottom. Whenever a match is detected, the action specified in the matching rule is applied to the traffic and further checks for application entry matches are stopped. Because of this, you can use both actions to create a complex rule with fewer entries.

In the Application Control List menu, you can enable monitoring so that your network is being monitored. Network monitoring is available only on models with a hard disk. When you select the check box beside Monitor in the Application Control Lists Setting page, you are enabling network monitoring. You can view this information from the Executive Summary page. For more information about configuring widgets in Log&Report > Report Access > Executive Summary.

Application Control lists are configured in UTM > Application Control > Application Control List. Use the following table when configuring application control lists.

### Application Control Lists page
Lists each individual black/white list that you created. On this page, you can edit, delete and create a new application control list.

<table>
<thead>
<tr>
<th>Create New</th>
<th>Creates a new application control black/white list. When you select Create New, you are automatically redirected to the New Application Control List page. This page provides a name field and a comment field; you must enter a name to go to the Edit Application Control List page where you can then configure settings for the new application control black/white list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The available application control lists.</td>
</tr>
<tr>
<td># of Entries</td>
<td>The number of application rules in each application control list.</td>
</tr>
<tr>
<td>Comments</td>
<td>An optional description of each application control list.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the application control black/white list from within the list on the page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies settings within an application black/white list. When you select Edit, you are automatically redirected to the Edit Application Control List page.</td>
</tr>
</tbody>
</table>

### Edit Application Control List page
Provides settings for configuring the applications for the list. When you are editing a list, you are redirected to this page.

<table>
<thead>
<tr>
<th>Name</th>
<th>If you are editing an existing application control list and want to change the name, enter a new name in the field. You must select OK to save the change.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>If you are editing an existing list and want to change the description, enter the changes in the field. You must select OK to save the change.</td>
</tr>
<tr>
<td>OK</td>
<td>Select to save changes that you made to the Name and/or Comment fields.</td>
</tr>
<tr>
<td>Enable Logging</td>
<td>Select to enable logging for the application control black/white list.</td>
</tr>
<tr>
<td>Enable Monitoring</td>
<td>Select to enable network monitoring.</td>
</tr>
<tr>
<td>Create New</td>
<td>Creates a new application entry. When you select Create New, you are automatically redirected to the New Application Entry page.</td>
</tr>
<tr>
<td>ID</td>
<td>A unique number used primarily when re-ordering application entries.</td>
</tr>
<tr>
<td>Category</td>
<td>The category indicates the scope of the applications included in the application entry if Application is set to all. For example, if Application is all and Category is toolbar, then all the toolbar applications are included in the application entry even though they are not specified individually. If Application is a single application, the value in Category has no effect on the operation of the application entry.</td>
</tr>
</tbody>
</table>
Application
The unit will examine network traffic for the listed application. If Application is all, every application in the selected category is included.

Action
If the unit detects traffic from the specified application, the selected action will be taken.

Logging
If traffic from the specified application is detected, the unit will log the occurrence and the action taken.

Delete
Removes the application control entry in the list.
To remove multiple application control entries from within the list, on the Application Control List Settings page, in each of the rows of the entries you want removed, select the check box and then select Delete.
To remove all application control entries from the list, on the Application Control List Settings page, select the check box in the check box column and then select Delete.

Edit
Modifies settings within the application control entry. When you select Edit you are automatically redirected to the Edit Application Entry page.

Insert
Creates a new application control entry above the entry you highlighted. When you select Insert, you are automatically redirected to the New Application Entry page.

Move To
Moves the application control entry to any position in the list. When you select Move To, the Move Application Control Entry window appears.
To move an application control entry, select the new position Before or After, which will place the current entry before or after the entry you enter in the Application ID field. Use the number found in the ID column when entering the new position in the Application ID field.

Page Controls
Use to navigate through the application control entries within an application control list.

New Application Entry page
Category
The applications are categorized by type. If you want to choose an IM application, for example, select the im category, and the application control list will show only the im applications.
The Category selection can also be used to specify an entire category of applications. To select all IM applications for example, select the im category, and select all as the application. This specifies all the IM applications with a single application control black/white list entry.

Application
The unit will examine network traffic for the listed application. If Application is all, every application in the selected category is included.

Action
If the unit detects traffic from the specified application, the selected action will be taken.

Options
The options that you can select for the list.

Session TTL
The application's session TTL. If this option is not enabled, the TTL defaults to the setting of the config system session-ttl CLI command.

Enable Logging
When enabled, the unit will log the occurrence and the action taken if traffic when the specified application is detected.

Enable Packet Logging
When enabled, the unit will log the occurrence of packet logs which concern application control.
Application List

The application list displays applications, which also shows their popularity and risk. You can view the details of each application by selecting the application’s name; this link redirects you to the FortiGuard Application Control List where the details are given for the application. You can also filter the information that appears in UTM > Application Control > Application List.

You can go to the FortiGuard Application Control List to see the complete list of applications supported by FortiGuard. This web page lists all of the supported applications. You can select any application name to see details about the application.

Application lists are configured in UTM > Application Control > Application List.

**Application List page**

Lists the applications that are available on the unit, which includes their category, popularity rating and risk.

<table>
<thead>
<tr>
<th>Page Controls</th>
<th>Use to navigate through the list to view the applications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Total: 1083]</td>
<td>The maximum number of applications that are in the FortiGuard Application Control List.</td>
</tr>
<tr>
<td>Application Name</td>
<td>The name of the application.</td>
</tr>
<tr>
<td>Category</td>
<td>The category that the application is associated with.</td>
</tr>
<tr>
<td>Popularity</td>
<td>The level of popularity of the application. The popularity contains three levels: low, medium and high.</td>
</tr>
<tr>
<td>Risk</td>
<td>The level of risk associated with the application. The risk contains three levels: low, medium and high.</td>
</tr>
</tbody>
</table>

VoIP

The unit can effectively secure VoIP solutions since it supports VoIP protocols and associates state at the signaling layer with packet flows at the media layer. By using SIP ALG controls, the unit can interpret the VoIP signaling protocols used in the network and dynamically open and close ports (pinholes) for each specific VoIP call to maintain security.

In UTM > VoIP > Profile, you can configure multiple profiles for applying to firewall policies that concern only VoIP protocols.

Profile

The Profile menu allows you to configure VoIP profiles for applying to firewall policies. A profile is specific information that defines how the traffic within a policy is examined and what action may be taken based on the examination.

VoIP profiles are configured in UTM > VoIP > Profile. Use the following table to configure VoIP profiles.

<table>
<thead>
<tr>
<th>Profile page</th>
<th>Lists the profiles that you created for SIP and SCCP protocols. On this page, you can edit, delete or create a new profile for VoIP protocols.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new VoIP profile. When you select Create New, you are automatically redirected to the New VoIP Profile page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies settings within a VoIP profile. When you select Edit, you are automatically redirected to the Edit VoIP Profile page.</td>
</tr>
</tbody>
</table>
Delete | Removes a VoIP profile from the list on the Profile page. To remove multiple VoIP profiles from within the list, on the Profile page, in each of the rows of the profiles you want removed, select the check box and then select Delete. To remove all VoIP profiles from the list, on the Profile page, select the check box in the check box column and then select Delete.

Name | The name of the profile.

Comments | A description about the profile. This is an optional setting.

**New VoIP Profile page**

Provides settings for configuring SIP and SCCP options within the profile. When you edit a VoIP profile, you are automatically redirected to the Edit VoIP Profile page.

**SIP**

Limit REGISTER requests | Enter a number for limiting the time it takes to register requests.

Limit INVITE requests | Enter a number to limit invitation requests.

Enable Logging | Select to log SIP requests.

Enable Logging of Violations | Select to log SIP violations.

**SCCP**

Limit Call Setup | Enter a number to limit call setup time.

Enable Logging | Select to log SCCP.

Enable Logging of Violations | Select to log SCCP violations.

**Log section of the New GTP Profile page**

Log Frequency | Enter the number of messages to drop between logged messages. An overflow of log messages can sometimes occur when logging rate-limited GTP packets exceed their defined threshold. To conserve resources on the syslog server and the FortiOS Carrier unit, you can specify that some log messages are dropped. For example, if you want only every twentieth message to be logged, set a logging frequency of 20. This way, 20 messages are skipped and the next logged. Acceptable frequency values range from 0 to 2147483674. When set to '0', no messages are skipped.

Forwarded Log | Select to log forwarded GTP packets.

Denied Log | Select to log GTP packets denied or blocked by this GTP profile.

Rate Limited Log | Select to log rate-limited GTP packets.

State Invalid Log | Select to log GTP packets that have failed stateful inspection.

Tunnel Limit Log | Select to log packets dropped because the maximum limit of GTP tunnels for the destination GSN is reached.
Extension Log  
Select to log extended information about GTP packets. When enabled, this additional information will be included in log entries:
• IMSI
• MSISDN
• APN
• Selection Mode
• SGSN address for signaling
• SGSN address for user data
• GGSN address for signaling
• GGSN address for user data

Traffic count Log  
Select to log the total number of control and user data messages received from and forwarded to the GGSNs and SGSNs the unit protects.

The unit can report the total number of user data and control messages received from and forwarded to the GGSNs and SGSNs it protects. Alternately, the total size of the user data and control messages can be reported in bytes. The unit differentiates between traffic carried by each GTP tunnel, and also between GTP-User and GTP-Control messages.

The number of messages or the number of bytes of data received from and forwarded to the SGSN or GGSN are totaled and logged if a tunnel is deleted.

When a tunnel is deleted, the log entry contains:
• Timestamp
• Interface name (if applicable)
• SGSN IP address
• GGSN IP address
• TID
• Tunnel duration time in seconds
• Number of messages sent to the SGSN
• Number of messages sent to the GGSN
VPN

This section introduces you to the VPN menu. If you require more information about the features in the VPN menu, see the FortiOS Handbook.

This section contains the following topics:

- IPsec VPN
- SSL VPN

IPsec VPN

The IPsec VPN menu contains settings and options for configuring an IPsec VPN. An IPsec VPN is a virtual private network that uses the IPsec protocol suite to provide security and protection for the virtual private network; this means that any data coming into the network and any data going out is encrypted.

IPsec VPNs that are configured must be configured by using the following general procedure:

1. Define the phase 1 parameters that the unit needs to authenticate remote peers or clients and establish a secure a connection.

2. Define the phase 2 parameters that the unit needs to create a VPN tunnel with a remote peer or dialup client.

   **Note:** You must use steps 1 and 2 if you want the unit to generate unique IPsec encryption and authentication keys automatically. If a remote VPN peer or client requires a specific IPsec encryption or authentication key, you must configure the unit to use manual keys instead. For more information, see “Manual Key” on page 306.

3. Create a firewall policy to permit communication between your private network and the VPN. For a policy-based VPN, the firewall policy action is IPSEC. For an interface-based VPN, the firewall policy action is ACCEPT.

Phase 1 is a group of settings that configure the first part of the IPsec VPN. These settings are used to authenticate remote peers or clients, and establishes a secure connection.

Phase 2 is a group of settings that configure the second and last of the IPsec VPN, and provide the information the unit needs to create a VPN tunnel with a remote peer or dialup client.

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, supported in NAT/Route mode only, creates a virtual interface for the local end of a VPN tunnel.

This topic contains the following:

- Auto Key (IKE)
- Manual Key
- Internet browsing
- Concentrator
MonitoringVPNs

L2TP and IPSec is supported for native Windows XP, Windows Vista and Mac OS X native VPN clients. However, in Mac OS X (OS X 10.6.3, including patch releases) the L2TP feature does not work properly on the Mac OS side. For more information, see the What's New chapter of the FortiOS Handbook.

Auto Key (IKE)

You can configure two VPN peers (or a FortiGate dialup server and a VPN client) to generate unique Internet Key Exchange (IKE) keys automatically during the IPsec phase 1 and phase 2 exchanges.

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.

Two VPN peers are configured in VPN > IPsec > Auto Key (IKE).

Auto Key (IKE) page

Lists each phase 1 and phase 2 configurations of the two VPN peers that make up the IKE key.

Create Phase 1

Creates a new phase 1 tunnel configuration. When you select Create New, you are automatically redirected to the New Phase 1 page. For more information, see “Phase 1 configuration” on page 300.

Create Phase 2

Creates a new phase 2 configuration. When you select Create New, you are automatically redirected to the New Phase 2 page. For more information, see “Phase 2 configuration” on page 304.

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.

Edit

Modifies settings within the configured phase. When you select Edit, you are automatically redirected to the editing page of the phase, for example Edit Phase 1 page.

Delete

Removes a phase from the Auto Key (IKE) page.

To remove multiple phases from the list, on the Auto Key (IKE) page, in each of the rows of the phases you want removed, select the check box and then select Delete.

To remove all phases in the list, on the Auto Key (IKE) page, select the check box in the check box column, and then select Delete.

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.
New Phase 1 page
Provides settings for configuring a phase 1. When you select Create New Phase 1 on the Auto Key (IKE) page, you are automatically redirected to the New Phase 1 page.

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 where the remote connection originates. For a route-based tunnel, the unit also uses the name for the virtual IPsec interface that it creates automatically.

Remote Gateway
Select the category of the remote connection:
- Static IP Address — If the remote peer has a static IP address.
- Dialup User — If one or more FortiClient or FortiGate dialup clients with dynamic IP addresses will connect to the FortiGate unit.
- Dynamic DNS — If a remote peer that has a domain name and subscribes to a dynamic DNS service will connect to the unit.

IP Address
If you selected Static IP Address, type the IP address of the remote peer.

Dynamic DNS
If you selected Dynamic DNS, 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 unit.
By default, the local VPN gateway IP address is the IP address of the interface that you selected. Optionally, you can specify a unique IP address for the VPN gateway in the Advanced settings.

Mode
Select Main (ID Protection) 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.

Authentication Method
Select Preshared Key or RSA Signature.

Pre-shared Key
If you selected Pre-shared Key, type the pre-shared key that the 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 be known only 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 you selected RSA Signature, select the name of the server certificate that the unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. For information about obtaining and loading 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.
### Phase 1 advanced configuration settings

You use the advanced *P1 Proposal* parameters to select the encryption and authentication algorithms that the unit uses to generate keys for the IKE exchange. You can also select these advanced settings to ensure the smooth operation of phase 1 negotiations.

<table>
<thead>
<tr>
<th><strong>Advanced section of the New Phase 1 page</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable IPsec Interface Mode</strong></td>
</tr>
<tr>
<td><strong>IKE Version</strong></td>
</tr>
<tr>
<td><strong>IPv6 Version</strong></td>
</tr>
<tr>
<td><strong>Local Gateway IP</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
**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.

Select one 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 Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.
- **AES192** — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.
- **AES256** — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.

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.
- **SHA256** — Secure Hash Algorithm 2, which produces a 256-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, 5 and 14. At least one of the DH Group settings on the remote peer or client must match one the selections on the FortiGate unit.

**Keylife**

Type the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172,800 seconds.

**Local ID**

If the unit will act as a VPN client and you are using peer IDs for authentication purposes, enter the identifier that the unit will supply to the VPN server during the phase 1 exchange.

If the unit will act as a VPN client, and you are using security certificates for authentication, select the distinguished name (DN) of the local server certificate that the unit will use for authentication purposes.

If the unit is a dialup client and will not be sharing a tunnel with other dialup clients (that is, the tunnel will be dedicated to this FortiGate dialup client), set Mode to Aggressive.

**XAuth**

This option supports the authentication of dialup clients. It is available for IKE v1 only.

- **Disable** — Select if you do not use XAuth.
- **Enable as Client** — If the unit is a dialup client, type the user name and password that the unit will need to authenticate itself to the remote XAuth server.

  - **Enable as Server** — This is available only if Remote Gateway is set to Dialup User. Dialup clients authenticate as members of a dialup user group. You must first create a user group for the dialup clients that need access to the network behind the unit. For more information, see “User Group” on page 324.

You must also configure the unit to forward authentication requests to an external RADIUS or LDAP authentication server. For information about these topics, see “RADIUS” on page 327 or “LDAP” on page 329.
Phase 2 configuration

After IPsec phase 1 negotiations end successfully, you begin phase 2. You configure the phase 2 parameters to define the algorithms that the unit may use to encrypt and transfer data for the remainder of the session. During phase 2, you select specific IPsec security associations needed to implement security services and establish a tunnel.

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.

New Phase 2 page

Provides settings for configuring Phase 2. When you select Create Phase 2 on the Auto Key (IKE) page, you are automatically redirected to the New Phase 2 page.

**Name**
Type a name to identify the phase 2 configuration.

**Phase 1**
Select the phase 1 tunnel configuration. For more information, see “Phase 1 configuration” on page 300. 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.

**Advanced**
Define advanced phase 2 parameters. For more information, see “Phase 2 advanced configuration settings” on page 304.

Phase 2 advanced configuration settings

In phase 2, the FortiGate unit and the VPN peer or client exchange keys again to establish a secure communication channel between them. You select the encryption and authentication algorithms needed to generate keys for protecting the implementation details of Security Associations (SAs). These are called P2 Proposal parameters. The keys are generated automatically using a Diffie-Hellman algorithm.

You can use a number of additional advanced phase 2 settings to enhance the operation of the tunnel.
Advanced section of New Phase 2 page

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, at least one of the proposals that you specify must match configuration on the remote peer.

Initially there are two proposals. Add and Delete icons are next to the second Authentication field. To specify only one proposal, select Delete to remove the second proposal. To specify a third proposal, select Add.

It is invalid to set both Encryption and Authentication to NULL.

Encryption
Select one 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 Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.
- **AES192** — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.
- **AES256** — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.

Authentication
Select one 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.
- **SHA256** — Secure Hash Algorithm 2, which produces a 256-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, 5 or 14). This must match the DH Group that the remote peer or dialup client uses.

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 172 800 seconds, or from 5120 to 2 147 483 648 KB.

Autokey Keep Alive
Select the check box if you want the tunnel to remain active when no data is being processed.

DHCP-IPSec
Provide IP addresses dynamically to VPN clients. This is available for phase 2 configurations associated with a dialup phase 1 configuration.

You also need configure a DHCP server or relay on the private network interface. You must configure the DHCP parameters separately. For more information, see “DHCP servers and relays” on page 89.

If you configure the DHCP server to assign IP addresses based on RADIUS user group attributes, you must also set the Phase 1 Peer Options to Accept peer ID in dialup group and select the appropriate user group. See “Phase 1 configuration” on page 300.

If the unit acts as a dialup server and you manually assigned FortiClient dialup clients VIP addresses that match the network behind the dialup server, selecting the check box will cause the unit to act as a proxy for the dialup clients.
Quick Mode Selector Optionally specify the source and destination IP addresses to be used as selectors for IKE negotiations. If the FortiGate unit is a dialup server, you should keep the default value 0.0.0.0/0 unless you need to circumvent problems caused by ambiguous IP addresses between one or more of the private networks making up the VPN. You can specify a single host IP address, an IP address range, or a network address. You may optionally specify source and destination port numbers and a protocol number.

If you are editing an existing phase 2 configuration, the Source address and Destination address fields are unavailable if the tunnel has been configured to use firewall addresses as selectors. This option exists only in the CLI.

Source address If the unit is a dialup server, type the source IP address that corresponds to the local senders or network behind the local VPN peer (for example, 172.16.5.0/24 or 172.16.5.0/255.255.255.0 for a subnet, or 172.16.5.1/32 or 172.16.5.1/255.255.255.255 for a server or host, or 192.168.10.0/24 or 192.168.10.0/255.255.255.0 for an address range). A value of 0.0.0.0/0 means all IP addresses behind the local VPN peer.

If the unit is a dialup client, source address must refer to the private network behind the FortiGate dialup client.

Source port Type the port number that the local VPN peer uses to transport traffic related to the specified service (protocol number). The range is from 0 to 65535. To specify all ports, type 0.

Destination address Type the destination IP address that corresponds to the recipients or network behind the remote VPN peer (for example, 192.168.20.0/24 for a subnet, or 172.16.5.1/32 for a server or host, or 192.168.10.0/24 or 192.168.10.0/255.255.255.0 for an address range). A value of 0.0.0.0/0 means all IP addresses behind the remote VPN peer.

Destination port Type the port number that the remote VPN peer uses to transport traffic related to the specified service (protocol number). The range is from 0 to 65535. To specify all ports, type 0.

Protocol Type the IP protocol number of the service. The range is from 0 to 255. To specify all services, type 0.

Note: You can configure settings so that VPN users can browse the Internet through the unit. For more information, see “Internet browsing” on page 308.

Manual Key

Caution: You should use manual keys only if it is unavoidable. There are potential difficulties in keeping keys confidential and in propagating changed keys to remote VPN peers securely.

If required, you can manually define cryptographic keys for establishing an IPsec VPN tunnel. You would define manual keys in situations where:

- You require prior knowledge of the encryption or authentication key (that is, one of the VPN peers requires a specific IPsec encryption or authentication key).
- You need to disable encryption and authentication.

In both cases, you do not specify IPsec phase 1 and phase 2 parameters; you define manual keys by going to VPN > IPsec > Manual Key instead.
New manual key configuration

**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.

If one of the VPN devices is manually keyed, the other VPN device must also be manually keyed with the identical authentication and encryption keys. In addition, it is essential that both VPN devices be configured with complementary Security Parameter Index (SPI) settings. The administrators of the devices need to cooperate to achieve this. 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. You must manually specify an SPI for each SA. There is an SA for each direction, so for each VPN you must specify two SPIS, a local SPI and a remote SPI, to cover bidirectional communications between two VPN devices.

**New Manual Key page**

Provides settings for configuring a cryptographic key for the IPSec VPN.

- **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 unit. The valid range is from 0x100 to 0xffffffff. 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 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 unit obtains the IP address of the interface from the network interface settings. For more information, see “Interface configuration and settings” on page 58.

### Encryption Algorithm
Select one of the following symmetric-key encryption 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 Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.
- **AES192** — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.
- **AES256** — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.

**Note:** The algorithms for encryption and authentication cannot both be NULL.

### Encryption Key
Enter an encryption key appropriate to the encryption algorithm:
- for **NULL**, nothing is required.
- for **DES**, type a 16-character hexadecimal number (0-9, a-f).
- for **3DES**, type a 48-character hexadecimal number (0-9, a-f) separated into three segments of 16 characters.
- for **AES128**, type a 32-character hexadecimal number (0-9, a-f) separated into two segments of 16 characters.
- for **AES192**, type a 48-character hexadecimal number (0-9, a-f) separated into three segments of 16 characters.
- for **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:
- **NULL** — Do not use a message digest.
- **MD5** — Message Digest 5 algorithm, which produces a 128-bit message digest.
- **SHA1** — Secure Hash Algorithm 1, which produces a 160-bit message digest.
- **SHA256** — Secure Hash Algorithm 2, which produces a 256-bit message digest.

**Note:** The Algorithms for encryption and authentication cannot both be NULL.

### Authentication Key
Enter an authentication key appropriate to the authentication algorithm:
- for **MD5**, type a 32-character hexadecimal number separated into two segments of 16 characters.
- for **SHA1**, type a 40-character hexadecimal number separated into two segments of 16 characters and a third segment of 8 characters.
- for **SHA256**, type a 64-character hexadecimal number separated into four segments of 16 characters.

**Note:** Digits can be 0 to 9, and a to f.

### IPsec Interface Mode
Create a virtual interface for the local end of the VPN tunnel. Select this check box to create a route-based VPN, clear it to create a policy-based VPN. This is available only in NAT/Route mode.

### Internet browsing
By using appropriate firewall policies, you can enable VPN users to browse the Internet through the unit. The required policies are different for policy-based and route-based VPNs. For more information, see “Policy” on page 203.
Concentrator

In a hub-and-spoke configuration, policy-based VPN connections to a number of remote peers radiate from a single, central unit. Site-to-site connections between the remote peers do not exist; however, you can establish VPN tunnels between any two of the remote peers through the unit’s “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. You create the concentrator in VPN > IPSec > Concentrator. A concentrator configuration specifies which spokes to include in an IPsec hub-and-spoke configuration.

Monitoring VPNs

You can use the IPsec 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.

For dialup VPNs, the list provides status information about the VPN tunnels established by dialup clients, including their IP addresses. The number of tunnels shown in the list can change as dialup clients connect and disconnect.

For static IP or 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.

You can use filters to control the information displayed in the list. For more information, see “Adding filters to web-based manager lists” on page 24.
SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. SSL VPN does not require the installation of specialized client software on end users’ computers, and is ideal for applications including web-based email, business and government directories, file sharing, remote backup, remote system management, and consumer-level electronic commerce.

The two modes of SSL VPN operation (supported in NAT/Route mode only) are:

- web-only mode, for thin remote clients equipped with a web-browser only.
- tunnel mode, for remote computers that run a variety of client and server applications.
When the unit provides services in web-only mode, a secure connection between the remote client and the unit is established through the SSL VPN security in the unit and the SSL security in the web browser. After the connection has been established, the unit provides access to selected services and network resources through a web portal. The FortiGate SSL VPN web portal has a widget-based layout with customizable themes. Each widget is displayed in a 1- or 2-column format with the ability to modify settings, minimize the widget window, or other functions depending on the type of content within the widget.

When users have complete administrative rights over their computers and use a variety of applications, tunnel mode allows remote clients to access the local internal network as if they were connected to the network directly.

This topic contains the following:

- General configuration steps
- Config
- Portal
- Virtual Desktop Application Control
- Host Check
- SSL VPN monitor list

Note: The FortiMobile SSL VPN app for either the iPhone or iPod touch allows you to connect directly to your FortiGate unit’s SSL VPN. The app supports web mode access only. With this app, you can add, edit, or delete user-defined bookmarks. For more information about the FortiMobile SSL VPN app, see the What’s New chapter of the FortiOS Handbook as well as the iTunes app store.

**General configuration steps**

For best results in configuring FortiGate SSL VPN technology, use the following general configuration steps. These general configuration steps should be followed in the order given, because if you perform any additional actions between procedures, your configuration may have different results.

1. Enable SSL VPN connections and set the basic options needed to support SSL VPN configurations.
2. Create a web portal to define user access to network resources. If you want to provide different types of access to different groups of users, you need to create multiple web portals.
3. Create user accounts for the remote clients. Create SSL VPN users groups and associate them with the web portal or portals that you created. Assign users to the appropriate SSL VPN user groups.
4. Configure the firewall policies and the remaining parameters needed to support the VPN mode of operation.
5. For tunnel-mode operation, add routing to ensure that client tunnel-mode packets reach the SSL VPN interface.
6. Optionally, define SSL VPN event-logging parameters, and monitor active SSL VPN sessions.
ssl.root

The unit has a virtual SSL VPN interface called ssl.<vdomname>. The root VDOM, called ssl.root, appears in the firewall policy interface lists and static route interface lists. You can use the ssl-root interface to allow access to additional networks and facilitate a connected user’s ability to browse the Internet through the unit.

SSL VPN tunnel-mode access requires the following firewall policies:

- **External > Internal**, with the action set to SSL, with an SSL user group
- **ssl.root > Internal**, with the action set to Accept
- **Internal > ssl.root**, with the action set to Accept.

Access also requires a new static route: Destination network - <ssl tunnel mode assigned range> interface ssl.root.

If you are configuring Internet access through an SSL VPN tunnel, you must add the following configuration: ssl.root > External, with the action set to Accept, NAT enabled.

**Config**

You can configure 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. SSL VPN configuration is located in **VPN > SSL > Config**.

**Note:** If required, you can enable SSL version 2 encryption (for compatibility with older browsers) through a CLI command.

### SSL-VPN Settings page

Provides settings for configuring an SSL-VPN. This page also provides advanced configuration settings for DNS and WINS servers.

**Enable SSL VPN**
Select to enable SSL VPN connections.

**IP Pools**
Select **Edit** to select the range or subnet firewall addresses that represent IP address ranges reserved for tunnel-mode SSL VPN clients. If the appropriate addresses do not exist, go to **Firewall > Address** to create them. You cannot add the **all** firewall address or a FQDN firewall address. You also cannot add an address group that includes the **all** firewall address or a FQDN address.

**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 check box. 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 can match a cipher suite greater than or equal to 128 bits, select this option.

- **High - AES(128/256 bits) and 3DES**
  If the web browser on the remote client can match 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 cipher suite greater than or equal to 64 bits.
The SSL VPN Service portal allows you to access network resources through a secure channel using a web browser. FortiGate administrators can configure log in privileges for system users and which network resources are available to the users, such as HTTP/HTTPS, telnet, FTP, SMB/CIFS, VNC, RDP and SSH.

The portal configuration determines what the system user sees when they log in to the unit. Both the system administrator and the system user have the ability to customize the SSL VPN portal.

There are three pre-defined default web portal configurations available:

- **full-access**: Includes all widgets available to the user - Session Information, Connection Tool, Bookmarks, and Tunnel Mode.
- **tunnel-access**: Includes Session Information and Tunnel Mode widgets.
- **web-access**: Includes Session Information and Bookmarks widgets.

You can also choose to create your own web portal from VPN > SSL > Portal.

This topic includes the following:

- Portal settings
- Portal widgets

### Portal settings

**Idle Timeout**  
Type the period of time (in seconds) to control how long the connection can remain idle before the system forces the user to log in again. The range is from 10 to 28800 seconds. You can also set the value to 0 to have no idle connection timeout. This setting applies to the SSL VPN session. The interface does not time out when web application sessions or tunnels are up.

**Advanced (DNS and WINS Servers)**

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Server #1</td>
<td>Enter up to two DNS Servers to be provided for the use of clients.</td>
</tr>
<tr>
<td>DNS Server #2</td>
<td></td>
</tr>
<tr>
<td>WINS Server #1</td>
<td>Enter up to two WINS Servers to be provided for the use of clients.</td>
</tr>
<tr>
<td>WINS Server #2</td>
<td></td>
</tr>
</tbody>
</table>

### Portal widgets

- **Portal page**

Lists all the web portals that you have created, as well as the default web portals. On this page, you can edit, delete or create a new web portal. If you want, you can also edit a default web portal.

- **Create New**  
  Creates a new web portal. When you select Create New, you are automatically redirected to the Portal Settings page.

- **Edit**  
  Modifies settings within the concentrator. When you select Edit, you are automatically redirected to the same page where you created the portal.

- **Delete**  
  Removes a portal configuration from the Portal page.
  To remove multiple portals from the list, on the Portal page, in each of the rows of the portals you want removed, select the check box and then select Delete.
  To remove all portals in the list, on the Portals page, select the check box in the check box column, and then select Delete.

- **Name**  
  The name of the web portal.

- **Portal Settings page**

Provides settings for configuring the SSL VPN Service page.

- **Settings window**  
  Provides general, virtual desktop and security control settings for the SSL VPN Service portal page. This window appears when you select Settings. This window also appears whenever you select Create New and are automatically redirected to the Portal Settings page. For more information, see “Portal settings” on page 314.
Portal settings

A web portal defines SSL VPN user access to network resources, such as HTTP/HTTPS, telnet and SSH. The portal configuration determines what SSL VPN users see when they log in to the unit. Both the FortiGate administrator and the SSL VPN user have the ability to customize the web portal settings. Portal settings are configured in VPN > SSL > Portal.

The Settings Window provides settings for configuring general, virtual desktop and security console options for your web portal.

The virtual desktop options, available for Windows XP and Windows Vista client PCs, are configured to completely isolate the SSL VPN session from the client computer’s desktop environment. All data is encrypted, including cached user credentials, browser history, cookies, temporary files, and user files created during the session. When the SSL VPN session ends normally, the files are deleted. If the session ends due to a malfunction, files might remain, but they are encrypted, so the information is protected.

When the user starts an SSL VPN session with virtual desktop enabled, the virtual desktop replaces the user’s normal desktop. When the virtual desktop exits, the user’s normal desktop is restored.

Virtual desktop requires the Fortinet host check plugin. If the plugin is not present, it is automatically downloaded to the client computer.

Security control options provide cache cleaning and host checking to the clients of your web portal. Cache cleaning clears information from the client browser cache just before the SSL VPN session ends. The cache cleaner is effective only if the session terminates normally. The cache is not cleaned if the session ends due to a malfunction, such as a power failure.
Host checking enforces the client’s use of antivirus or firewall software. Each client is checked for security software that is recognized by the Windows Security Center. As an alternative, you can create a custom host check that looks for specific security software selected from the Host Check list located at VPN > SSL > Host Check. See “Host Check” on page 318.

**Settings Window**

Provides settings for configuring general, virtual desktop and security console options. When you select OK, these settings appear on the Portal Settings page. For example, if you selected the general color scheme orange, the widgets and page take on that color scheme after OK is selected.

**General tab**

The general overall settings for the page, such as color scheme.

- **Name**
  - Enter a name for the web portal configuration.

- **Applications**
  - Select the abbreviated name of the server applications or network services clients can use.

- **Portal Message**
  - Enter the caption that appears at the top of the web portal home page.

- **Theme**
  - Select the color scheme for the web portal home page from the list.

- **Page Layout**
  - Select the one or two page column format for the web portal home page.

- **Redirect URL**
  - The web portal can display a second HTML page in a popup window when the web portal home page is displayed. Enter the URL.

**Virtual Desktop tab**

The virtual desktop settings that allow users certain options, such as allow to switch between the virtual desktop and the regular desktop.

- **Enable Virtual Desktop**
  - Select to enable the virtual desktop feature.

- **Allow switching between virtual desktop and regular desktop**
  - Select to allow users to switch between the virtual desktop, and their regular desktop.

- **Allow clipboard contents to be shared with regular desktop**
  - Select to allow users access to the clipboard contents when they are using the regular desktop.

- **Allow use of removable media**
  - Select to allow users to use removable media.

- **Allow network share access**
  - Select to allow users to have network share access.

- **Allow printing**
  - Select to allow users to print from the virtual desktop.

- **Quit the virtual desktop and logout session when browser is closed**
  - Select to have the virtual desktop close and log the user out of the current session whenever the browser is closed.

- **Application Control List**
  - Select a virtual desktop application list from the drop-down list.

**Security Control tab**

The security controls for the portal.

- **Clean Cache**
  - Select to have the unit remove residual information from the remote client computer just before the SSL VPN session is done.

- **Host Check**
  - Select to enable host checking.

- **Interval**
  - Enter how often to recheck the host.

- **Policy**
  - Select the specific host check software to look for. This is available only when Custom is selected in Host Check.
Portal widgets

Portal widgets are widgets that you can specify certain things when users are viewing the portal. These specifications can be certain web URL bookmarks, or connecting to network resources. If a portal has tunnel access, the Tunnel Mode widget allows you to configure how many tunnel mode clients are assigned IP addresses, as well as enabling split tunneling configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Modifies the information within the widget. These options appear within the widget after selecting Edit.</td>
</tr>
<tr>
<td>OK</td>
<td>Select to save the Session Information configuration.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Select to exit the Session Information widget without saving any changes.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a customized name for the Session Information widget.</td>
</tr>
<tr>
<td>Remove widget</td>
<td>Select to close the widget and remove it from the web portal home page.</td>
</tr>
</tbody>
</table>

Session Information

The Session Information widget displays the login name of the user, along with the amount of time the user has been logged in and the inbound and outbound traffic statistics of HTTP and HTTPS.

Bookmarks

Bookmarks are used as links to specific resources on the network. When a bookmark is selected from a bookmark list, a pop-up window appears with the requested web page. Telnet, VNC, and RDP all pop up a window that requires a browser plug-in. FTP and Samba replace the bookmarks page with an HTML file-browser.

A web bookmark can include login credentials to automatically log the SSL VPN user into the web site. This means that once the user logs into the SSL VPN, he or she does not have to enter any more credentials to visit preconfigured web sites. When the administrator configures bookmarks, the web site credentials must be the same as the user’s SSL VPN credentials. Users configuring their own bookmarks can specify alternative credentials for the web site.

Connection Tool

You can use the Connection Tool widget to connect to a network resource without adding a bookmark to the bookmark list. You select the type of resource and specify the URL or IP address of the host computer.

Tunnel Mode

If your web portal provides tunnel mode access, you need to configure the Tunnel Mode widget. These settings determine how tunnel mode clients are assigned IP addresses. Also, you can enable a split tunneling configuration so that the VPN carries only the traffic for the networks behind the unit. The user’s other traffic follows its normal route.

Virtual Desktop Application Control

You can control which applications users can run on their virtual desktop. To do this, you create a list of either allowed or blocked applications which you then select when you configure the virtual desktop. Configuration is located in VPN > SSL > Virtual Desktop Application Control.
**Virtual Desktop Application Control page**

Lists each individual virtual desktop application list that you created. On this page you can edit, delete or create a new virtual desktop application list.

- **Create New**: Creates a new virtual desktop application control list. When you select Create New, you are automatically redirected to the Virtual Desktop Application Control page.

- **Name**: The names of the virtual desktop application control lists.

- **Action**: The action configured for each virtual desktop application control list: Block the applications on this list and allow all others or Allow the applications on this list and block all others.

- **Edit**: Modifies the settings within the virtual desktop application control list. When you select Edit, you are automatically redirected to the Virtual Desktop Application Control List page.

- **Delete**: Removes a virtual desktop application list from the Virtual Desktop Application Control page.
  - To remove single list, select the check box and then select Delete.
  - To remove all lists, select the check box in the check box column, and then select Delete.

- **Clone**: Makes a copy of an application control list to create a new application control list using the same settings as another list. When you select Clone, you are automatically redirected to the Virtual Desktop Application Control List page.

---

**Virtual Desktop Application Control List page**

Provides settings for configuring a virtual desktop application list which contains multiple applications. This list can either block applications or allow applications.

- **Name**: Enter a name for the virtual desktop application list.

- **Allow the applications on the list and block all others**: Select to allow the applications on this list and block all others.

- **Block the application on the list and allow all others**: Select to block the applications on the list and allow all others.

- **Create New**: Creates a new application signature. When you select Create New, the Application Signatures window appears.

- **Edit**: Modifies the settings within the application signature. When you select Edit, you are automatically redirected to the Application Signatures window.

- **Delete**: Removes an application signature from the list on the Virtual Desktop Application Control List page.
  - To remove single signature, select the check box and then select Delete.
  - To remove all signatures, select the check box in the check box column, and then select Delete.

- **Applications**: The name of the application.

- **Application Signatures**
Host Check

When you enable AV, FW, or AV-FW host checking in the web portal Security Control settings, each client is checked for security software that is recognized by the Windows Security Center. As an alternative, you can create a custom host check that looks for security software selected from the Host Check list. For more information, see “Portal settings” on page 314.

The Host Check list includes default entries for many security software products. Use the following table when configuring host check.

**Name**

Enter the name of the application. This name does not have to match the official name of the application.

**MD5 Signatures (one per line)**

Enter the MD5 signature for application executable file. You can enter more than one but each one needs to be on a separate line. You can use a third-party utility to calculate MD5 signatures or hashes for the file.

Entering multiple MD5 signatures helps to match multiple versions of the application.

---

**Host Check**

When you enable AV, FW, or AV-FW host checking in the web portal Security Control settings, each client is checked for security software that is recognized by the Windows Security Center. As an alternative, you can create a custom host check that looks for security software selected from the Host Check list. For more information, see “Portal settings” on page 314.

The Host Check list includes default entries for many security software products. Use the following table when configuring host check.

**Name**

Enter the name of the application. This name does not have to match the official name of the application.

**MD5 Signatures (one per line)**

Enter the MD5 signature for application executable file. You can enter more than one but each one needs to be on a separate line. You can use a third-party utility to calculate MD5 signatures or hashes for the file.

Entering multiple MD5 signatures helps to match multiple versions of the application.

---

**Host Check page**

Lists each individual host check list that you created for host checking for a web portal. On this page, you can edit, delete or create a new host check list.

**Create New**

Creates a new application to the host check list. When you select Create New, you are automatically redirected to the Host Check Software page.

**Name**

The name of the applications added to the host check list. The name does not need to match the actual application name.

**Type**

The type of host check application. Can be AV for antivirus or FW for firewall.

**Version**

The version of the host check application.

**Edit**

Modifies the settings within the host check list. When you select Edit, you are automatically redirected to the Host Check Software page.

**Delete**

Removes a host check list from the list on the Host Check page.

To remove multiple lists from the list, on the Host Check page, in each of the rows of the lists you want removed, select the check box and then select Delete.

To remove all lists in the list, on the Host Check page, select the check box in the check box column, and then select Delete.

**Host Check Software page**

Provides settings for configuring a host check list which contains applications and how those applications will be checked.

**Name**

Enter a name for the host check list.

**Type**

Select the type of host checking, either AV or FW.

**GUID**

Enter the globally unique identifier (GUID) for the host check application. The GUID is usually in the form xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx, where each x is a hexadecimal digit. Windows uses GUIDs to identify applications in the Windows Registry.

**Version**

Enter the software’s version.

**Create New**

Creates a new check item to add to the list below. When you select Create New, the Check Item window appears.

**Edit**

Modifies the settings within the software. When you select Edit, the Check Item window appears.

**Delete**

Removes the check software item from the list on the Host Check Software page.

To remove multiple check software items from the list, on the Host Check Software page, in each of the rows of the lists you want removed, select the check box and then select Delete.

To remove all check software items in the list, on the Host Check Software page, select the check box in the check box column, and then select Delete.
SSL VPN monitor list

You can view 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 the connection was made. You can also see which services are being provided, and delete an active web or tunnel session from the unit. For more information, see “SSL VPN” on page 310.

Monitor page

Lists all the current monitored SSL VPN sessions. On this page, you can also remove an SSL VPN session that is currently being monitored.

<table>
<thead>
<tr>
<th>No.</th>
<th>The connection identifiers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user names of all connected remote users.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The IP addresses of the host devices connected to the FortiGate unit.</td>
</tr>
<tr>
<td>Begin Time</td>
<td>The starting time of each connection.</td>
</tr>
<tr>
<td>Description</td>
<td>For an SSL VPN tunnel subsession, the client’s assigned tunnel IP address is shown.</td>
</tr>
<tr>
<td>Action</td>
<td>Select action to apply to current SSL VPN tunnel session or subsession.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the current session or subsession.</td>
</tr>
</tbody>
</table>

To remove multiple sessions from within the list, on the Monitor page, in each of the rows of the sessions you want removed, select the check box and then select Delete.

To remove all sessions from the list, on the Monitor page, select the check box in the check box column and then select Delete.
User

This section provides an introduction to the User menu. If you require more information about the features in the User menu, see the FortiOS Handbook.

The following topics are included in this section:

- User
- User Group
- Remote
- Directory Service
- PKI
- Monitor

User

The User menu allows you to configure authentication settings and user accounts. The User menu also allows you to configure user groups, remote servers, as well as monitor users.

A user is a user account that consists of a user name, password and in some cases, other information that can be configured on the FortiGate unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group. For more information about user groups, see “User Group” on page 324.

This topic contains the following:

- Local user accounts
- IM users
- Authentication settings

Local user accounts

A local user is a user configured on a FortiGate unit. The user can be authenticated with a password stored on the unit (the user name and password must match a user account stored on the unit) or with a password stored on an authentication server. The user name must match a user account stored on the unit and the user name and password must match a user account stored on the authentication server associated with the user.

Local users are configured in User > User > User. Use the following table when configuring local user accounts.

<table>
<thead>
<tr>
<th>User page</th>
<th>Lists each individual local user’s list that you created. On this page, you can edit, delete or create a new local users list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new local user account. When you select Create New, you are automatically redirected to New User page.</td>
</tr>
<tr>
<td>User Name</td>
<td>The local user name.</td>
</tr>
</tbody>
</table>
IM users

Instant Messenger (IM) 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. FortiGate units allow you to set up IM users that either allow or block the use of applications, to determine which applications are allowed.

IM users are configured in the CLI first, and then appear in User > User > IM. IM users must be configured using the config imp2p command in the CLI. Use the following table when configuring IM users.

<table>
<thead>
<tr>
<th>Type</th>
<th>The authentication type to use for this user. The authentication types are Local (user and password stored on FortiGate unit), LDAP, RADIUS, and TACACS+ (user and password matches a user account stored on the authentication server).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Removes a user from the list. Removing the user name removes the authentication configured for the user. The delete icon is not available if the user belongs to a user group. To remove multiple local user accounts from within the list, on the User page, in each of the rows of user accounts you want removed, select the check box and then select Delete. To remove all local user accounts from the list, on the User page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies a user’s account settings. When you select Edit, you are automatically redirected to the Edit User page.</td>
</tr>
</tbody>
</table>

New User page

Provides settings for configuring whether to allow or block a local user from authenticating.

<table>
<thead>
<tr>
<th>User Name</th>
<th>A name that identifies the user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable</td>
<td>Select to prevent this user from authenticating.</td>
</tr>
<tr>
<td>Password</td>
<td>Select to authenticate this user using a password stored on the FortiGate unit and then enter the password. The password should be at least six characters.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Select to authenticate this user using a password stored on an LDAP server. Select the LDAP server from the list. You can select only an LDAP server that has been added to the FortiGate LDAP configuration. For more information, see “LDAP” on page 329.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Select to authenticate this user using a password stored on a RADIUS server. Select the RADIUS server from the list. You can select only a RADIUS server that has been added to the FortiGate RADIUS configuration. For more information, see “RADIUS” on page 327.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Select to authenticate this user using a password stored on a TACACS server. Select the TACACS+ server from the list. You can select only a TACACS server that has been added to the FortiGate TACACS configuration. For more information, see “TACACS+” on page 331.</td>
</tr>
</tbody>
</table>

IM page

Lists each individual IM user. On this page, you can edit, delete or create a new IM user. You can also filter the information by protocol or policy.

<table>
<thead>
<tr>
<th>Create New</th>
<th>Creates an IM user. When you select Create New, you are automatically redirected to the Edit User page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Modifies an IM user’s settings. When you select Edit, you are automatically redirected to the Edit User page.</td>
</tr>
</tbody>
</table>
Authentication settings

The Authentication submenu provides settings for configuring authentication timeout, protocol support, and authentication certificates.

When user authentication is enabled within a firewall policy, the authentication challenge is normally issued for any of the four protocols (depending 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. Users 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.

When you enable user authentication within a firewall policy, the firewall policy user will be challenged to authenticate. For user ID and password authentication, users must provide their user names and passwords. For certificate authentication (HTTPS or HTTP redirected to HTTPS only), you can install customized certificates on the FortiGate unit and the users can also have customized certificates installed on their browsers. Otherwise, users will see a warning message and have to accept a default FortiGate certificate.

Authentication settings are configured in User > User > Authentication. Use the following table when configuring authentication settings.
User Group

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, LDAP, or TACACS+ server
- a RADIUS, LDAP, or TACACS+ server (all identities on the server can authenticate)
- a user or user group defined on a Directory Service server.

Each user group belongs to one of three types: Firewall, Directory Service or SSL VPN.

In most cases, the unit authenticates users by requesting each user name and password. The FortiGate unit checks local user accounts first. If the unit does not find a match, it checks the RADIUS, LDAP, or TACACS+ servers that belong to the user group. Authentication succeeds when the unit finds a matching user name and password.

For a Directory Service user group, the Directory Service server authenticates users when they log in to the network. The unit receives the user’s name and IP address from the FSAE collector agent. For more information about FSAE, see the Fortinet Server Authentication Extension Administration Guide.

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 groups are configured in User > User Group > User Group. Use the following table when configuring user groups.

**User Group page**

Lists each individual user group list according to their type of group. On this page, you can edit, delete or create a new user group list.

<table>
<thead>
<tr>
<th>Create New</th>
<th>Creates a new user group. When you select Create New, you are automatically redirected to New User Group page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The name of the user group. User group names are listed by type of user group: Firewall, Directory Service and SSL VPN. For more information, see &quot;Directory Service user groups&quot; on page 326, and &quot;SSL VPN user groups&quot; on page 326.</td>
</tr>
<tr>
<td>Members</td>
<td>The Local users, RADIUS servers, LDAP servers, TACACS+ servers, Directory Service users/user groups or PKI users found in the user group.</td>
</tr>
</tbody>
</table>

**Authentication Settings**

Provides settings for defining how users authenticate a session. For example, the authentication timeout is configured for 10 minutes so a user’s session, if idle for 10 minutes, will log them out of the session automatically.

**Authentication Timeout**

Enter a length of time in minutes, from 1 to 480. Authentication Timeout controls how long an authenticated firewall connection can be idle before the user must authenticate again. The default value is 30.

**Protocol Support**

Select the protocols to challenge during firewall user authentication.

**Certificate**

If using HTTPS protocol support, select the Local certificate to use for authentication. Available only if HTTPS protocol support is selected.

**Apply**

Applies the selections for user authentication settings.

*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.
## Firewall user groups

A firewall user group provides access to a firewall policy that requires 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.

You can also authenticate a user by certificate if you have selected this method.
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 unit.

**Note:** A user group cannot be a dialup group if any member is authenticated using a RADIUS or LDAP server.

You can also use a firewall user group to provide override privileges for FortiGuard web filtering.

### Directory Service user groups

On a network, you can configure the unit to allow access to members of Directory Service server user groups who have been authenticated on the network. The Fortinet Server Authentication Extensions (FSAE) must be installed on the network domain controllers.

A Directory Service user group provides access to a firewall policy that requires Directory Service type authentication and lists the user group as one of the allowed groups. The members of the user group are Directory Service users or groups that you select from a list that the unit receives from the Directory Service servers that you have configured. For more information, see “Directory Service” on page 331.

**Note:** A Directory Service user group cannot have SSL VPN access.

You cannot use Directory Service user groups directly in FortiGate firewall policies. You must add Directory Service groups to FortiGate user groups. A Directory Service group should belong to only one FortiGate user group. If you assign it to multiple FortiGate user groups, the unit recognizes only the last user group assignment.

You can also use a Directory Service user group to provide override privileges for FortiGuard web filtering.

### SSL VPN user groups

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.

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. You configure the user’s VPN client 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 unit.

**Note:** A user group cannot be an IPSec dialup group if any member is authenticated using a RADIUS or LDAP server.
For information on configuring user groups, see "User Group" on page 324. For information on configuring SSL VPN user group options, see "SSL VPN identity-based firewall policies" on page 210.

**Note:** By default, the web-based manager displays Firewall options. The following figures show the variations that display for each of the user group types: Firewall, Directory Service, and SSL VPN.

You cannot add local users to a group that is used to authenticate administrators.

**Dynamically assigning VPN client IP addresses from a user group**

SSL VPN tunnel mode, dialup IPSec VPN, and PPTP VPN sessions can assign IP addresses to remote users by getting the IP address to assign to the user from the Framed-IP-Address field in the RADIUS record received when the RADIUS server confirms that the user has authenticated successfully. For more information about RADIUS fields, see RFC 2865 and RFC 2866.

For the unit to dynamically assign an IP address, the VPN users must be configured for RADIUS authentication and you must include the IP address to assign to the user in the Framed-IP-Address RADIUS field on your RADIUS server. You configure each type of VPN differently. In each case you are associating the configuration that assigns IP addresses to users with a user group.

Assigning IP addresses from a RADIUS record replaces dynamically assigning IP addresses from an address range. You cannot include an IP address range and assigning IP addresses from a RADIUS record in the same configuration.

**Remote**

Remote authentication is generally used to ensure that employees working offsite can remotely access their corporate network with appropriate security measures in place. In general terms, authentication is the process of attempting to verify the (digital) identity of the sender of a communication such as a login request. The sender may be someone using a computer, the computer itself, or a computer program. Since a computer system should be used only by those who are authorized to do so, there must be a measure in place to detect and exclude any unauthorized access.

On a unit, you can control access to network resources by defining lists of authorized users, called user groups. To use a particular resource, such as a network or VPN tunnel, the user must:

- belong to one of the user groups that is allowed access
- correctly enter a user name and password to prove his or her identity, if asked to do so.

**RADIUS**

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. FortiGate units use the authentication function of the RADIUS server. You must configure the server before you configure the FortiGate users or user groups that will need it to use the RADIUS server for authentication.

If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the 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 unit. If the RADIUS server cannot authenticate the user, the unit refuses the connection. You can override the default authentication scheme by selecting a specific authentication protocol or changing the default port for RADIUS traffic.
If you want to configure settings for UTF-8 encoding, you must enable this in the CLI using the `config vpn ssl setting` command. The following is the command syntax used to enable UTF-8 encoding.

RADIUS servers are configured in User > Remote > RADIUS. Use the following table when configuring RADIUS servers.

### RADIUS page
Lists each individual RADIUS server that you created. On this page, you can edit, delete or create a new RADIUS server.

- **Create New**: Creates a new RADIUS server. The maximum number is 10. When you select Create New, you are automatically redirected to the New RADIUS Server page.
- **Name**: Name that identifies the RADIUS server on the unit.
- **Server Name/IP**: Domain name or IP address of the RADIUS server.
- **Delete**: Removes a RADIUS server from the list on the RADIUS page. You cannot delete a RADIUS server that has been added to a user group. To remove multiple RADIUS servers from within the list, on the RADIUS page, in each of the rows of servers you want removed, select the check box and then select Delete. To remove all RADIUS servers from the list, on the RADIUS page, select the check box in the check box column and then select Delete.
- **Edit**: Modifies settings within a RADIUS server configuration. When you select Edit, you are automatically redirected to the Edit RADIUS Server page.

### New RADIUS Server page
Provides settings for configuring a RADIUS server.

- **Name**: Enter the name that is used to identify the RADIUS server on the unit.
- **Primary Server Name/IP**: Enter the domain name or IP address of the primary RADIUS server.
- **Primary Server Secret**: Enter the RADIUS server secret key for the primary RADIUS server. The primary server secret key should be a maximum of 16 characters in length. Note: The server secret key should be a maximum of 16 characters in length.
- **Secondary Server Name/IP**: Enter the domain name or IP address of the secondary RADIUS server, if you have one.
- **Secondary Server Secret**: Enter the RADIUS server secret key for the secondary RADIUS server. The secondary server secret key should be a maximum of 16 characters in length.
- **Authentication Scheme**: Select Use Default Authentication Scheme to authenticate with the default method. The default authentication scheme uses PAP, MS-CHAP-V2, and CHAP, in that order. Select Specify Authentication Protocol to override the default authentication method, and choose the protocol from the list: MS-CHAP-V2, MS-CHAP, CHAP, or PAP, depending on what your RADIUS server needs.
- **NAS IP/Called Station ID**: Enter the NAS IP address and Called Station ID (for more information about RADIUS Attribute 31, see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address that the FortiGate interface uses to communicate with the RADIUS server will be applied.
- **Include in every User Group**: Select to have the RADIUS server automatically included in all user groups.
LDAP

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. An LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

If you have configured LDAP support and require a user to authenticate using an LDAP server, the unit contacts the LDAP server for authentication. To authenticate with the unit, the user enters a user name and password. The unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the unit successfully authenticates the user. If the LDAP server cannot authenticate the user, the unit refuses the connection.

FortiGate LDAP supports password renewal, and these settings are configured in the CLI. There are settings for a warning that the password is going to expire, and threshold of the expiry as well. The following commands are used to configure password renewal for LDAP:

```bash
config user ldap
edit <name>
  set password-expiry-warning {enable | disable}
  set password-renewal {enable | disable}
end
```

LDAP servers are configured in User > Remote > LDAP. Use the following table when configuring LDAP servers.

<table>
<thead>
<tr>
<th>LDAP page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists each individual LDAP server that you created. On this page, you can edit, delete or create a new LDAP server.</td>
</tr>
</tbody>
</table>

| Create New | Creates a new LDAP server. The maximum number is 10. When you select Create New, you are automatically redirected to the New LDAP Server page. |
| Name | The name that identifies the LDAP server on the unit. |
| Server Name/IP | The domain name or IP address of the LDAP server. |
| Port | The TCP port used to communicate with the LDAP server. |
| Common Name Identifier | The common name identifier for the LDAP server. Most LDAP servers use 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 servers use. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. |
| Delete | Removes the LDAP server configuration from the list on the LDAP page. To remove multiple LDAP servers from within the list, on the LDAP page, in each of the rows of servers you want removed, select the check box and then select Delete. To remove all LDAP servers from the list, on the LDAP page, select the check box in the check box column and then select Delete. |
| Edit | Modifies settings from within an LDAP server configuration. When you select Edit, you are automatically redirected to the Edit LDAP Server page. |

| New LDAP Server page | Provides settings for configuring an LDAP server. |
| Name | Enter the name that identifies the LDAP server on the FortiGate unit. |
| Server Name/IP | Enter the domain name or IP address of the LDAP server. |
### Server Port
Enter the TCP port used to communicate with the LDAP server. By default, LDAP uses port 389. If you use a secure LDAP server, the default port changes when you select Secure Connection.

### Common Name Identifier
Enter the common name identifier for the LDAP server. The maximum number of characters is 20.

### Distinguished Name
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. The maximum number of characters is 512.

### Query icon
View the LDAP server Distinguished Name Query tree for the LDAP server that you are configuring so that you can cross-reference to the Distinguished Name. The Query icon is located beside the Distinguished Name field. For more information, see “Using Query” on page 330.

### Bind Type
Select the type of binding for LDAP authentication.

- **Regular**: Connect to the LDAP server directly with user name/password, then receive accept or reject based on search of given values.
- **Anonymous**: Connect as an anonymous user on the LDAP server, then retrieve the user name/password and compare them to given values.
- **Simple**: Connect directly to the LDAP server with user name/password authentication.

### Filter
Enter the filter to use for group searching. Available if Bind Type is Regular or Anonymous.

### User DN
Enter the Distinguished name of the user to be authenticated. Available if Bind Type is Regular.

### Password
Enter the password of the user to be authenticated. Available if Bind Type is Regular.

### Secure Connection
Select to use a secure LDAP server connection for authentication.

### Protocol
Select a secure LDAP protocol to use for authentication. Depending on your selection, the value in Server Port will change to the default port for the selected protocol. Available only if Secure Connection is selected.

- **LDAPS**: port 636
- **STARTTLS**: port 389

### Certificate
Select a certificate to use for authentication from the list. The certificate list comes from CA certificates at System > Certificates > CA Certificates.

---

### Using Query
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. To see the distinguished name associated with the Common Name identifier, select the Expand Arrow beside the CN identifier and then select the DN from the list. The DN you select is displayed in the Distinguished Name field. Select OK to save your selection in the Distinguished Name field of the LDAP Server configuration.

To see the users with the LDAP Server user group for the selected Distinguished Name, select the expand arrow beside the Distinguished Name in the LDAP Distinguished Name Query tree.
TACACS+

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ allows a client to accept a user name and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user. The default TCP port for a TACACS+ server is 49.

TACACS+ servers are configured in User > Remote > TACACS+. Use the following table when configuring TACACS+ servers.

TACACS+ page
Lists each individual TACACS+ server that you created. On this page, you can edit, delete or create a new TACACS+ server.

- **Create New**
  Creates a new TACACS+ server. The maximum number is 10. When you select Create New, you are automatically redirected to the New TACACS+ Server page.

- **Server**
  The server domain name or IP address of the TACACS+ server.

- **Authentication Type**
  The supported authentication method. TACACS+ authentication methods include: Auto, ASCII, PAP, CHAP, and MSCHAP.

- **Delete**
  Removes a TACACS+ server from the list on the TACACS+ page. To remove multiple TACACS+ servers from within the list, on the TACACS+ page, in each of the rows of servers you want removed, select the check box and then select Delete. To remove all TACACS+ servers from the list, on the TACACS+ page, select the check box in the check box column and then select Delete.

- **Edit**
  Modifies settings within a TACACS+ server configuration. When you select Edit, you are automatically redirected to the Edit TACACS+ Server page.

New TACACS+ Server page
Provides settings for configuring a TACACS+ server.

- **Name**
  Enter the name of the TACACS+ server.

- **Server Name/IP**
  Enter the server domain name or IP address of the TACACS+ server.

- **Server Key**
  Enter the key to access the TACACS+ server. The server key should be a maximum of 16 characters in length.

- **Authentication Type**
  Select the authentication type to use for the TACACS+ server. Selection includes: Auto, ASCII, PAP, CHAP, and MSCHAP. Auto authenticates using PAP, MSCHAP, and CHAP (in that order).

Directory Service

Windows Active Directory (AD) and Novell eDirectory provide central authentication services by storing information about network resources across a domain (a logical group of computers running versions of an operating system) in a central directory database. Each person who uses computers within a domain receives his or her own unique account/user name. This account can be assigned access to resources within the domain. In a domain, the directory resides on computers that are configured as domain controllers. A domain controller is a server that manages all security-related features that affect the user/domain interactions, security centralization, and administrative functions.
FortiGate units use firewall policies to control access to resources based on user groups configured in the policies. Each FortiGate user group is associated with one or more Directory Service user groups. When a user logs in to the Windows or Novell domain, a Fortinet Server Authentication Extension (FSAE) sends the unit the user’s IP address and the names of the Directory Service user groups to which the user belongs.

The FSAE has two components that you must install on your network:

- The domain controller (DC) agent must be installed on every domain controller to monitor user logins and send information about them to the collector agent.
- The collector agent must be installed on at least one domain controller to send the information received from the DC agents to the FortiGate unit.

The unit uses this information to maintain a copy of the domain controller user group database. Because the domain controller authenticates users, the unit does not perform authentication. It recognizes group members by their IP address.

You must install the Fortinet Server Authentication Extensions (FSAE) on the network and configure the unit to retrieve information from the Directory Service server. For more information about FSAE, see the *Fortinet Server Authentication Extension Administration Guide*.

Directory Service servers are configured in *User > Directory Service > Directory Service*. Use the following table when configuring directory service servers.

**Directory Service page**
Lists each individual directory service server, which includes all FSAE collector agents configured for that server. On this page, you can edit, delete or create a new directory service.

**Note:** You can create a redundant configuration on your unit if you install a collector agent on two or more domain controllers. If the current (or first) collector agent fails, the FortiGate unit switches to the next one in its list of up to five collector agents.

- **Create New** Add a new Directory Service server. When you select Create New, you are automatically redirected to the New page.
- **Name** Select the Expand arrow beside the server/domain/group name to display Directory Service domain and group information.
- **AD Server** The name defined for the Directory Service server.
- **Domain** The domain name imported from the Directory Service server.
- **Groups** The group names imported from the Directory Service server.
- **FSAE Collector IP** The IP addresses and TCP ports of up to five FSAE collector agents that send Directory Service server login information to the FortiGate unit.
- **Delete** Removes a Directory Service server from the list on the Directory Service page.
  
  To remove multiple Directory Service servers from within the list, on the Directory Service page, in each of the rows of servers you want removed, select the check box and then select Delete. To remove all Directory Service servers from the list, on the Directory Service page, select the check box in the check box column and then select Delete.

  - **Edit** Modifies settings within a directory service server configuration. When you select Edit, you are automatically redirected to the Edit page.
  - **Add User/Group** Adds a user or group to the list on the Directory Service page. You must know the distinguished name for the user or group.
    
    When you select Add User/Group, you are automatically redirected to the Add User/Group page.
  - **Refresh** Refreshes the current information on the page.
  - **Edit Users/Groups** Modifies users or groups from the remote server. When you select Edit Users/Groups, you are automatically redirected to the Edit Users/Groups page.
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 user name or password are necessary. Firewall and SSL VPN are the only user groups that can use PKI authentication.

If your unit is currently running FortiOS 4.0 MR2, you must configure a PKI user first to enable the PKI menu in the web-based manager. You can then configure other PKI users in User > PKI > PKI.

Use the following table when configuring PKI users.

### PKI page
Lists each individual PKI user that you have created. On this page, you can edit, delete or create a new PKI user.

- **Create New**: Creates a new PKI user. When you select Create New, you are automatically redirected to the New PKI User page.
- **Name**: The name of the PKI user.
- **Subject**: The text string that appears in the subject field of the certificate of the authenticating user.
- **CA**: The CA certificate that is used to authenticate this user.
- **Delete**: Removes a PKI user from the list on the PKI page. The delete icon is not available if the peer user belongs to a user group. Remove it from the user group first. To remove multiple PKI users from within the list, on the PKI page, in each of the rows of users you want removed, select the check box and then select Delete. To remove all PKI users from the list, on the PKI page, select the check box in the check box column and then select Delete.
- **Edit**: Modifies settings within the PKI user configuration. When you select Edit, you are automatically redirected to the Edit PKI User page.
New PKI User page
Provides settings for configuring a new PKI user.

Name
Enter the name of the PKI user.

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.

Two-factor authentication section

Require two-factor authentication
Require this PKI user to authenticate by password in addition to certificate authentication. Enter a Password.

Password
Enter the password that this PKI user must enter.

Peer users and peer groups
You can define peer users and peer groups used for authentication in some VPN configurations and for PKI certificate authentication in firewall policies. Defining peer users and peer groups is configured in the CLI.

A peer user is a digital certificate holder that can use PKI authentication. Before using PKI authentication, you must define peer users to include in the user group that is incorporated into the firewall authentication policy.

To define a peer user, you need:
• a peer user name
• the text from the subject field of the certificate of the authenticating peer user, or the CA certificate used to authenticate the peer user.

You can add or modify other configuration settings for PKI authentication.

Peer users are created in User > PKI > PKI for authentication; however, you must enter a value for at least one of the fields, Subject or CA. You can configure peer user groups only through the CLI.

Monitor
You can go to the Monitor menu to view lists of currently authenticated users, authenticated IM users, and banned users. For each authenticated user, the list includes the user name, user group, how long the user has been authenticated (Duration), how long until the user’s session times out (Time left), and the method of authentication used. The list of IM users includes the source IP address, protocol, and last time the protocol was used. The Banned User list includes users configured by administrators in addition to those quarantined based on AV, IPS, or DLP rules.

This topic contains the following:
• Firewall user monitor list
• IM user monitor list
• The Banned User list
Firewall user monitor list

In some environments, it is useful to determine which users are authenticated by the FortiGate unit and allow the system administrator to de-authenticate (stop current session) users. With the Firewall monitor, you can de-authenticate all currently authenticated users, or select single users to de-authenticate. To permanently stop a user from re-authenticating, change the FortiGate configuration (disable a user account) and then use the User monitor to immediately end the user’s current session.

Monitored firewall users are viewed from User > Monitor > Firewall.

Firewall page

Lists all authenticated firewall users that are currently authenticated by the FortiGate unit and are active. This page allows you to refresh the information on the page, as well as filter the information.

Refresh
Refresh the Firewall user monitor list.

Page Controls
User to navigate through the list.

Column Settings
Customize the table view. You can select the columns to hide or display and specify the column displaying order in the table.

Clear All Filters
Remove all filters applied to the Firewall user monitor list.

De-authenticate All Users
Stop authenticated sessions for all users in the firewall user monitor list. User(s) must re-authenticate with the firewall to resume their communication session.

Filter icons
Edit the column filters to filter or sort the firewall user monitor list according to the criteria you specify.

User Name
The user names of all connected remote users. By selecting the green arrow, you can list the user names according to descending or ascending order.

User Group
The user group that the remote user is part of.

Duration
Length of time since the user was authenticated.

Time-left
Length of time remaining until the user session times out. Only available if the authentication time of the session will be automatically extended (authentication keepalive is enabled). If authentication keepalive is not enabled, the value in Time-left will be N/A.

IP Address
The user’s source IP address.

Traffic Volume
The amount of traffic through the FortiGate unit generated by the user.

Method
Authentication method used for the user by the FortiGate unit (authentication methods can be FSAE, firewall authentication, or NTLM).

IM user monitor list

User lists can be managed to allow or block certain users. Each user can be assigned a policy to allow or block activity for each IM protocol. Each IM function can be individually allowed or blocked providing the administrator the granularity to block the more bandwidth consuming features such as voice chat while still allowing text messaging. The IM user monitor list displays information about instant messaging users who are currently connected. The list can be filtered by protocol. After IM users connect through the firewall, the FortiGate unit displays which users are connected. You can analyze the list and decide which users to allow or block.

Active IM users are viewed from User > Monitor > IM.

IM page

Lists all active IM users that are currently active. This page allows you to view blocked users as well as users that are currently using a particular IM protocol, such as MSN.

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.
The Banned User list

The Banned User list shows all IP addresses and interfaces blocked by NAC quarantine. The list also shows all IP addresses, authenticated users, senders, and interfaces blocked by Data Leak Prevention (DLP). The system administrator can selectively release users or interfaces from quarantine or configure quarantine to expire after a selected time period.

All sessions started by users or IP addresses on the Banned User list are blocked until the user or IP address is removed from the list. All sessions to an interface on the list are blocked until the interface is removed from the list.

You can configure NAC quarantine to add users or IP addresses to the Banned User list under the following conditions:

- **Users or IP addresses that originate attacks detected by IPS** - To quarantine users or IP addresses that originate attacks, enable and configure Quarantine Attackers in an IPS Sensor Filter. For more information, see "File filter configuration" on page 244.

- **IP addresses or interfaces that send viruses detected by virus scanning** - To quarantine IP addresses that send viruses or interfaces that accept traffic containing a virus, enable Quarantine Virus Sender in an antivirus profile. For more information, see "AntiVirus" on page 242.

- **Users or IP addresses that are banned or quarantined by Data Leak Prevention** - Set various options in a DLP sensor to add users or IP addresses to the Banned User list. For more information, see "Compound rules" on page 284.

Banned users are viewed from User > Monitor > Banned User.

---

**Banned User page**

Lists all banned users.

**Page Controls** Use to navigate through the list.

**Clear** Removes all users and IP addresses from the Banned User list.

**#** The position number of the user or IP address in the list.

**Application Protocol** The protocol that was used by the user or IP address added to the Banned User list.

**Cause or rule** The FortiGate function that caused the user or IP address to be added to the Banned User list. Cause or rule can be IPS, Antivirus, or Data Leak Prevention.

**Created** The date and time the user or IP address was added to the Banned User list.

**Expires** The date and time the user or IP address will be automatically removed from the Banned User list. If Expires is Indefinite you must manually remove the user or host from the list.

**Delete** Removes the selected user or IP address from the Banned User list.
WAN optimization and web caching

This section provides an introduction to the WAN Opt. & Web Cache menu. If you require more information about the features in the WAN Opt. & Web Cache menu, see the FortiOS Handbook.

The following topics are included in this section:

- WAN optimization rules
- WAN optimization peers
- Peer authentication groups
- WAN optimization monitoring
- Web cache settings
- Cache exempt list

WAN optimization rules

The Rules menu allows you to configure WAN optimization rules. These rules are similar to firewall policies, as the unit decides after matching a WAN optimization rule how to optimize the traffic over the WAN. WAN optimization rules also apply features, such as byte-caching to optimized traffic.

The Rules menu allows you to add, delete, edit, and re-order rules in the list. WAN optimization rules are displayed in the list in their order of matching precedence.

Before you add WAN optimization rules, you must add firewall policies to accept the traffic that you want to optimize. Then you add WAN optimization rules that match WAN traffic to be optimized that is accepted by a firewall policy according to source and destination addresses and destination port of the traffic. You also must add the WAN optimization techniques to be applied to the traffic.

WAN optimization rules are configured in WAN Opt & Cache > Rule > Rule.

<table>
<thead>
<tr>
<th>Rule page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists each individual WAN opt rule that you created. On this page, you can delete, edit or create a new WAN opt rule. You can also insert or move a WAN opt rule in the list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a new rule set. New rules are added to the bottom of the list. When you select Create New, you are automatically redirected to the New WAN Optimization Rule page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select to enable a rule or deselect to disable a rule. A disabled rule is out of service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>The rule identifier. Rules are numbered in the order they are added to the rule list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>The source address or address range that the rule matches.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>The destination address or address range that the rule matches.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>The destination port number or port number range that the rule matches.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates whether you have selected byte caching in the WAN optimization rule.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Auto-Detect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates whether the rule is an active (client) rule, a passive (server) rule or if auto-detect is off. If auto-detect is off, the rule can be a peer-to-peer rule or a Web Cache Only rule.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td><strong>Peer</strong></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
</tr>
<tr>
<td><strong>SSL</strong></td>
</tr>
<tr>
<td><strong>Secure Tunnel</strong></td>
</tr>
<tr>
<td><strong>Delete</strong></td>
</tr>
<tr>
<td><strong>Edit</strong></td>
</tr>
<tr>
<td><strong>Insert WAN Optimization Rule Before</strong></td>
</tr>
<tr>
<td><strong>Move To</strong></td>
</tr>
<tr>
<td>• <strong>Rule ID</strong></td>
</tr>
<tr>
<td>• <strong>Move To</strong></td>
</tr>
<tr>
<td>For example, you are moving Rule 1 to be above Rule 12 so the ID is 12.</td>
</tr>
</tbody>
</table>

### New WAN Optimization Rule page

Provides settings for configuring a WAN opt rule. The options that appear in WAN optimization rules depend on how you configure the rule. This section describes all of the options.

| **Mode** | Select Full Optimization to add a rule that can apply all WAN optimization features. Select Web Cache Only to add a rule that just applies web caching. If you select Web Cache Only, you can configure the source and destination address and port for the rule. You can also select Transparent Mode and Enable SSL. |
| **Source** | Enter an IP address, followed by a forward slash (/), then subnet mask, or enter an IP address range separated by a hyphen. Only packets whose source address header contains an IP address matching this IP address or address range will be accepted by and subject to this rule. For a passive rule, the server (passive) source address range should be compatible with the source addresses of the matching client (active) rule. To match one passive rule with many active rules, the passive rule source address range should include the source addresses of all of the active rules. |
| **Destination** | Enter an IP address, followed by a forward slash (/), then subnet mask, or enter an IP address range separated by a hyphen. Only a packet whose destination address header contains an IP address matching this IP address or address range will be accepted by and subject to this rule. Tip: For a Web Cache Only rule, if you set Destination to 0.0.0.0, the rule caches web pages on the Internet or any network. For a passive rule, the server (passive) destination address range should be compatible with the destination addresses of the matching client (active) rule. To match one passive rule with many active rules, the passive rule destination address range should include the destination addresses of all of the active rules. |
| **Port** | Enter a single port number or port number range. Only packets whose destination port number matches this port number or port number range will be accepted by and subject to this rule. For a passive rule, the server (passive) port range should be compatible with the port range of the matching client (active) rule. To match one passive rule with many active rules, the passive rule port range should include the port ranges of all of the active rules. |
Auto-Detect

Available only if Mode is set to Full Optimization.
Specify whether the rule is an Active (client) rule, a Passive (server) rule or if auto-detect is Off. If auto-detect is off the rule is a peer-to-peer rule.

- For an Active (client) rule, you must select all of the WAN optimization features to be applied by the rule. You can select the protocol to optimize, transparent mode, byte caching, SSL offloading, secure tunneling, and an authentication group.
- A Passive (server) rule uses the settings in the active rule on the client FortiGate unit to apply WAN optimization settings. You can also select web caching for a passive rule.
- If Auto-Detect is Off, the rule must include all required WAN optimization features and you must select a Peer for the rule. Select this option to configure peer-to-peer WAN optimization where this rule can start a WAN optimization tunnel with this peer only.

Protocol

Available only if Mode is set to Full Optimization, and Auto-Detect is set to Off or Active.
Select CIFS, FTP, HTTP, or MAPI to apply protocol optimization for one of these protocols.
Select TCP if the WAN optimization tunnel accepts sessions that use more than one protocol or that do not use the CIFS, FTP, HTTP, or MAPI protocol.

Peer

Available only if Mode is set to Full Optimization, and Auto-Detect is set to Off. Select the peer host ID of the peer that this peer-to-peer WAN optimization rule will start a WAN optimization tunnel with. You can also select [Create New ...] to add a new peer.

Enable Web Cache

Available only if Mode is set to Full Optimization, and Auto-Detect is set to Off or Passive. If Auto-Detect is set to Off, then Protocol must be set to HTTP.
Select to apply WAN optimization web caching to the sessions accepted by this rule.

Transparent Mode

Servers receiving packets after WAN optimization “see” different source addresses depending on whether or not you select Transparent Mode. You can select this option if Auto-Detect is set to Active or Off. You can also select it for Web Cache Only rules.
Select this option to keep the original source address of the packets when they are sent to servers. The servers appear to receive traffic directly from clients. The server network should be configured to route traffic with client source IP addresses from the server side FortiGate unit to the server and back to the server side FortiGate unit.
If this option is not selected, the server side FortiGate unit changes the source address of the packets received by servers to the address of the server side FortiGate unit interface that sends the packets to the servers. So servers appear to receive packets from the server side FortiGate unit. Routing on the server network is usually simpler in this case because client addresses are not involved, but the server sees all traffic as coming from the server side FortiGate unit and not from individual clients.

Enable Byte Caching

Available only if Mode is set to Full Optimization, and Auto-Detect is set to Off or Active.
Select to apply WAN optimization byte caching to the sessions accepted by this rule.

Enable SSL

Available only if Auto-Detect is set to Active or Off.
Select to apply SSL offloading for HTTPS traffic. You can use SSL offloading to offload SSL encryption and decryption from one or more HTTP servers to the unit. If you enable this option, you must configure the rule to accept SSL-encrypted traffic, for example, by configuring the rule to accept HTTPS traffic by setting Port to 443.
If you enable SSL offloading, you must also use the CLI command `config wanopt ssl-server` to add an SSL server for each HTTP server that you want to offload SSL encryption/decryption for.
WAN optimization peers

The Peers menu allows you to configure WAN optimization peers. A WAN optimization peer is a client-side FortiGate unit which sends a WAN optimization tunnel request to another peer, which is a server-side FortiGate unit. During this communicative process, the WAN optimization peers identify and authenticate with each other.

Peers are configured in **WAN Opt. & Cache > Peer > Peer**.

**Peer page**
Lists each individual WAN opt peer that you created.

- **Create New**
  Creates a new peer. When you select Create New, you are automatically redirected to the New WAN Optimization Peer page.

- **Local Host ID**
  Enter the local host ID of this FortiGate unit and select Apply. If you add this unit as a peer to another unit, use this local host ID as its peer host ID.

- **Apply**
  Save a change to the Local Host ID to the FortiGate configuration.

- **Edit**
  Modifies settings within the peer. When you select Edit, you are automatically redirected to the Edit WAN Optimization Peer page.

**New WAN Optimization Peer page**
Provides settings for configuring a peer host ID and IP address for the peer.

- **Peer Host ID**
  The peer host ID of the peer FortiGate unit. This is the local host ID added to the peer FortiGate unit.

- **IP Address**
  The IP address of the unit. Usually, this is the IP address of the FortiGate interface connected to the WAN.

---

**Peer authentication groups**

You need to add authentication groups to support authentication and secure tunneling between WAN optimization peers. Authentication groups are groups of WAN optimization peers.

Authentication groups are configured in **WAN Opt. & Cache > Peer > Authentication Group**.

**Authentication Group page**
Lists each individual authentication group that you created. On this page, you can edit, delete or create a new authentication group.

- **Create New**
  Creates a new authentication group. When you select Create New, you are automatically redirected to the New Authentication Group page.

- **Name**
  The name of the authentication group.
### Authentication method
The method used to authenticate the tunnels: certificate (plus certificate name) or pre-shared key.

### Peer(s)
The host IDs of the peers added to the authentication group. When you add the authentication group to a WAN optimization rule, only these units can authenticate to use this WAN optimization rule. Peer(s) can be any peer, a peer added to the unit peer list (defined peers), or a selected peer.

### Delete
Removes an authentication group from the list on the Authentication Group page. You must delete each authentication group individually because removing multiple authentication groups at one time is not supported.

### Edit
Modifies settings within the authentication group. When you select *Edit*, you are automatically redirected to the Edit Authentication Group page.

### New Authentication Group page
Provides settings for configuring an authentication group.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Add or change the name of the authentication group. Select this name when adding the authentication group to a rule. Other units that participate in WAN optimization tunnels with this unit must have an authentication group with the same name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Method</strong></td>
<td>Select the authentication method to use. Select <em>Certificate</em> if you want to use a certificate to authenticate and encrypt WAN optimization tunnels. Select <em>Pre-shared key</em> if you want to use a pre-shared key or password to authenticate and encrypt WAN optimization tunnels.</td>
</tr>
<tr>
<td><strong>Certificate (list)</strong></td>
<td>Available only when Authentication Method is <em>Certificate</em>. Select a local certificate that has been added to this unit. Other units that participate in WAN optimization tunnels with this unit must have an authentication group with the same name and certificate. Go to System &gt; Certificates &gt; Local Certificates to add a local certificate to a unit.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Available only when Authentication Method is <em>Pre-shared key</em>. Add the password (or pre-shared key) used by the authentication group. Other units that participate in WAN optimization tunnels with this unit must have an authentication group with the same name and password. The key must contain at least 6 printable characters and should be known only by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Peer Acceptance</strong></td>
<td>One or more of the following options are available to authenticate WAN optimization peers:</td>
</tr>
<tr>
<td><strong>Accept Any Peer</strong></td>
<td>Authenticate with any peer. Use this setting if you do not know the peer host IDs or IP addresses of the peers that will use this authentication group. This setting is most often used for WAN optimization with the FortiClient application.</td>
</tr>
<tr>
<td><strong>Accept Defined Peers</strong></td>
<td>Authenticate with any peer in the unit's peer list.</td>
</tr>
<tr>
<td><strong>Specify Peer</strong></td>
<td>Authenticate with the selected peer only. Select this option and then select the peer to add to this authentication group.</td>
</tr>
</tbody>
</table>

### WAN optimization monitoring
By using WAN optimization monitoring, you can view and improve WAN optimization performance. The monitoring tools help isolate performance problems, aid in troubleshooting, and enable network optimization and capacity planning.

The monitor unit uses collected log information and presents it in a graphical format to show network traffic summary and bandwidth optimization information.

WAN optimization monitoring is viewed from *WAN Opt. & Cache > Monitor > Monitor*. 

---

**Feedback**

[http://docs.fortinet.com/](http://docs.fortinet.com/) • [Feedback](http://docs.fortinet.com/)
**Monitor page**

Provides two widgets that display information about traffic and bandwidth optimization. The Traffic Summary widget displays protocol information as well as a pie chart. The Bandwidth Optimization widget displays its information in the form of a bar chart, however you can change the type of chart.

**Traffic Summary widget of the Monitor page**

This section provides traffic optimization information. The pie chart illustrates the percentage of traffic for supported applications processed during the selected *Period*. The table displays how much traffic has been reduced by WAN optimization by comparing the amount of LAN and WAN traffic for each protocol.

<table>
<thead>
<tr>
<th>Refresh</th>
<th>Refresh the Traffic Summary.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Period</strong></td>
<td>Select a time period to show traffic summary for. You can select:</td>
</tr>
<tr>
<td></td>
<td>• Last 10 Minutes</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Hour</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Day</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Week</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Month</td>
</tr>
<tr>
<td><strong>Reduction Rate</strong></td>
<td>Displays each application’s optimization rate. For example, a rate of 80 percent means the amount of data processed by that application has been reduced by 20 percent.</td>
</tr>
<tr>
<td><strong>LAN</strong></td>
<td>The amount of data in MB received from the LAN for each application.</td>
</tr>
<tr>
<td><strong>WAN</strong></td>
<td>The amount of data in MB sent across the WAN for each application. The greater the difference between the LAN and WAN data, the greater the amount of data reduced by WAN optimization byte caching, web caching, and protocol optimization.</td>
</tr>
</tbody>
</table>

**Bandwidth Optimization widget of the Monitor page**

This section shows network bandwidth optimization per time *Period*. A line or column chart compares an application’s pre-optimized (LAN data) size with its optimized size (WAN data).

<table>
<thead>
<tr>
<th>Refresh</th>
<th>Select to refresh the Bandwidth Optimization display.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Period</strong></td>
<td>Select a time frame to show bandwidth optimization. You can select:</td>
</tr>
<tr>
<td></td>
<td>• Last 10 Minutes</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Hour</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Day</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Week</td>
</tr>
<tr>
<td></td>
<td>• Last 1 Month</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Select <em>All</em> to display bandwidth optimization for all applications. Select an individual protocol to display bandwidth optimization for that individual protocol.</td>
</tr>
<tr>
<td><strong>Chart Type</strong></td>
<td>Select to display bandwidth optimization with a line chart or a column chart.</td>
</tr>
</tbody>
</table>

**Web cache settings**

In most cases the default settings for the WAN optimization web cache are acceptable. However, you may want to change them to improve performance, increase or decrease the size of objects that can be cached, or optimize the cache for your configuration.

If you want to allow exempt URLs from being cached, you must enable this setting in the CLI and then configure a URL filter list of the exempted URLs that you do not want cached. The command syntax for exempting URLs from being cached is:

```
config wanopt webcache
set explicit enable
set cache-exempt enable
end
```

For more information about many of these web cache settings, see RFC 2616.
Web cache settings are configured in **WAN Opt. & Cache > Cache > Settings**.

**Settings page**
Provides settings for configuring a the WAN opt web cache.

- **Always revalidate**
  Select to always revalidate requested cached objects with content on the server before serving them to the client.

- **Max Cache Object Size**
  Set the maximum size of objects (files) that are cached. The default size is 512000 KB. This setting determines the maximum object size to store in the web cache. Objects that are larger than this size are still delivered to the client but are not stored in the FortiGate web cache.

- **Negative Response Duration**
  Set how long in minutes to cache negative responses. The default is 0, meaning negative responses are not cached. The content server might send a client error code (4xx HTTP response) or a server error code (5xx HTTP response) as a response to some requests. If the web cache is configured to cache these negative responses, it returns that response in subsequent requests for that page or image for the specified number of minutes.

- **Fresh Factor**
  Set the fresh factor as a percentage. The default is 100, and the range is 1 to 100. For cached objects that do not have an expiry time, the web cache periodically checks the server to see if the objects have expired. The higher the **Fresh Factor** the less often the checks occur.

  For example, if you set the **Max TTL** value and **Default TTL** to 7200 minutes (5 days) and set the **Fresh Factor** to 20, the web cache check the cached objects 5 times before they expire, but if you set the **Fresh Factor** to 100, the web cache will check once.

- **Max TTL**
  The maximum amount of time (Time to Live) an object can stay in the web cache without the cache checking to see if it has expired on the server. The default is 7200 minutes (120 hours or 5 days).

- **Min TTL**
  The minimum amount of time an object can stay in the web cache before the web cache checks to see if it has expired on the server. The default is 5 minutes.

- **Default TTL**
  The default expiry time for objects that do not have an expiry time set by the web server. The default expiry time is 1440 minutes (24 hours).

- **Explicit Proxy**
  Indicates whether the explicit web proxy has been enabled for the FortiGate unit. See "Configuring the explicit web proxy" on page 85.

- **Enable Cache Explicit Proxy**
  Select to use WAN optimization web caching to cache content received by the explicit web proxy.

- **Ignore If-modified-since**
  By default, if the time specified by the if-modified-since (IMS) header in the client's conditional request is greater than the last modified time of the object in the cache, it is a strong indication that the copy in the cache is stale. If so, HTTP does a conditional GET to the Overlay Caching Scheme (OCS), based on the last modified time of the cached object.

  Enable ignoring if-modified-since to override this behavior.

- **HTTP 1.1 Conditionals**
  HTTP 1.1 provides additional controls to the client over the behavior of caches toward stale objects. Depending on various cache-control headers, the unit can be forced to consult the OCS before serving the object from the cache. For more information about the behavior of cache-control header values, see RFC 2616.

- **Pragma-no-cache**
  Typically, if a client sends an HTTP GET request with a pragma no-cache (PNC) or cache-control no-cache header, a cache must consult the OCS before serving the content. This means that the unit always re-fetches the entire object from the OCS, even if the cached copy of the object is fresh. Because of this behavior, PNC requests can degrade performance and increase server-side bandwidth utilization. However, if you enable ignoring Pragma-no-cache, then the PNC header from the client request is ignored. The unit treats the request as if the PNC header is not present.
Cache exempt list

The Cache exempt list is a list of URL addresses that will be exempted from being cached. You can enable or disable each URL address within the list. Cache exempt lists are configured in WAN Opt. & Cache > Cache > Exempt List.

**Exempt List page**
Lists all the URL addresses that will be exempted from being cached. On this page, you can edit, delete, or enter a new URL address and add it to the list.

- **Create New**
  Creates a new URL address that is added to the web cache exempt list on the Exempt List page. When you select Create New, you are automatically redirected to the New Exempt URL page.

- **Edit**
  Modifies the URL address. When you select Edit, you are automatically redirected to the Edit Exempt URL page.

- **Delete**
  Removes the URL address from the list on the Exempt List page.
  To remove multiple URLs from within the list on the Exempt List page, in each of the rows of the URLs you want removed, select the check box and then select Delete.
  To remove all URLs from the list, on the Exempt List page, select the check box in the check box column, and then select Delete.

- **URL Pattern**
  The URL address.

- **Status**
  The status of the URL address. A green check mark indicates that it is enabled and will be included in the list. A gray x indicates that it is disabled and will not be included in the list.

**New Exempt URL page**
Provides settings for configuring a new URL address to add to the list.

- **URL Pattern**
  Enter the URL address in the field provided.

- **Enable**
  Select the check box to enable the URL address within the list.
  To disable a URL address, edit the URL address and then select the check box beside Enable to disable it.
Endpoint

Endpoint enforces the use of the FortiClient End Point Security (Enterprise Edition) application on your network. It can also allow or deny endpoints access to the network based on the applications installed on them.

FortiClient enforcement can check that the endpoint is running the most recent version of the FortiClient application, that the antivirus signatures are up-to-date and that the firewall is enabled. An endpoint is most often a single PC with a single IP address being used to access network services through a FortiGate unit.

You enable endpoint in a firewall policy. When traffic attempts to pass through the firewall policy, the unit runs compliance checks on the originating host on the source interface. Non-compliant endpoints are blocked. If web browsing, the endpoints are redirected to a web portal that explains the non-compliance and provides a link to download the FortiClient application installer.

Introducing endpoint into your network is easy because the FortiGate unit can optionally recommend to non-compliant users to install FortiClient software, but allow them to continue without doing so.

You can monitor the endpoints that are subject to endpoint, viewing information about the computer, its operating system and detected applications.

This section includes the following topics:

- Endpoint configuration overview
- NAC
- Network Vulnerability Scan
- Monitoring endpoints

Note: Endpoint does not function if enabled in a firewall policy that contains a load balance VIP.

In FortiOS 4.0 MR2 GA (build-272), the network vulnerability scan feature does not work properly. Fortinet recommends upgrading to FortiOS 4.0 MR2 Patch 1 release (build-279) because it resolves the issues. The patch release also includes the Discovery Assets, Start Scan and Last Scan icons to the Asset page.

Endpoint configuration overview

Endpoint requires that all hosts using the firewall policy have the FortiClient Endpoint Security application installed. Make sure that all hosts affected by this policy are able to install this application. Currently, FortiClient Endpoint Security is available for Microsoft Windows 2000 and later only.

To set up endpoint, you need to

- Enable Central Management by the FortiGuard Analysis & Management Service if you will use FortiGuard Services to update the FortiClient application or antivirus signatures. You do not need to enter account information.
- Configure the minimum required version of FortiClient and the source of FortiClient installer downloads for non-compliant endpoints. See “Configuring FortiClient installer download and version enforcement” on page 349.
• Define application detection lists to specify which applications are allowed or not allowed. Optionally, you can deny access to endpoints that have applications installed that are not on the detection list. See “Configuring application sensors” on page 347.

• Configure Endpoint profiles which specify the FortiClient enforcement settings and the application detection list to apply. You select the Endpoint profile to use when you enable Endpoint in the firewall policy.

• Enable Endpoint in firewall policies.

• Optionally, modify the inactivity timeout for endpoints. The default is 5 minutes. After that time period, the FortiGate unit rechecks the endpoint for Endpoint compliance. To change the timeout, adjust the compliance-timeout value in the config endpoint-control settings CLI command.

You can also modify the appearance of the Endpoint Download Portal and the Endpoint Recommendation Portal. These are replacement messages.

NAC

The NAC menu allows you to configure profiles, application sensors and databases, including network monitoring.

This topic includes the following:

• Configuring Endpoint profiles
• Configuring FortiClient installer download and version enforcement
• Configuring application sensors
• Viewing the application database

Configuring Endpoint profiles

An Endpoint profile contains FortiClient enforcement settings and can specify an application detection list. Firewall policies can apply an Endpoint profile to the traffic they handle.

Configure endpoint profiles from Endpoint > NAC > Profile, using the following table.

| Profile page | Creates a new endpoint profile. You can apply these profiles to firewall policies. When you select Create New, you are automatically redirected to New Endpoint NAC Profile page. |
| Create New | | |
| Edit | Modifies settings within the NAC profile. When you select Edit, you are automatically redirected to the Edit Endpoint NAC Profile page. |
| Delete | Removes a NAC profile from the Profile page. |
| Name | The name of the endpoint profile. |
| Action | The type of action that the unit will take. |
| Additional Client Options | Green check mark icon - enabled. |
| Application Detection List | The application detection list specified in this profile. |

To remove multiple NAC profiles from within the list, on the Profile page, in each of the rows of the profiles you want removed, select the check box and then select Delete. To remove all profiles from the list, on the Profile page, select the check box in the check box column, and then select Delete.
Application sensors determine which applications are permitted or not permitted on network endpoints. An application sensor is part of an Endpoint profile that you can apply in your firewall policies. You can create multiple lists.

Application sensor is based on application signatures provided by FortiGuard Services. You create your application detection list entries by selecting applications from FortiGuard-supplied lists of categories, vendors, and application names. To view application information from FortiGuard services, go to Endpoint > NAC > Application Database.

Application sensor checks applications against the database from the top down until it finds a match. Specific entries, such as those that list one particular application, should precede more general entries, such as those that match all applications of a particular category.

Configure application sensors from Endpoint > NAC > Application Sensor, using the following table.
### Viewing the application database

You can view the application list provided by FortiGuard Services. Go to Endpoint > NAC > Application Database.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Delete | Removes an application sensor from the list on the Application Sensor page. To remove multiple application sensors from within the list, on the Application Sensor page, in each of the rows of the sensors you want removed, select the check box and then select Delete.
To remove all application sensors from the list, on the Application Sensor page, select the check box in the check box column, and then select Delete. |
| Name | The name of the application sensor. |
| # of Entries | The number of application entries in the list. |
| Profiles | The Endpoint profiles that use this application detection list. |
| Comments | The description, if given, to the application sensor. |

### Application Sensor Settings page

Provides settings for configuring sensors that contain applications.

| Name | Enter a name for the application sensor. |
| Comments | Enter a description for the application sensor. This is optional. |
| Other Applications (not specified below) | Select what to do if applications not included in this list are installed on the endpoint: • Allow — allow the endpoint to connect • Deny — quarantine the endpoint • Monitor — include this endpoint’s information in statistics and logs |
| OK | Select to save changes you made on the Application Sensor configuration settings page. |
| Create New | Creates a new application detection entry. When you select Create New on the Application Sensor Settings page, you are automatically redirected to the New Application Detection Entry page. |
| Category | Select a category from the drop-down list. |
| Vendor | Select a vendor from the drop-down list. The vendor is the application software’s creator. For example, if you select Adobe, Adobe Systems Incorporated is its vendor. |
| Application | Select an application from the drop-down list. |
| Status | Select the status of the application, whether its installed, running, not running or not installed. |
| Action | Select an action that the FortiGate unit will take. |
| ID | The identification number of the sensor in the list. This number identifies the sensor’s placement in the list. |
| Category | The category chosen for that application. |
| Vendor | The vendor chosen for that application. |
| Application | The name of the application. |
| Status | The action the FortiGate unit will take. |
| Edit | Select to modify an application’s settings. |
| Delete | Select to remove an application from the list on the page. |
| Insert | Select to insert a new application in the list on the page. |
| Move | Select to move an application either above or below another application in the list. |
**Application Database page**

Lists all the applications that are provided by FortiGuard Services

**Page controls**
Shows the current page number in the list. Select the left and right arrows to display the first, previous, next or last page of known endpoints.

**[Total Signatures: <number>]**
Displays the total number of signatures that are currently available.

**Column Settings**
Select the columns to display in the list. You can also determine the order in which they appear. For more information, see "Using column settings to control the columns displayed" on page 26.

**Clear All Filters**
Clear any column display filters you might have applied.

**Filter icons**
Edit the column filters to filter or sort the endpoints list according to the criteria you specify. For example, you could add a filter to the Detected Software column to display all endpoints running BitTorrent software. For more information, see "Adding filters to web-based manager lists" on page 24.

**Category**
The category the application is associated with.

**Name**
The name of the application.

**Vendor**
The vendor that the application is associated with. For example, the Adobe Reader is associated with the vendor, Adobe Systems Incorporated.

---

**Configuring FortiClient installer download and version enforcement**

You can set the minimum FortiClient version that endpoints are required to run from Endpoint > NAC > FortiClient. The FortiClient page also configures the download source for the FortiClient installer.

**FortiClient Endpoint Security page**
Provides settings for configuring and managing FortiClient installations.

**Information section**
Indicates the FortiGuard availability and current versions of antivirus and application signatures packages. This section also allows you to update your antivirus and application signature packages, as well as downloading a Windows Installer.

- **FortiGuard Availability**
  FortiGuard Services is available if the indicator is green.

- **FortiClient Endpoint Versions**
  FortiClient software versions available from FortiGuard Services are listed. Select the Download link to download the installer.

- **AV Signature Package**
  The latest AV signature package available from FortiGuard Services.

- **Application Signature Package**
  The latest application signature package available from FortiGuard Services.

- **FortiClient Downloads**
  The number of FortiClient software downloads through this FortiGate unit.

- **Update Now**
  Retrieve the latest information from FortiGuard Services.

**FortiClient Installer Download Location section**

Select one of the following options to determine the link that the FortiClient Download Portal provides to non-compliant users to download the FortiClient installer.

- **FortiGuard Distribution Network**
  The FortiClient application is provided by the FortiGuard Distribution Network. The FortiGate unit must be able to access the FortiGuard Distribution Network. If the FortiGate unit contains a hard disk drive, the files from FortiGuard Services are cached to more efficiently serve downloads to multiple end points.
Network Vulnerability Scan

The Network Scan menu allows you to configure scanning of your network, which was previously only found on FortiAnalyzer units or FortiScan.

This topic includes the following:

- Configuring assets
- Schedule a scan

Configuring assets

You can configure multiple assets in the Network Vulnerability Scan menu.

Configure assets from Endpoint > Network Vulnerability Scan > Asset, using the following table.

<table>
<thead>
<tr>
<th>Asset page</th>
<th>Lists each individual asset that you created. On this page, you can edit, delete or create a new asset.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new asset. When you select Create New, you are automatically redirected to the Asset page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies an asset. When you select Edit, you are automatically redirected to the Asset page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select to remove an asset from the list on the page.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the asset.</td>
</tr>
<tr>
<td>IP Address/Range</td>
<td>If Host was chosen as the type for the asset, then the IP address of the host displays. If Range was chosen as the type for the asset, the IP address range appears.</td>
</tr>
<tr>
<td>Enable Scan</td>
<td>Displays whether or not the asset is enabled for scanning.</td>
</tr>
<tr>
<td>Last Discovery</td>
<td>The last discovery that the asset found.</td>
</tr>
</tbody>
</table>

Asset Settings page

Provides settings for configuring an asset.

Name | Enter a name for the asset that you are creating.

Note: Select This FortiGate or Custom URL if you want to provide a customized FortiClient application. This is required if a FortiManager unit will centrally manage FortiClient applications. For information about customizing the FortiClient application, see the FortiClient Administration Guide.
Schedule a scan

You can configure a network scan for monitoring purposes. Schedule a scan from Endpoint > Network Vulnerability Scan > Scan using the following table.

Network Scan page
Provides settings for scheduling a scan and what type of scanning you want the unit to perform.

<table>
<thead>
<tr>
<th><strong>Scan Mode</strong></th>
<th>Select the mode the unit will use to scan for vulnerabilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick</td>
<td>checks only the most commonly used ports</td>
</tr>
<tr>
<td>Standard</td>
<td>checks only the ports used by the most known applications</td>
</tr>
<tr>
<td>Full</td>
<td>checks all TCP and UDP ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Schedule</strong></th>
<th>Select the schedule to begin and end the vulnerability scan.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually</td>
<td>performs a scan only on request</td>
</tr>
<tr>
<td>Schedule</td>
<td>a schedule of when the scan will be performed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Recurrence</strong></th>
<th>Select to have the schedule occur on a daily, weekly, or monthly basis.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weekly</td>
<td>the Day of Week drop-down list appears. If you select Monthly, the Day of Month drop-down list appears.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Time</strong></th>
<th>Select the time to start the schedule, in the format HH:MM.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Day of Week</strong></th>
<th>Select a day of the week from the drop-down list when you want to schedule a scan during the week.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Day of Month</strong></th>
<th>Select a day of the month from the drop-down list when you want to schedule a scan on that day of the month.</th>
</tr>
</thead>
</table>

Monitoring endpoints

Once an endpoint is added to the list, it remains there until you manually delete it or until the unit restarts. Every time an endpoint accesses network services through the unit (or attempts to access services) the entry for the endpoint is updated.

The endpoints list can provide an inventory of the endpoints on your network. Entries for endpoints not running the FortiClient application include the IP address, last update time, and traffic volume/attempts. The “non-compliant” status indicates the endpoint is not running the FortiClient application.

Entries for endpoints running the FortiClient application show much more information, depending on what is available for the FortiClient application to gather. Detailed information you can view includes endpoint hardware (CPU and model name) and the software running on the endpoints. You can adjust column settings and filters to display this information in many different forms.
From the endpoints list, you can view information for each endpoint, temporarily exempt endpoints from endpoint, and restore exempted end points to their blocked state.

View the list of known endpoints from Endpoint > Monitor > Endpoint Monitor. An endpoint is added to the list when it uses a firewall policy that has Endpoint enabled.

**Endpoint Monitor page**

Lists all the endpoints that are currently being monitored by the unit.

- **Refresh**
  Update the list.

- **View**
  Display Compliant or Non-compliant endpoints or Both. Compliant endpoints are running the minimum required version of FortiClient or a more recent version. To configure the minimum required version of FortiClient, see "Configuring FortiClient installer download and version enforcement" on page 349.

  The Status column displays a gray icon if the endpoint is non-compliant and a green icon if the endpoint is compliant. The Status column displays a green icon with an hourglass if the endpoint is non-compliant but has been temporarily exempted.

- **Page controls**
  Use to navigate through the list of monitored endpoints.

- **Column Settings**
  Select the columns to display in the list. You can also determine the order in which they appear. For more information, see "Using column settings to control the columns displayed" on page 26.

- **Clear All Filters**
  Clear any column display filters you might have applied.

- **Filter icons**
  Edit the column filters to filter or sort the endpoints list according to the criteria you specify. For example, you could add a filter to the Detected Software column to display all endpoints running BitTorrent software. For more information, see "Adding filters to web-based manager lists" on page 24.

- **View**
  View details about a selected endpoint. Select this icon to display the information about the endpoint found by the FortiClient application.

- **Exempt Temporarily icon**
  Exempt the selected endpoint from Endpoint. This means an endpoint that is blocked and added to the endpoint list can temporarily access network services through the unit. When you select this icon you can specify how long the end point is exempted from Endpoint. The default exempt duration is 600 seconds.

- **Restore to Blocked State icon**
  Resume blocking access for a temporarily exempted endpoint.

- **Column Settings**
  Select Column Settings determine which of the following columns to display. All information that appears in the columns is reported by the FortiClient application running on the endpoint, unless otherwise noted.

- **AV signature**
  The version of the FortiClient antivirus signatures installed on the endpoint.

- **Computer Manufacturer**
  The name of the manufacturer of the endpoint.

- **Computer Model**
  The model name of the endpoint.

- **CPU Model**
  The CPU running on the endpoint.

- **Compliant**
  The name of the compliant signature.

- **Detected Applications**
  The software applications detected on this endpoint. See "Configuring application sensors" on page 347. You can control the applications that appear in the Detected Software column by editing the Detected Software filter. See "Adding filters to web-based manager lists" on page 24.

- **FortiClient Version**
  The version of the FortiClient application running on the endpoint.

- **Host Name**
  The host name of the endpoint.

- **Installed FCT Features**
  The FortiClient features enabled on the endpoint.
<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong></td>
<td>The IP address of the endpoint as found from the communication session. The FortiClient application is not required to obtain this information.</td>
</tr>
<tr>
<td><strong>Last Update</strong></td>
<td>The time that the status of the endpoint was last verified by the unit. The FortiClient application is not required to obtain this information.</td>
</tr>
<tr>
<td><strong>Memory Size</strong></td>
<td>The amount of memory installed on the endpoint.</td>
</tr>
<tr>
<td><strong>OS Version</strong></td>
<td>The version of the operating system running on the endpoint.</td>
</tr>
<tr>
<td><strong>System Uptime</strong></td>
<td>The system up time of the endpoint.</td>
</tr>
<tr>
<td><strong>Traffic Volume/Attempts</strong></td>
<td>If the endpoint is compliant, this column displays the amount of data passed through the unit by communication sessions originating from the endpoint. If the endpoint is non-compliant, this column displays the number of times the endpoint has attempted to connect through the unit. The FortiClient application is not required to obtain this information.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>The name of the active user account on the endpoint.</td>
</tr>
</tbody>
</table>
Wireless Controller

Most FortiGate units, but not FortiWiFi models, can act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi units. All units must be running the most recent FortiOS 4.0 firmware.

You create virtual access points that can be associated with multiple physical access points. Clients can roam amongst the physical access points, extending the range of the wireless network.

The following topics are included in this section:

- Configuration overview
- Enabling the wireless controller
- Configuring FortiWiFi units as managed access points
- Configuring a virtual wireless access point
- Configuring a physical access point
- Configuring DHCP for your wireless LAN
- Configuring firewall policies for the wireless LAN
- Monitoring wireless clients
- Monitoring rogue APs

Configuration overview

When you begin setting up a wireless network, you need to do the following:

- Enable the wireless controller, if it is not already enabled.
- Configure FortiWiFi units to be managed by the wireless controller.
- Configure each virtual access point (VAP). A VAP has the SSID and security configuration settings you would find on a wireless access point device. Optionally, you can limit the number of simultaneous wireless clients who can use this VAP.
- Configure each physical access point (AP). The AP settings include the radio settings and rogue AP scan settings. You select the VAPs that will be carried on the physical access point. Optionally, you can limit the number of simultaneous clients this AP will accept.
- Configure DHCP service to provide addresses to your wireless clients.
- Configure firewall policies to enable communication between the wireless LAN and other networks.
Enabling the wireless controller

The wireless controller feature is hidden by default on some FortiGate models. If you decide to disable the Wireless Controller feature, all of the related configuration is discarded.

To enable the wireless controller
1. Go to System > Admin > Settings.
2. Select Enable Wireless Controller.
3. Select Apply.

Configuring FortiWiFi units as managed access points

You also need to enable each FortiWiFi unit to act as a managed physical access point (AP). You can do this in the CLI on each unit as follows:

```
config system global
    set wireless-terminal enable
end
```

The wireless functionality of a FortiWiFi unit in wireless terminal mode cannot be controlled from the unit itself.

If there are firewall devices between the wireless controller FortiGate unit and the managed FortiWiFi units, make sure that ports 5246 and 5247 are open. These ports carry, respectively, the encrypted control channel data and the wireless network data. If needed, you can change these ports in the CLI:

```
config system global
    set wireless-controller-port <port_int> (access controller)
    set wireless-terminal-port <port_int> (access point)
end
```

These commands set the control channel port. The data channel port is always the control port plus one. The port setting must match on the access controller and all access points.

Configuring a virtual wireless access point

A Virtual Access Point (VAP) defines the SSID and security settings for a wireless LAN. For each VAP, the FortiGate unit creates a virtual network interface. You create firewall policies to control traffic between the VAP interface and other networks. Users need the correct security settings to connect to the access point, and they can also be required to authenticate to use a firewall policy.

Configure VAP from Wireless Controller > Virtual AP > Virtual AP, using the following table.

<table>
<thead>
<tr>
<th>Virtual AP page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists each individual virtual AP that you have created. On this page, you can edit, delete or create a new virtual AP.</td>
<td></td>
</tr>
</tbody>
</table>

Create New: Creates a new VAP. When you select Create New, you are automatically redirected to the New Virtual AP page.

Edit: Modifies a virtual AP’s settings. When you select Edit, you are automatically redirected to the Edit Virtual AP page.
Delete
Removes a VAP from the list on the Virtual AP page.
To remove multiple VAPs from within the list, on the Virtual AP page, in each of the rows of the VAPs you want removed, select the check box and then select Delete.
To remove all VAPs from the list, on the Virtual AP page, select the check box in the check box column and then select Delete.

Name
The name of the virtual AP.

SSID
The SSID or network name for the wireless interface.

SSID Broadcast
The SSID broadcast that the clients use to connect to your wireless network.

Security mode
The type of security for the wireless interface.

Data Encryption
The type of encryption for the wireless interface.

Authentication
The type of authentication that the clients will use.

Clients
The maximum number of clients that is permitted to connect simultaneously.

New Virtual AP page
Provides settings for configuring a virtual AP which defines SSID and security settings for a wireless LAN.

Name
Enter a name to identify the VAP. This is also the name of the virtual network interface you will use in firewall policies.

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 with this network name.

SSID Broadcast
Select to broadcast the SSID. Broadcasting the SSID enables clients to connect to your wireless network without first knowing the SSID. For better security, do not broadcast the SSID.

Security Mode
Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface.

- **None** — has no security. Any wireless user can connect to the wireless network.
- **WEP64** — 64-bit web equivalent privacy (WEP). To use WEP64 you must enter a Key containing 10 hexadecimal digits (0-9 a-f) and inform wireless users of the key.
- **WEP128** — 128-bit WEP. To use WEP128 you must enter a Key containing 26 hexadecimal digits (0-9 a-f) and inform wireless users of the key.
- **WPA** — 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 eight characters or select a RADIUS server. If you select a RADIUS server, the wireless clients must have accounts on the RADIUS server.
- **WPA2** — WPA with more security features. To use WPA2 you must select a data encryption method and enter a pre-shared key containing at least eight characters or select a RADIUS server. If you select a RADIUS server the wireless clients must have accounts on the RADIUS server.
- **WPA2 Auto** — the same security features as WPA2, but 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. If you select a RADIUS server the wireless clients must have accounts on the RADIUS server.

Data Encryption
Select TKIP or AES encryption as appropriate for the capabilities of your wireless clients. This is available for WPA security modes.
Configuring a physical access point

The access controller needs to be configured to identify the FortiWiFi unit that provides the physical access point and the radio settings for the wireless LAN.

Configure physical access points from Wireless Controller > Physical AP > Managed Physical AP, using the following table.

### Managed Physical AP page

Lists each individual physical AP that you created. On this page, you can edit, delete or create a new physical AP.

- **Create New**
  Creates a new physical AP. When you select Create New, you are automatically redirected to the page New Managed Access Point.

- **Edit**
  Modifies a managed physical AP settings. When you select Edit, you are automatically redirected to the Configure Managed Access Point page.

- **Delete**
  Removes a managed physical AP in the list on the Managed Physical AP page.
  To remove multiple managed APs from within the list, on the Managed Physical AP page, in each of the rows of the APs you want removed, select the check box and then select Delete.
  To remove all APs in the list, on the Managed Physical AP page, select the check box in the check box column, and then select Delete.

- **Refresh**
  Select to refresh the current information on the page.

- **Admin**
  The type of access the virtual AP has. Disabled means that the AP is not managed.

- **Name**
  The name of the physical AP.

- **Virtual AP**
  The virtual APs that are carried on the physical.

- **Band/Channel**
  The band or channel that is being used for that physical AP.

- **Clients**
  The maximum number of clients that are permitted to connect simultaneously.

- **Rogue-AP Scan**
  The type of scan used to detect other APs and report on them in Wireless Controller > Rogue AP > Rogue AP.

- **Join Time**
  The time when the virtual APs connected to the physical AP.

### New Managed Access Point page

Provides settings for configuring a physical access point.

- **Serial Number**
  Enter the serial number of the FortiWiFi unit. This field is completed automatically if the AP discovers this AC and registers itself.

- **Name**
  Enter a name for the physical AP.
Configuring DHCP for your wireless LAN

Go to System > DHCP Server > Service to configure DHCP services to provide IP addresses to your wireless clients. Your Virtual Access Point is listed as an interface. See “Service” on page 90.

Configuring firewall policies for the wireless LAN

For your VAP clients to communicate with other networks, including other wireless LANs, you must have appropriate firewall policies. Your VAP has a virtual interface of the same name that you can select as the source or destination interface in firewall policies.

Monitoring wireless clients

In Wireless Controller > Wireless Client > Wireless Client, you can view information about wireless clients of your managed access points.

**Wireless Client page**

Lists all wireless clients that are associated with your managed access points. This page also allows you to view their bandwidth and signal strength.

**Refresh**

Update the information in the table.

**Page Controls**

Shows the current page number in the list. Select the left and right arrows to display the first, previous, next or last page of known endpoints.
Monitoring rogue APs

When you access the Rogue AP page, the page is divided into three sections, the Unknown Access Points section, Rogue Access Points, and Accepted Access Points.

The Unknown Access Points section displays detected access points that have not been designated as either Rogue or Accepted.

View information about detected APs in Wireless Controller > Rogue AP > Rogue AP.

### Rogue AP page

- **Refresh Interval**: Set time between information updates. *none* means no updates.
- **Refresh**: Updates displayed information now.
- **Inactive Access Points**: Select which inactive access points to show: all, none, those detected less than one hour ago, or those detected less than one day ago.
- **Online**: A green checkmark indicates an active access point. A grey X indicates that the access point is inactive.
- **SSID**: The wireless service set identifier (SSID) or network name for the wireless interface.
- **MAC Address**: The MAC address of the Wireless interface.
- **Signal Strength/Noise**: The signal strength and noise level.
- **Channel**: The wireless radio channel that the access point uses.
- **Rate**: The data rate of the access point.
- **First Seen**: The data and time when the FortiWifi unit first detected the access point.
- **Last Seen**: The data and time when the FortiWifi unit last detected the access point.

---

**Column Settings**

Select the columns to display in the list. You can also determine the order in which they appear. For more information, see "Using column settings to control the columns displayed" on page 26.

**Clear All Filters**

Clear any column display filters you might have applied.

**Filter icons**

Edit the column filters to filter or sort the endpoints list according to the criteria you specify. For example, you could add a filter to the Detected Software column to display all endpoints running BitTorrent software. For more information, see "Adding filters to web-based manager lists" on page 24.

**Information columns**

Actual columns displayed depends on Column Settings.

- **Association Time**: How long the client has been connected to this access point.
- **Bandwidth Rx**: Received bandwidth used by the client, in Kbps.
- **Bandwidth Tx**: Transmit bandwidth used by the client, in Kbps.
- **Bandwidth Tx/Rx**: \( \text{Bandwidth Rx} + \text{Bandwidth Tx} \).
- **Idle Time**: The total time this session that the client was idle.
- **IP**: The IP address assigned to the wireless client.
- **MAC**: The MAC address of the wireless client.
- **Physical AP**: The name of the physical access point with which the client is associated.
- **Signal Strength/Noise**: The signal-to-noise ratio in deciBels calculated from signal strength and noise level.
- **Virtual AP**: The name of the virtual access point with which the client is associated.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as ‘Accepted AP’</td>
<td>Select the icon to move this entry to the Accepted Access Points list.</td>
</tr>
<tr>
<td>Mark as ‘Rogue AP’</td>
<td>Select the icon to move this entry to the Rogue Access Points list.</td>
</tr>
<tr>
<td>Forget AP</td>
<td>Return item to Unknown Access Points list from Accepted Access Points list</td>
</tr>
<tr>
<td></td>
<td>or Rogue Access Points list.</td>
</tr>
</tbody>
</table>
Log&Report

This section introduces you to the Log&Report menu. If you require more information about the features within the Log&Report menu, see the FortiOS Handbook.

The following topics are included in this section:

- Log&Report overview
- How a FortiGate unit stores logs
- Event Log
- Alert E-mail
- Accessing and viewing log messages
- Archived logs
- Quarantine
- Reports

Note: If the unit is in transparent mode, certain settings and options for logging may not be available because certain features do not support logging, or are not available in transparent mode. For example, SSL VPN events are not available in transparent mode.

Log&Report overview

The Log&Report menu provides users with configuration settings for either remote or local logging setup, as well as a central location for viewing all types of log messages that are recorded by the unit.

From this menu, you can also configure an alert email message. An alert email message is a message that is sent to an email address that notifies the recipient of a specific activity that occurred, such as an administrator logging out, or when an intrusion is detected. An alert email message can also notify you how many days before your FortiGuard license expires.

The Log&Report menu also provides configuration settings for reports. A report is a collection of log information, which is then displayed in the report in the form of text, graphs and tables. This provides a clear, concise overview of the activities on your network, without manually going through large amounts of log messages.

You can also configure SQL reports, if you have an SQL database and are sending your log files to the SQL database. SQL reports display their information in widgets in Log&Report > Report Access > Executive Summary. These report widgets are similar to the widgets available on the Dashboard page, but are not customizable. They display the collected log information as either a bar or pie chart.

The Log&Report menu allows users to view quarantined files and archives. Quarantine file details are available on Log&Report > Quarantine Files, and these details provide valuable information about why the file is suspicious. You can also filter the files to customize what you are viewing on the Quarantine Files page.
There are two types of archives: DLP and IPS. DLP archives are archived logs containing information about DLP logs, such as email and instant messaging. IPS archives are historical IPS packet logs that administrators can analyze packets for forensics and false positive detection. The archive feature is available on a FortiAnalyzer unit or the FortiGuard Analysis server if subscribed to the FortiGuard Analysis and Management service.

How a FortiGate unit stores logs

The type and frequency of log messages you intend to save determines the type of log storage to use. For example, if you want to log traffic and content logs, you need to configure the 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 do not have a FortiAnalyzer unit and want to create reports.

This topic contains the following:

- Remote logging to a FortiAnalyzer unit
- Remote logging to the FortiGuard Analysis and Management Service
- Remote logging to a syslog server
- Local logging to memory
- Local logging to disk

Remote logging to a FortiAnalyzer unit

FortiAnalyzer units are network devices that provide integrated log collection, analysis tools and data storage. Detailed log reports provide historical as well as current analysis of network activity to help identify security issues and reduce network misuse and abuse.

You can configure the FortiGate unit to log up to three FortiAnalyzer units. The FortiGate unit sends logs to all three FortiAnalyzer units. Each FortiAnalyzer unit stores the same information. Logging to multiple FortiAnalyzer units provides real-time backup protection in the event one of the FortiAnalyzer units fails. Configuring multiple FortiAnalyzer units is available only in the CLI.

The FortiAnalyzer unit needs to be configured to receive logs from the FortiGate unit after you have configured log settings on the FortiGate unit. Contact a FortiAnalyzer administrator to complete the configuration.

Remote Logging & Archiving section of the Log Settings page

<table>
<thead>
<tr>
<th>FortiAnalyzer</th>
<th>Enables the FortiAnalyzer configuration settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The internal IP address of the FortiAnalyzer unit that you want to log to. Enter the IP address of the FortiAnalyzer unit in the field. When the IP address is entered, the Test Connectivity becomes available for testing the connection between the FortiAnalyzer unit and the FortiGate unit.</td>
</tr>
</tbody>
</table>
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. During testing, the FortiGate unit displays information about specific settings for transmitting and receiving logs, reports, DLP archive and quarantine files.

The FortiGate unit must learn the IP address of the FortiAnalyzer unit before testing the connection. A false test report failure may result if testing the connection occurs before the FortiGate unit learns the IP address of the FortiAnalyzer unit.

You can test the connection status between the FortiGate unit and the FortiAnalyzer unit from the CLI using the following command syntax:

```
execute log fortianalyzer test-connectivity
```

The command displays the connection status and the amount of disk usage in percent.

<table>
<thead>
<tr>
<th>Test Connectivity</th>
<th>Tests the connection between the two units. This is disabled until the IP address is entered in the IP address field. Select Test Connectivity to verify both units are successfully connected.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> The test connectivity feature also provides a warning when a FortiGate unit requires a higher-end FortiAnalyzer unit or when the maximum number of VDOMs/FortiGate units has been reached on the FortiAnalyzer unit.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Minimum log level</th>
<th>The minimum log level that logs will be logged at.</th>
</tr>
</thead>
</table>

**Note:** You can specify the source IP address of self-originated traffic when configuring a FortiAnalyzer unit for logging; however, this is available only in the CLI.
Remote logging to the FortiGuard Analysis and Management Service

You can configure logging to a FortiGuard Analysis server after registering for the FortiGuard Analysis and Management Service on the Fortinet support web site. Fortinet recommends verifying that the connection is working properly before configuring logging to a FortiGuard Analysis server.

Remote logging to the FortiGuard Analysis server is similar to logging to a FortiAnalyzer unit because you can also enable archive logging. You can also use widgets to drill-down through information that was gathered from logs.

Logging to a FortiGuard Analysis server is configured in Log&Report > Log Config > Log Settings.

Remote 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 system, such as Linux, Unix, and Intel-based Windows can run syslog software.

When configuring logging to a syslog server, you need to configure the facility and the log file format, which is either normal or Comma Separated Values (CSV). The CSV format contains commas whereas the normal format contains spaces. Logs saved in the CSV file format can be viewed in a spread-sheet application, while logs saved in normal format are viewed in a text editor (such as Notepad) because they are saved as plain text files.

Configuring a facility easily identifies the device that recorded the log file. You can choose from many different facility identifiers, such as daemon or local7.

If you are configuring multiple Syslog servers, configuration is available only in the CLI. You can also enable the reliable delivery option for Syslog log messages in the CLI.

From the CLI, you can enable reliable delivery of syslog messages using the reliable option of the config log {syslog | syslog2 | syslog3} settings command. The FortiGate unit implements the RAW profile of RFC 3195 for reliable delivery of log messages. Reliable syslog protects log information through authentication and data encryption and ensures that the log messages are reliably delivered in the correct order. This feature is disabled by default.

Remote Logging & Archiving section of the Log Settings page

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/FQDN</td>
<td>The IP address or fully qualified domain name of the syslog server. For example, the FQDN could be log.example.com.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number for communication with the syslog server, typically port 514.</td>
</tr>
<tr>
<td>Minimum log level</td>
<td>The unit logs all messages at and above the logging severity level you select.</td>
</tr>
<tr>
<td>Facility</td>
<td>Facility indicates to the syslog server the source of a log message. By default, the unit reports Facility as local7. You may want to change Facility to distinguish log messages from different units.</td>
</tr>
<tr>
<td>Enable CSV Format</td>
<td>If you enable CSV format, the 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 appear on the Log Settings page. You can configure multiple syslog servers in the CLI using the config log {syslog | syslog2 | syslog3} settings CLI command.

Note: You can specify the source IP address of self-originated traffic when configuring a Syslog server; however, this is available only in the CLI.
**Local logging to memory**

The FortiGate system memory has a limited capacity for log messages. The FortiGate system memory displays only the most recent log entries. It can store traffic and content logs in system memory. When the system memory is full, the unit overwrites the oldest messages. All log entries are cleared when the unit restarts.

<table>
<thead>
<tr>
<th>Local Logging &amp; Archiving section of the Log Settings page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Memory</strong></td>
</tr>
<tr>
<td>Stores logs on the unit's system memory.</td>
</tr>
<tr>
<td><strong>Minimum log level</strong></td>
</tr>
<tr>
<td>The unit logs all messages at and above the logging severity level you select.</td>
</tr>
<tr>
<td><strong>Enable IPS Packet Archive</strong></td>
</tr>
<tr>
<td>Enables archiving of IPS packet logs. Select to archive the IPS Packet logs.</td>
</tr>
</tbody>
</table>

**Local logging to disk**

If your unit contains a hard disk you can configure logging to disk. You can specify the minimum log level and how the unit handles local logging if the hard disk becomes full.

For local logs, the SQL log storage format is the default for all log types except content archiving and traffic logs. This is the only format from which you can generate reports. Archiving logs is not available in SQL format. You can enable SQL format logging for traffic logs, but this can cause some loss of logs because SQL format writing is slower than the compressed format.

Log rolling settings are configured in the CLI.

<table>
<thead>
<tr>
<th>Local Logging &amp; Archiving section of the Log Settings page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disk</strong></td>
</tr>
<tr>
<td>Stores local logs on the unit’s hard disk.</td>
</tr>
<tr>
<td><strong>Minimum log level</strong></td>
</tr>
<tr>
<td>The unit logs all messages at and above the logging severity level you select.</td>
</tr>
<tr>
<td><strong>When log disk is full</strong></td>
</tr>
<tr>
<td>The unit will take the specified action, either to overwrite the oldest logs or stop logging altogether, when the disk is at the maximum capacity of storage space for logs. Select one of the following:</td>
</tr>
<tr>
<td>• Overwrite oldest logs – overwrites the oldest log message to continue logging.</td>
</tr>
<tr>
<td>• Stop logging – stops all logging when the disk is full.</td>
</tr>
<tr>
<td><strong>Enable SQL Logging</strong></td>
</tr>
<tr>
<td>If you have an SQL database configured on your unit, you can enable this feature to store logs on the SQL database. Select the logs that you want to send to the SQL database. Note: When you log to the SQL database, you can collect the log information and put that information into a report widget on Log&amp;Report &gt; Report &gt; Executive Summary.</td>
</tr>
</tbody>
</table>

**Local archiving**

You can archive DLP and IPS packet logs to a FortiAnalyzer unit, local hard disk if applicable, and FortiGuard Analysis and Management Services if you have a subscription to it. Archiving is the historical storage of logs which can be accessed at any time, regardless of how old they are. Archived logs are located in Log&Report > Archive Access.
Enabling archiving of these logs is configured within their own configuration. For example, when configuring a DLP rules or compound rules in a sensor, there is the Archive options within that rule to choose which type of archiving to have, either Full or Summary. The type of archiving is important since full archiving archives all information within the log message, which allows for email attachments if archiving emails, and summary archiving archives only the basic information.

When archiving to a local disk, you can configure options for rolling archives; however, configuring these options are only available in the CLI and on the following FortiGate units:

- new generation HDD
- ASM-S08 or ASM-SAS
- FMC or FSM module storage

The CLI command syntax for archiving to a hard disk is:

```
cfg log disk filter
   set dlp-archive {enable | disable}
end
```

## Event Log

In the Event Log menu, you can enable what type of events that you want logged. These event logs are viewed from Log&Report > Log Config > Event Log.

### Event Log page

Lists all the events that you can enable logging for. This list varies depending on the unit. This list also varies depending on the type of mode the unit is in.

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Activity event</td>
<td>All system-related events, such as ping server failure and gateway status.</td>
</tr>
<tr>
<td>IPSec negotiation event</td>
<td>All IPSec negotiation events, such as progress and error reports.</td>
</tr>
<tr>
<td>Admin event</td>
<td>All administration events, such as user logins, resets, and configuration updates.</td>
</tr>
<tr>
<td>HA activity event</td>
<td>All high availability events, such as link, member and state information.</td>
</tr>
<tr>
<td>Firewall authentication event</td>
<td>All firewall-related events, such as user authentication.</td>
</tr>
<tr>
<td>Pattern update event</td>
<td>All pattern update events, such as antivirus and IPS pattern updates and update failures.</td>
</tr>
<tr>
<td>Wireless activity event</td>
<td>All wireless controller activity.</td>
</tr>
<tr>
<td>CPU &amp; memory usage (every 5 minutes)</td>
<td>All real-time CPU and memory events at five minute intervals.</td>
</tr>
<tr>
<td>VoIP event</td>
<td>All VoIP activity, such as SIP and SCCP violations.</td>
</tr>
<tr>
<td>NAC Quarantine event</td>
<td>All endpoint activity that have quarantined hosts when Endpoint NAC is checking hosts.</td>
</tr>
<tr>
<td>Wireless activity event</td>
<td>All wireless controller activities, such as Rogue AP.</td>
</tr>
<tr>
<td>AMC interface bypass mode event</td>
<td>All AMC interface bypass mode events that occur.</td>
</tr>
<tr>
<td>SSL VPN user authentication event</td>
<td>All user authentication events for an SSL VPN connection, such as logging in and out, and timeout due to inactivity.</td>
</tr>
<tr>
<td>SSL VPN administration event</td>
<td>All administration events related to SSL VPN, such as SSL configuration and CA certificate loading and removal.</td>
</tr>
<tr>
<td>SSL VPN session event</td>
<td>All session activity, such as application launches and blocks, timeouts, and verifications.</td>
</tr>
</tbody>
</table>
Alert E-mail

You can use the Alert E-mail feature to monitor logs for log messages, and to send email notification about a specific activity or event logged. For example, if you require notification about administrators logging in and out, you can configure an alert email that is sent whenever an administrator logs in and out.

You can also base alert email messages on the severity levels of the logs. These alert email messages are sent only when the specified severity level was reached.

Alert emails are configured in Log&Report > Log Config > Alert E-mail.

**Alert E-mail page**

Provides settings for configuring the type of alert email notification you want sent.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>The name/address of the SMTP email server.</td>
</tr>
<tr>
<td>Email from</td>
<td>The email address the alert messages will come from.</td>
</tr>
<tr>
<td>Email to</td>
<td>Enter up to three email address recipients for the alert email message.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select the authentication Enable check box to enable SMTP authentication.</td>
</tr>
<tr>
<td>SMTP user</td>
<td>Enter the user name for logging on to the SMTP server to send alert email messages. You need to do this only if you have enabled the SMTP authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for logging on to the SMTP server to send alert email. You need to do this only if you selected SMTP authentication.</td>
</tr>
<tr>
<td>Send alert email for the following</td>
<td>Select to have the alert email sent for one or multiple events that occur, such as an administrator logging in and out.</td>
</tr>
<tr>
<td>Interval Time</td>
<td>Enter the minimum time interval between consecutive alert emails. Use this to rate-limit the volume of alert emails.</td>
</tr>
<tr>
<td>Intrusion detected</td>
<td>Select if you require an alert email message based on attempted intrusion detection.</td>
</tr>
<tr>
<td>Virus detected</td>
<td>Select if you require an alert email message based on virus detection.</td>
</tr>
<tr>
<td>Web access blocked</td>
<td>Select if you require an alert email message based on blocked web sites that were accessed.</td>
</tr>
<tr>
<td>HA status changes</td>
<td>Select if you require an alert email message based on HA status changes.</td>
</tr>
<tr>
<td>Violation traffic detected</td>
<td>Select if you require an alert email message based on violated traffic that is detected by the FortiGate unit.</td>
</tr>
<tr>
<td>Firewall authentication failure</td>
<td>Select if you require an alert email message based on firewall authentication failures.</td>
</tr>
<tr>
<td>SSL VPN login failure</td>
<td>Select if you require an alert email message based on any SSL VPN logins that failed.</td>
</tr>
<tr>
<td>Administrator login/logout</td>
<td>Select if you require an alert email message based on whether administrators log in or out.</td>
</tr>
<tr>
<td>IPSec tunnel errors</td>
<td>Select if you require an alert email message based on whether there is an error in the IPSec tunnel configuration.</td>
</tr>
<tr>
<td>L2TP/PPTP/PPPoE errors</td>
<td>Select if you require an alert email message based on errors that occurred in L2TP, PPTP, or PPPoE.</td>
</tr>
</tbody>
</table>
Accessing and viewing log messages

The Log Access menu provides submenus for viewing logs according to the log type, such as Log&Report > Log Access > DLP.

When viewing log information, you can select a row and view that log message’s information within a table, which appears on the side of the page. Within this table, you can clearly see each field that is in that particular log message. This table is available only when viewing logs in Format.

The columns that appear reflect the fields that are found in the log file. These columns can be removed to view only certain information. You can also use the filter icons to view specific information as well. Log messages can also be viewed in Formatted or Raw. In Formatted view, you can customize the columns, or filter log messages. In Raw view, the log message appears 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 may want to display only event log messages that have a severity level of alert.

The following appears on the Archive Access and Log Access pages when viewing each log type’s log messages

<table>
<thead>
<tr>
<th>Configuration changes</th>
<th>Select if you require an alert email message based on any changes made to the FortiGate configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGuard license expiry time (1-100 days)</td>
<td>Enter the number of days before the FortiGuard license expiry time notification is sent. For more information, see the Knowledge Base article FortiGuard license is expired log messages.</td>
</tr>
<tr>
<td>FortiGuard log quota usage</td>
<td>Select if you require an alert email message based on the FortiGuard Analysis server log disk quota getting full.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>Select if you require an alert email when the internal hard disk or AMC disk reaches a disk usage level. You can set the disk usage level at which the alert email is sent.</td>
</tr>
<tr>
<td>Send alert email for logs based on severity</td>
<td>Select if you want to send an alert email that is based on a specified log severity, such as warning.</td>
</tr>
<tr>
<td>Minimum log level</td>
<td>Select a log severity from the list.</td>
</tr>
</tbody>
</table>

Note: You can specify the source IP address of self-originated traffic for an alert email message, however, this is available only in the CLI.
Archived logs

You can view many archive log types including DLP archives or IPS Packet archives from the unit. Archives are historical logs that are stored on a log device that supports archiving, such as the FortiAnalyzer unit.

These logs are accessed from Log\&Report > Archive Access. If you subscribed to the FortiGuard Analysis and Management Service, you can also view log archives from there as well.

The DLP Archive menu is only visible if:

- You have configured the FortiGate unit for remote logging and archiving to a FortiAnalyzer unit. See "Remote logging to a FortiAnalyzer unit" on page 364.
- You have subscribed to the FortiGuard Analysis and Management Service. See the FortiGuard Analysis and Management Service Administration Guide.

The following submenus are available when you are viewing DLP archives for one of these protocols.

- **E-mail** to view POP3, IMAP, SMTP, POP3S, IMAPS, SMTPS, and spam email archives.
- **Web** to view HTTP and HTTPS archives.
- **FTP** to view FTP archives.
- **IM** to view AIM, ICQ, MSN, and Yahoo! archives.
- **VoIP** to view session control (SIP, SIMPLE and SCCP) archives.
- **IPS Packet** logs that were archived are also available.

If you need to view log archives in Raw format, select Raw beside Formatted.

### Quarantine

Within the Log Access menu, you can view detailed information about each quarantined file. The information can either be sorted or filtered, depending on what you want to view.

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.

On Log\&Report > Archive Access > Quarantine, the file quarantine list displays the following information about each quarantined file.

**Raw or Formatted**

By default, log messages are displayed in Formatted mode. Select Formatted to view log messages in Raw mode, without columns. When in Raw mode, select Formatted to switch back to viewing log messages organized in columns.

When log messages are displayed in Formatted view, you can customize the columns, or filter log messages.

**Clear All Filters**

Clear all filter settings.

**Note:** The FortiAnalyzer unit must be running firmware version 3.0 or higher to view logs from the FortiGate unit.
Quarantine page

Lists all files that are considered quarantined by the FortiGate unit. On this page you can filter information so that only specific files are displayed on the page.

Source

Either FortiAnalyzer or Local disk, depending where you configure to quarantined files to be stored.

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 either Status (infected, blocked, or heuristics) or Service (IMAP, POP3, SMTP, FTP, HTTP, IM, or NNTP), Select Apply to complete the filtering. Heuristics mode is configurable through the CLI only.

If your FortiGate unit supports SSL content scanning and inspection Service can also be IMAPS, POP3S, SMTPS, or HTTPS. For more information, see the UTM chapter of the FortiOS Handbook.

Apply

Select to apply the sorting and filtering selections to the list of quarantined files.

Delete

Select to delete the selected files.

Page Controls

Use the controls to page through the list. For more information, see “Using page controls on web-based manager lists” on page 25.

Remove All Entries

Removes all quarantined files from the local hard disk.

File Name

The file name of the quarantined file.

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 duplicates are quarantined.

Service

The service from which the file was quarantined (HTTP, FTP, IMAP, POP3, SMTP, IM, NNTP, IMAPS, POP3S, SMTPS, or HTTPS).

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.

Upload status

Y indicates the file has been uploaded to Fortinet for analysis, N indicates the file has not been uploaded.

This option is available only if the FortiGate unit has a local hard disk.

Download

Select to download the corresponding file in its original format.

This option is available only if the FortiGate unit has a local hard disk.

Submit

Select to upload a suspicious file to Fortinet for analysis.

This option is available only if the FortiGate unit has a local hard disk.

Note: Duplicates of files (based on the checksum) are not stored, only counted. The TTL value and the duplicate count are updated each time a duplicate of a file is found.

Reports

Reports provide an easy way to analyze and view the information from logs. A report is a collection of log information, which is then displayed in the report in the form of text, graphs and tables. You can configure the following reports:

• FortiOS reports – provides configuration of a report schedule as well as cloned report
Executive Summary reports – widgets that display collected log information from the SQL database; limited configuration settings

FortiAnalyzer report schedules – provides configuration of a report schedule that is generated on a FortiAnalyzer unit but viewed on either a Fortigate unit or FortiAnalyzer unit.

FortiOS reports are available only on units that contain local hard drives. You also require enabling the following in the CLI so that the Report menu appears in the web-based manager:

```
cfg log fortianalyzer setting
  set gui-display enable
end
```

This topic contains the following:

- FortiOS reports
- Executive Summary reports from SQL logs
- FortiAnalyzer report schedules

**Note:** If you are currently running FortiOS 4.0 MR2, basic traffic reports in Log&Report > Report Access > Memory are no longer available.

**FortiOS reports**

FortiOS reports are configured from logs stored on the unit's hard drive and generated by the unit as well. This provides a central location to create and store reports generated from logs files, since previously this feature was only available on FortiAnalyzer units.

FortiOS reports are configured in Log&Report > Report Config.

**Note:** FortiOS reports are available only on FortiGate units with local hard drives. If upgrading from FortiOS 4.0 MR1 or earlier, FortiAnalyzer reports will only be available on the FortiAnalyzer unit and no configuration settings for FortiAnalyzer reports is supported in FortiOS 4.0 MR2.

You need to enable the report menus before you can configure reports. Report Config and Report Access are enabled in the CLI. The following is the command syntax you need to use to enable Report Config and Report Access menus in the web-based manager.

```
cfg log fortianalyzer setting
  set gui-display enable
end
```

This topic contains the following:

- Themes
- Layouts
- Charts
- Images
- Viewing generated FortiOS reports

**Themes**

A theme allows you to configure how the information displays on the page, as well as the type of font, page orientation, and if there will be multiple columns.

If you want, you can apply the two default themes that are available in the Add Report Layout page.
To configure a theme for a report, log in to the CLI and then enter the following commands.

```
config report theme
edit <theme_name>
  set column-count [ 1 | 2 | 3]
  set default-html-style <string>
  set default-pdf-style <string>
  set graph-chart-style <string>
  set heading1-style <string>
  set heading2-style <string>
  set heading3-style <string>
  set heading4-style <string>
  set hline-style <string>
  set image-style
  set normal-text-style
  set page-footer-style
  set page-header-style
  set page-orient {landscape | portrait}
  set page-style
  set report-subtitle-style
  set report-title-style
  set table-chart-caption-style
  set table-chart-even-row-style
  set table-chart-head-style
  set table-chart-odd-row-style
  set table-chart-style
  set toc-heading1-style
  set toc-heading2-style
  set toc-heading3-style
  set toc-heading4-style
  set toc-title-style
end
```

**Layouts**

A report layout, similar to the layout that you must configure for a FortiAnalyzer report, contains settings for including charts, sections, adding images and scheduling when the layout will be generated.

The Report Components section on the Add Report Layout page provides a place where you can view what charts, sections, and images you have chosen for that report. This section also allows you to move the parts, such as charts, to where you want them in the report.

A report layout is configured in Log&Report > Report Config > Layout. Use the following table when configuring a report’s layout.

<table>
<thead>
<tr>
<th>Layout page</th>
<th>Lists all the report layouts that you configured, as well as default layouts. On this page, you can edit, delete, clone a report, or create a new report.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new layout for a report. When you select Create New, you are automatically redirected to the Add Report Layout page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies a report layout’s settings. When you select Edit, you are automatically redirected to the Edit Report Layout page.</td>
</tr>
</tbody>
</table>
Delete
Removes a layout from within the list on the Layout page.
To remove multiple layouts from within the list, on the Layout page, in each
of the rows of the layouts you want removed, select the check box and then
select Delete.
To remove all layouts from the list, on the Layout page, select the check box
in the check box column, and then select Delete.
Clone
Use to base a new report layout on an existing one.
Run
Immediately generates a report.
Report Layout
The name of the report layout.
Title
The name of the title that appears on the generated report.
Format
The type of format that the report is in, either PDF or HTML.
Schedule
The time that the report is generated on.
Description
A description about the report.

Add Report Layout page
Provides settings for configuring a report layout.

Name
Enter a name of the report layout. This is not the name that will be the
report’s title.
Report Theme
Select a theme from the drop-down list.
Description
Enter a description, if you want, to explain what the report is about. This
does not appear within the report.
Output Format
The type of format the report will be generated in. You can choose PDF to
have the report generated as a PDF.
Schedule
Select what type of schedule you want the report generated on. The type of
schedule can be on a daily basis, weekly, on demand (whenever you want),
or only once.
If you select On Demand, the report can be generated whenever you want it.
If you select Once, the report is generated as soon as the report is saved.
Title
Enter a name for the title of the report.
Sub Title
Enter a name that will be the sub title of the report.
Option
Select to include all or some of the following report options:
• Table of Contents – includes a table of contents in the report
• Auto Heading Number – automatically provides a heading number for
each heading, in numerical format.
• HTML navigation bar – provides a navigational bar to help you navigate
in report whose format is HTML
• Chart Name as Heading – allows for a chart’s name to be the heading

Add Component page
Text
Select the type of format the heading will have. For example, if you select
Heading 1, the headings will be in the Heading 1 format.
When you select Normal, you will be providing a comment for a section
within the report.
Chart
Select a category from the Categories drop-down list. Each category
contains different charts that are specific to that category.
Image
Select an image to include within the report.
Misc
Select a page break, column break, or horizontal line to include in the report.
Charts

There are default charts available when configuring a report layout; however, you can configure your own charts for report layouts that you can create for report layouts. When configuring charts, you must also configure datasets because they are used to gather specific data from the SQL database. You should configure the datasets you need for a report layout first, and then configure chart.

You must have prior knowledge about SQL before configuring datasets because datasets require SQL statements. Datasets are configured only in the CLI.

A chart is configured in Log&Report > Report Config > Chart. Use the following table when configuring your own chart, or modifying a default chart.

<table>
<thead>
<tr>
<th>Chart page</th>
<th>Lists all the charts, both default and the ones that you created. On this page, you can edit, delete and create new charts.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new chart that is a graph or table. When creating a new chart, you must select the down arrow to reveal the type of chart you want to create, Graph Chart or Table Chart. After selecting the type of chart you want to create, you are redirected to that type's page. For example, Add Graph Report Chart.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies a chart's settings. You can modify any of the default charts. When you select Edit, you are automatically redirected to the Edit Report Layout page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a chart from within the list on the Layout page. You can only remove charts that you created. To remove multiple charts from within the list, on the Chart page, in each of the rows of the charts you want removed, select the check box and then select Delete.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the chart.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of information that will display within the chart. For example, a bar chart displays attack log information in the Attacks_February chart.</td>
</tr>
<tr>
<td>Dataset</td>
<td>The dataset that will be used for the chart.</td>
</tr>
<tr>
<td>Comments</td>
<td>The description about the chart.</td>
</tr>
</tbody>
</table>

Add Graph Report Chart page

Provides settings for configuring charts for report layouts.

| Name       | Enter a name for the chart. |
| Dataset    | Select a configured dataset for the chart. |
| Category   | Select a log category for the chart. |
| Comments   | Enter a comment to describe the chart. This is optional. |
| Graph Type | Select the type of graph that will display the information within the chart. If you select Pie, only Category Series and Value Series appears. |
| Category Series | Enter the fields for the category in the Databind field. The databind is a combination of the fields derived from the SQL statement or named fields in the CLI. For example, field(3). |
| Value Series | Enter the fields for the value in the Databind field. The databind is a combination of the fields derived from the SQL statement or named fields in the CLI. For example, field(3). |
| X-series   | The settings for the x axis of the line, bar or flow chart. |
| Databind   | Enter an SQL databind value expression for binding data to the series being configured. For example, field(3). |
| Category Axis | Select to have the axis show the type of log category. The default is no log category will appear on the axis. |
| Scale      | Sets the type of format to display the date and time on the x axis. |
Images
You can import an image to use for a report. The image formats that are supported are JPEG, JPG and PNG.

Images are imported in Log&Report > Report Config > Image. Use the following table when importing an image.

### Image page
Lists all the images that you have imported. On this page, you can delete an image, import an image from your local PC, or view an image.

#### Delete
Removes an image from the list on the page. You can only remove images that you created.
To remove multiple images from within the list, on the Image page, in each of the rows of the images you want removed, select the check box and then select Delete.

#### Import
Import an image from your local PC.

#### View
Displays the image. When you select View, you are automatically redirected to the View Image page where the image displays. Select Return to go back to the Image page.

#### Image Name
The file name of the image.

#### Thumbnail
A thumbnail image of the actual image you imported.

### Import Image File page
Provides settings for importing images.

#### File to Import
Enter the location of the image on the local PC or select Browse to locate the image file. Select OK to start importing the image file.

Viewing generated FortiOS reports
After creating a report layout, you can go to the Report Access > Disk to view your generated report. When you choose to generate a report only once, the report is generated right away.

### Disk page
Lists all the reports that are generated by the unit. You can also remove reports from the list.

#### Delete
Removes a report from the list on the Disk page.
To remove multiple reports from within the list, on the Disk page, in each of the rows of the reports you want removed, select the check box and then select Delete.
To remove all reports from the list, on the Disk page, select the check box in the check box column, and then select Delete.

#### Report File
The report name that the FortiGate unit gave the report. This name is in the format <scheduletype>-<report_title>-<yyyy-mm-dd>-<start_time>. For example, Once-examplereport_1-2010-02-12-083054, which indicates that the report titled examplereport_1 was scheduled to generate only once and did on February 12, 2010 at 8:30 am. The hour format is in hh:mm:ss format.
Executive Summary reports from SQL logs

On units that contain a hard drive, you can display Executive Summary reports based on logs stored in an SQL database. The log messages are stored in text format in the database.

There are many default reports that you can select and customize in the web-based manager. You can customize reports by selecting the report update schedule and location in the Executive Summary.

Executive summary reports are configured in Log&Report > Report Access > Executive Summary.

FortiAnalyzer report schedules

FortiAnalyzer report schedules are available only when a FortiAnalyzer unit is configured for logging purposes. A report layout is required before configuring a report schedule, so contact a FortiAnalyzer administrator before configuring report schedules from the FortiGate unit to verify that the appropriate report layout is configured. Report layouts can only be configured from the FortiAnalyzer unit.

You need to enable the report menus before configuring reports. Report Config and Report Access are enabled in the CLI. The following is the command syntax you need to use to enable Report Config and Report Access menus in the web-based manager.

```
cfg log fortianalyzer setting
  set gui-display enable
end
```

FortiAnalyzer report schedules are configured in Log&Report > Report Config > FortiAnalyzer. Use the following table when configuring a FortiAnalyzer report schedule.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Started</td>
<td>The time when the report began generating. The format is in yyyy-mm-dd hh:mm:ss.</td>
</tr>
<tr>
<td>Finished</td>
<td>The time when the report finished generating. The format is in yyyy-mm-dd hh:mm:ss.</td>
</tr>
<tr>
<td>Size</td>
<td>The size of the report after it was generated. The size is in bytes.</td>
</tr>
<tr>
<td>Other Formats</td>
<td>The other type of format you choose the report to be in, for example, PDF. When you select PDF in this column, the PDF opens up within the Disk page. You can save the PDF to your local PC when it is opened on the Disk page as well.</td>
</tr>
</tbody>
</table>

FortiAnalyzer page

Lists all report schedules that you created. On this page, you can edit, delete or create a new report schedule.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new report schedule. When you select Create New, you are automatically redirected to the Schedule page.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the report schedule.</td>
</tr>
<tr>
<td>Description</td>
<td>The comment made when the report schedule was created.</td>
</tr>
<tr>
<td>Report Layout</td>
<td>The name of the report layout used for the report schedule.</td>
</tr>
<tr>
<td>Schedule</td>
<td>When the report schedule will be generated. The time depends on what time period was selected when the report schedule was created: once, daily, or specified days of the week. For example, if you select monthly, the days of the month and time (hh:mm) will appear in the format Monthly 2, 10, 21, 12:00.</td>
</tr>
</tbody>
</table>
Delete
Removes a schedule from the list on the FortiAnalyzer page.
To remove multiple schedules from within the list, on the FortiAnalyzer page, in each of the rows of the schedules you want removed, select the check box and then select Delete.
To remove all schedules from the list, on the FortiAnalyzer page, select the check box in the check box column, and then select Delete.

Edit
Modifies settings within a schedule. When you select Edit, you are automatically redirected to the Edit Schedule page.

Clone
Creates a duplicate of the report schedule and use it as a basis for a new report schedule.

Create Schedule Settings page
Provides settings for configuring a report schedule. You require a report layout when configuring a report schedule.

Name
Enter a name for the schedule.

Description
Enter a description for the schedule. This is optional.

Report Layout
Select a configured report layout from the list. You must apply a report layout to a report schedule. For more information, see the FortiAnalyzer Administration Guide.

Language
Select the language you want used in the report schedule from the list.

Schedule
Select one of the following to have the report generate once only, daily, weekly, or monthly at a specified date or time period.

Once
Select to have the report generated only once.

Daily
Select to generate the report every date at the same time, and then enter the hour and minute time period for the report. The format is hh:mm.

These Days
Select to generate the report on specified days of the week, and then select the days of the week check boxes.

These Dates
Select to generate the report on a specific day or days of the month, and then enter the days with a comma to separate them. For example, if you want to generate the report on the first day, the 21st day and 30th day, enter: 1, 21, 30.

Log Data Filtering
You can specify the following variables for the report:

Virtual Domain
Select to create a report based on virtual domains. Enter a specific virtual domain to include in the report.

User
Select to create a report based on a network user. Enter the user or users in the field, separated by spaces. If a name or group name contains a space, it should be specified between quotes, for example, "user 1".

Group
Select to create a report based on a group of network users, defined locally. Enter the name of the group or groups in the field.

LDAP Query
Select the LDAP Query check box and then select an LDAP directory or Windows Active Directory group from the list.

Time Period
Select to include the time period of the logs to include in the report.

Relative to Report Runtime
Select a time period from the list. For example, this year.

Specify
Select to specify the date, day, year and time for the report to run.

- From – Select the beginning date and time of the log time range.
- To – Select the ending date and time of the log time range.

Output
Select the format you want the report to be in and if you want to apply an output template.
Output Types
Select the type of file format for the generated report. You can choose from PDF, MS Word, Text, and MHT.

Email/Upload
Select the check box if you want to apply a report output template from the list. This list is empty if a report output template does not exist. For more information, see the FortiAnalyzer Administration Guide.

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.
Index

Symbols

_email, 17
_fqdn, 17
_index, 17
_int, 17
_ipv4, 17
_ipv4/mask, 17
_ipv4mask, 17
_ipv6, 17
_ipv6mask, 17
_name, 17
_pattern, 17
_str, 17
_v4mask, 17
_v6mask, 17

Numerics

802.3ad aggregate interface
creating, 64

A
accept action
firewall policy, 342
access profile, See admin profile, 119
action
firewall policy, 205
active sessions
HA statistics, 96
adding, configuring or defining
  administrative access to interface, 68
  administrator password, 115
  administrator settings, 121
  authentication settings, 323
  BFD, 198
  CA certificates, 128
  cipher suite, 312
  custom signatures, 257
  DHCP interface settings, 65
  DHCP relay agent, 90
  Directory Service server, 331
  Directory Service user groups, 326
  Dynamic DNS on an interface, 67
  firewall policy, 205, 229, 230
  firewall policy, modem connections, 78
  firewall schedule, 226
  firewall user groups, 325
  firmware version, 40
  FortiAnalyzer report schedules, 378
  FortiWiFi-50B settings, 130, 132
  FortiWiFi-60B settings, 130, 132
  gateway for default route, 176
  HA, 92
  HA device priority, 96
  HA subordinate unit host name, 96
  health check monitor, 238
  IPSec encryption policy, 210
  IPSec VPN phase 1, 300
  IPSec VPN phase 1 advanced options, 302
  IPSec VPN phase 2, 304
  IPSec VPN phase 2 advanced options, 304
  LDAP authentication, 117
  LDAP server, 329
  license key, 152
  logging to a FortiAnalyzer unit, 364
  logging to a FortiGuard Analysis server, 366
  logging to a Syslog server, 366
  logging to memory, 367
  modem connections, firewall policy, 78
  modem interface, 75
  MTU size, 70
  network options, 79
  OSPF areas, 192
  OSPF basic settings, 190
  OSPF interface, operating parameters, 194
  OSPF networks, 193
  OSPF settings, advanced, 191
  override server, 146
  password, 117
  password, administrator, 115
  PKI authentication, 118
  PPPoE or PPPoA interface settings, 66
  push updates, 148
  RADIUS authentication, 117
  redundant interface, 65
  redundant mode, 77
  RIP settings, advanced, 188
  RIP-enabled interface, 189
  scripts, 151
  secondary IP address, 71
  SNMP community, 97, 98
  SSL VPN options, firewall policy, 210
  SSL VPN settings, 312
  SSL VPN user groups, 326
  standalone mode, 78
  static route, adding to routing table, 177
  system administrators, 114
  system certificates, 126
  system configuration backup and restore, 138
  system configuration backup and restore, FortiManager, 139
  system configuration, central management options, 139
  system time, 39
  TACACS+ authentication, 118
  TACACS+ server, 331
  updates for FDN and FortiGuard services, 141
  URL filter list, 265, 267
  user authentication settings, 323
  user groups, 324
  VDOM configuration settings, advanced, 156
  VDOM configuration settings, global, 156
  virtual IP, 231
  virtual IPSec interface, 68
  VPN firewall policy-based internet browsing, 308
  VPN route-based internet browsing, 308
  wireless interface, 132
  zone, 74

address
  firewall address group, 219
  list, 218
address group, 219
  adding, 219
  creating new, 219
  list, 219
Address Name
  firewall address, 218
admin
  administrator account, 28
  admin profile
    administrator account, 119
  viewing list, 119
administrative access
  changing, 29
  interface settings, 62, 72
  monitoring logins, 40
administrative interface. See web-based manager
administrator account
  admin, 28
  admin profile, 119
  netmask, 117
administrator login
  disclaimer, 107
administrator password
  changing, 28
administrator settings, 121
administrators
  viewing list, 115
administrators, monitoring, 40
Advanced Mezzanine Card (AMC), 44
AFS3, advanced file security encrypted file
  AFS3, 220
agent
  sFlow, 73
aggregate interface
  creating, 64
AH, predefined service, 220
alert email, 369
  options, 369
  SMTP user, 369
alert message console
  viewing, 45
allow inbound
  IPSec firewall policy, 210
allow outbound
  IPSec firewall policy, 210
AMC module, 60
antispam
  port 53, 144
  port 8888, 144
antispam. See also Email filter, 272
antivirus
  quarantine files list, 371
  virus list, 247
antivirus and attack definitions, 145
antivirus updates, 146
  manual, 42
  through a proxy server, 147
ANY
  service, 220
AOL
  service, 220
application control, 291
area border router (ABR), 193
ARP, 231
  proxy ARP, 231
attack updates
  manual, 42
  scheduling, 146
  through a proxy server, 147
Authentication
  IPSec VPN, phase 2, 305
authentication
  client certificates and SSL VPN, 312
  defining settings, 323
  MD5, 193
  RIP, 189
  server certificate and SSL VPN, 312
Authentication Algorithm
  IPSec VPN, manual key, 307, 308
Authentication Key
  IPSec VPN, manual key, 308
Authentication Method
  IPSec VPN, phase 1, 301
Auto Key
  IPSec VPN, 300
Autokey Keep Alive
  IPSec VPN, phase 2, 305
autonomous system (AS), 195

B
back to HA monitor
  HA statistics, 95
backing up
  3.0 config to FortiUSB, 163
  3.0 configuration, 161
  config using web-based manager, 3.0, 162
backup (redundant) mode
  modem, 75
backup and restore, system maintenance, 138
backup mode
  modem, 77
band
  wireless setting, 131
bandwidth
  guaranteed, 229
  maximum, 229, 337, 340
banned word
  character set, 265
banned word (email filter)
  catalog, 275
banned word (spam filter)
  list, 276
banned word list catalog
  viewing, 275
beacon interval
  wireless setting, 131
BFD
  disabling, 199
BGP
  AS, 195
  RFC 1771, 195
  service, 220
blackhole routing, 64
C
CA certificates
  importing, 128
  viewing, 128
catalog
  banned word, 275
  content filter, 261
  IP address black/white list, 276
central management, 120
Certificate Name
  IPSec VPN, phase 1, 301
certificate, security. See system certificate
certificate, server, 312
certificate. See system certificates
channel
  wireless setting, 131
color set
  converting, 265
  DLP, 265
  email filter, 265
  web filtering, 265
CIDR, 17
cipher suite
  SSL VPN, 312
CLI, 21
  connecting to from the web-based manager, 30
CLI configuration
  using in web-based manager, 48
  web category block, 271
CLI console, 48
client certificates
  SSL VPN, 312
client comforting, 264
cluster member, 94
  cluster members list, 95
  priority, 95
  role, 95
cluster unit
  disconnecting from a cluster, 96
collector
  sFlow, 73
column settings
  configuring, 26
  using with filters, 27
comforting
  client, 264
command line interface (CLI), 14
comments
  firewall policy, 209
comments, documentation, 19
concentrator
  IPSec tunnel mode, 309
  IPSec VPN, policy-based, 309
Concentrator Name
  IPSec VPN, concentrator, 309
configuring
  WAN optimization peer, 340
  WAN optimization rule, 337
connecting
  modem, dialup account, 79
  conserve mode, 45
contact information
  SNMP, 98
contacting customer support, 30
content archiving
  DLP archiving, 291
content block
  catalog, 261
content filtering
  character set, 265
content streams
  replacement messages, 99
CPU usage
  HA statistics, 96
CRL (Certificate Revocation List)
  viewing, 129
custom service
  list, 224
customer service, 18
customer support
  contacting, 30
CVSPSERVER, concurrent versions system proxy server, 220

D
data encryption
  wireless setting, 133
data leak protection, 282
date
  quarantine files list, 372
daylight saving changes, 39
DC
  quarantine files list, 372
DCE-RPC
  firewall service, 220
default
  password, 14
default gateway, 175
default route, 175
destination
  firewall policy, 205, 206, 209, 211
destination IP address
  system status, 50
device priority
  HA, 93
  subordinate unit, 96
DH Group
  IPSec VPN, phase 2, 305
DHCP
  and IP Pools, 207
  configuring relay agent, 90
  servers and relays, 89
  service, 90
  system, 89
  transparent mode, 89
  viewing address leases, 92
DHCP (Dynamic Host Configuration Protocol)
  configuring on an interface, 65
  service, 221
DHCP6
  service, 221
DHCP-IPSec
  IPSec VPN, phase 2, 305
diagnose
  commands, 30
dialup VPN
  monitor, 309
Directory Service
  configuring server, 331
disclaimer
  administrator login, 107
disconnecting
  modem, dialup account, 79
DLP
  archiving, 291
  character set, 265
  content archiving, 291
DLP archive
  viewing, 47
DLP archiving, 291
DLP, See data leak protection
DNS
  service, 221
  split, 80, 83
documentation
  commenting on, 19
  Fortinet, 18
DoS policy
  viewing, 213
dotted decimal, 17
dotted-decimal notation, 192
downgrading. See also reverting
  3.0 using the CLI, 169
  3.0 using web-based manager, 168
download
quarantine files list, 372
duplicates
quarantine files list, 372
Dynamic DNS
IPSec VPN, phase 1, 301
monitor, 309
network interface, 67
VPN IPSec monitor, 309
dynamic resources
VDOM resource limits, 158
dynamic routing, 186
OSPF, 189
PIM, 196
E
email alert, 369
e-mail filter, 272
Perl regular expressions, 279
Enable perfect forward secrecy (PFS)
IPSec VPN, phase 2, 305
Enable replay detection
IPSec VPN, phase 2, 305
enable session pickup
HA, 93
Encryption
IPSec VPN, phase 2, 305
Encryption Algorithm
IPSec VPN, manual key, 307, 308
Encryption Key
IPSec VPN, manual key, 308
end IP
IP pool, 234
enhanced reliability, 92
equal-cost multi-path (ECMP), 177
ESP
service, 221
exclude range
adding to DHCP server, 91
expire
system status, 50
expired
subscription, 143
explicit mode
WAN optimization, 339
explicit web proxy
FTP, 85
HTTPS, 85
PAC, 85
proxy auto-config, 85
SOCKS, 85
UTM, 86
exported server certificates
importing, 126
external interface
virtual IP, 232
external IP address
virtual IP, 232
external service port
virtual IP, 232
F
FDN
attack updates, 113
HTTPS, 145
override server, 143
port 443, 145
port 53, 144
port 8888, 144
port forwarding connection, 148
proxy server, 147
push update, 143
troubleshooting connectivity, 145
updating antivirus and attack definitions, 145
FDS, 140
file block
default list of patterns, 244
file name
quarantine files list, 372
filter
filtering information on web-based manager lists, 24
quarantine files list, 372
using with column settings, 27
web-based manager lists, 24
FINGER
service, 221
firewall, 226
address list, 218
configuring, schedule, 226
custom service list, 224
one-time schedule, 227
overview, firewall schedule, 226
predefined services, 220
recurring schedule, 226
virtual IP list, 231
firewall address
address group, 219
address name, 218
create new, 218
IP range/subnet, 218
list, 218
name, 218
subnet, 218
firewall address group
adding, 219
available addresses, 219
group name, 219
members, 220
firewall IP pool list, 233
firewall policy
  accept action, 342
  action, 205
  allow inbound, 210
  allow outbound, 210
  comments, 209
  creating new, 205, 229, 230
  destination, 205, 206, 209, 211
  guaranteed bandwidth, 229
  ID, 205
  inbound NAT, 210
  insert policy before, 206, 338
  log traffic, 208, 210
  maximum bandwidth, 229, 337, 340
  modem, 78
  outbound NAT, 210
  schedule, 205, 207
  service, 205, 207
  source, 205, 206, 211
  SSL VPN options, 210
  traffic priority, 337, 340
  traffic shaping, 208, 209
  user groups, 325
Index

firewall service
AFS3, 220
AH, 220
ANY, 220
AOL, 220
BGP, 220
CVSPSERVER, 220
dcE-RPC, 220
DHCP, 221
DHCP6, 221
DNS, 221
esP, 221
fINGER, 221
ftp, 221
Ftp_GET, 221
FTP_PUT, 221
gopher, 221
GRE, 221
H323, 221
HTTP, 221
HTTPS, 221
ICMP_ANY, 221
IKE, 221
IMAP, 221
INFO_ADDRESS, 221
INFO_REQUEST, 221
Internet-Locator-Service, 222
IRC, 222
L2TP, 222
LDAP, 222
MGCP, 222
MS-SQL, 222
MYSQL, 222
NetMeeting, 222
NFS, 222
NNTP, 222
NTP, 222
OCN-RPC, 222
OSPF, 222
PC-Anywhere, 222
PING, 222
PING6, 222
POP3, 222
PPTP, 222
QUAKE, 223
RAUDIO, 223
REXEC, 223
RIP, 223
RLOGIN, 223
RSH, 223
RTSP, 223
SAMBA, 223
SCCP, 223
SIP, 223
SIP-MSN, 223
SMTP, 223
SNMP, 223
SOCKS, 224
SQUID, 224
SSH, 224
SYSLOG, 224
TALK, 224
cTP, 224
tELNET, 224
tFTP, 224
tIMESTAMP, 224
UDP, 224
UUCP, 224
VDOLIVE, 224
viewing custom service list, 224
viewing list, 220
VNC, 224
WAIS, 224
WINFRAME, 224
WINS, 224
x-WINDOWS, 224
FortiAnalyzer, 13
configuring report schedules, 378
logging to, 364
FortiBridge, 13
FortiClient, 13
system maintenance, 136
FortiGate documentation
commenting on, 19
FortiGate SNMP event, 99
FortiGate-ASM-FB4, 60
FortiGuard, 13
Antispam, 14
Antivirus, 14
changing the host name, 271
CLI configuration, 271
manually configuring definition updates, 42
FortiGuard Distribution Network. See FDN
FortiGuard Distribution Server. See FDS
FortiGuard Intrusion Prevention System (IPS), 41
FortiGuard Management Services
remote management options, 139
FortiGuard Services, 140
antispam service, 141
configuring antispam service, 141
configuring updates for FDN and services, 141
configuring web filter service, 141
FortiGuard Management and Analysis Services, 141
licenses, 41, 141
management and analysis service options, 144
support contract, 142
web filtering, 141
web filtering and antispam options, 144
FortiMail, 13
FortiManager, 13
Fortinet customer service, 18
Fortinet documentation, 18
Fortinet Family Products, 13
Fortinet Knowledge Center, 19
Fortinet product
registering, 30
FortiWiFi-50B
wireless settings, 130
FortiWiFi-60B
wireless settings, 130
fragmentation threshold
wireless setting, 133
FTP
explicit web proxy, 85
service, 221
FTP_GET
  service, 221
FTP_PUT
  service, 221
fully qualified domain name (FQDN), 17

G
  geography
    wireless setting, 131
GOPHER
  service, 221
graphical user interface. See web-based manager
grayware
  updating antivirus and attack definitions, 145
GRE, 189
  service, 221
group name
  HA, 93
groups
  user, 324
guaranteed bandwidth
  traffic shaping, 229
guargraphic user interface. See web-based manager
HA, 92, 95
  changing cluster unit host names, 95
  cluster member, 95
  cluster members list, 94
  configuring, 92
  device priority, 93
  disconnecting a cluster unit, 96
  enable session pickup, 93
  group name, 93
  hash map, 94
  heartbeat interface, 94
  host name, 95
  interface monitoring, 94
  mode, 93
  password, 93
  port monitor, 94
  router monitor, 199
  routes, 199
  session pickup, 93
  subordinate unit device priority, 96
  subordinate unit host name, 96
  VDOM partitioning, 93, 94
  viewing HA statistics, 95

HA statistics
  active sessions, 96
  back to HA monitor, 95
  CPU usage, 96
  intrusion detected, 96
  memory usage, 96
  monitor, 95
  network utilization, 96
  refresh every, 95
  status, 95
  total bytes, 96
  total packets, 96
  unit, 95
  up time, 95
  virus detected, 96
HA virtual clustering, 93
  health check monitor
    configuring, 238
  heartbeat, HA
    interface, 94
  help
    navigating using keyboard shortcuts, 33
  searching the online help, 32
  using FortiGate online help, 30
  high availability (HA), 92
  high availability See HA, 92
  host name
    changing, 39
    changing for a cluster, 95
    viewing, 39
  hostname
    cluster members list, 95
HTTP
  service, 221
HTTPS, 21, 114
  explicit web proxy, 85
  service, 221

I
  ICMP_ANY
    service, 221
ID
  firewall policy, 205
idle timeout
  changing for the web-based manager, 29
  idssignaturecustom_newedit, 257
IEEE 802.3ad, 64
IKE
  service, 221
IMAP
  service, 221
inbound NAT
  IPSec firewall policy, 210
index number, 17
INFO_ADDRESS
  service, 221
INFO_REQUEST
  service, 221
insert policy before
  firewall policy, 206, 338
installation, 14
interface
  administrative access, 62, 72
  administrative status, 60
  configuring administrative access, 68
  GRE, 189
  loopback, 59
  modem, configuring, 75
  MTU, 62
  proxy ARP, 231
  wireless, 130
  WLAN, 130
Interface Mode, 64
interface monitoring, 94
  HA, 94
internet browsing
  IPSec VPN configuration, 308
Internet-Locator-Service
  service, 222
introduction
  Fortinet documentation, 18
intrusion detected
  HA statistics, 96
intrusion protection
  signatures, 256
IP
  virtual IP, 231
IP address
  antispam black/white list catalog, 276
  IPSec VPN, phase 1, 301
IP address, configuring secondary, 71
IP pool
  creating new, 233
  DHCP, 207
  end IP, 234
  IP range/subnet, 234
  list, 233
  name, 234
  PPPoE, 207
  proxy ARP, 231
  start IP, 233
IP range/subnet
  firewall address, 218
  IP pool, 234
IPS
  see intrusion protection
IPSec, 189
IPSec firewall policy
  allow inbound, 210
  allow outbound, 210
  inbound NAT, 210
  outbound NAT, 210
IPSec Interface Mode
  IPSec VPN, manual key, 308
IPSec VPN
  adding manual key, 307
  Auto Key list, 300
  concentrator list, 309
  configuring phase 1, 300
  configuring phase 1 advanced options, 302
  configuring phase 2, 304
  configuring phase 2 advanced options, 304
  configuring policy-, route-based Internet browsing, 308
  Manual Key list, 306
  monitor list, 309
IPv6, 175
IPv6 support
  settings, 122
IRC
  service, 222
K
  key
    license, 152
    wireless setting, 132
  keyboard shortcut
    online help, 33
Keylife
  IPSec VPN, phase 2, 305
L
L2TP
  service, 222
language
  changing the web-based manager language, 29
  web-based manager, 29, 122
LDAP
  configuring server, 329
  service, 222
LDAP server
  configuring authentication, 117
license key, 152
licenses
  viewing, 41
limit
  VDOM resources, 158
lists
  using web-based manager, 23
local certificates
  options, 125
  viewing, 124
Local Interface
  IPSec VPN, manual key, 308
  IPSec VPN, phase 1, 301
Local SPI
  IPSec VPN, manual key, 307
local user, 321
log
  raw or formatted, 371
  traffic, firewall policy, 208
  log traffic
    firewall policy, 210
logging
  alert email, configuring, 369
  configuring FortiAnalyzer report schedules, 378
  FortiGuard Analysis server, 366
  storing logs, 364
  testing FortiAnalyzer configuration, 365
to a FortiAnalyzer unit, 364
to memory, 367
to syslog server, 366
  viewing raw or formatted logs, 371
logging out
  web-based manager, 30
loopback interface, 59
lost password
  recovering, 29, 116, 117

M
  MAC address
    filtering, 133
  MAC filter
    wireless, 133
  Management Information Base (MIB), 97
  Manual Key
    IPSec VPN, 306
  map to IP
    virtual IP, 232
  map to port
    virtual IP, 232
  matched content, 239
  maximum bandwidth, 229, 337, 340
  firewall policy, 229, 337, 340
  traffic shaping, 229, 337, 340
MD5
  OSPF authentication, 193, 194
Members
  IPSec VPN, concentrator, 309
memory usage
  HA statistics, 96
menu
  web-based manager menu, 23
MGCP
  service, 222
Mode
  IPSec VPN, phase 1, 301
mode
  HA, 93
  operation, 14
modem
  adding firewall policies, 78
  backup mode, 77
  connecting and disconnecting to dialup account, 79
  redundant (backup) mode, 75
  standalone mode, 75, 78
  viewing status, 79
modem interface
  configuring, 75
monitor
  administrator logins, 40
  HA statistics, 95
  IPSec VPN, 309
  routing, 199
monitoring
  WAN optimization, 341
MS-SQL
  service, 222
MTU size, 62, 70
multicast, 196
multicast destination NAT, 198
MySQL
  service, 222

N
  Name
    IP pool, 234
    IPSec VPN, manual key, 307
    IPSec VPN, phase 1, 301
    IPSec VPN, phase 2, 304
NAT
  inbound, IPSec firewall policy, 210
  multicast, 198
  outbound, IPSec firewall policy, 210
  push update, 148
netmask
  administrator account, 117
NetMeeting
  service, 222
network
  configuring options, 79
  Network Time Protocol, 39
  network utilization
    HA statistics, 96
NFS
  service, 222
NNTP
  service, 222
  not registered
    subscription, 143
notification, 369
Not-so-stubby Area (NSSA), 192
not-so-stubby area (NSSA), 200
Novel edirectory, 331
NTP, 39
  service, 222
  sync interval, 39
  synchronizing with an NTP server, 39

O
  OFTP connection, 44
ONC-RPC
  service, 222
one-time schedule
  adding, 227
  creating new, 227
  list, 227
  start, 228
  stop, 228
online help
  content pane, 31
  keyboard shortcuts, 33
  navigation pane, 32
  search, 32
  using FortiGate online help, 30
operation mode, 14, 113
wireless setting, 131
operational history
viewing, 45
OSPF
area ID, 193
AS, 191
authentication, 193, 194
Dead Interval, 195
dead packets, 195
GRE, 194
Hello Interval, 195
interface definition, 194
IPSec, 194
LSA, 194
multiple interface parameter sets, 194
network, 191
network address space, 194
NSSA, 192, 200
regular area, 192
service, 222
settings, 190
stub, 192
virtual lan, 194
virtual link, 193
VLAN, 194
OSPF AS
defining, 190
outbound NAT
IPSec firewall policy, 210
override server
adding, 146
P
P2 Proposal
IPSec VPN, phase 2, 305
PAC
explicit web proxy, 85
default list of file block patterns, 244
password
administrator, 14
configuring authentication password, 117
HA, 93
recovering lost password, 29, 116, 117
pattern, 17
default list of file block patterns, 244
PC-Anywhere
service, 222
Peer option
IPSec VPN, phase 1, 301
Perl regular expressions
email filter, 279
persistent, 236
Phase, 304
phase 1
IPSec VPN, 300, 304
phase 1 advanced options
IPSec VPN, 302
phase 2
IPSec VPN, 304
phase 2 advanced options
IPSec VPN, 304
PIM
dense mode, 196
RFC 2362, 196
RFC 3973, 196
sparse mode, 196
PING
service, 222
PING6
firewall service, 222
PKI, 333
authentication, 118
policy
accept action, 342
action, 205
allow inbound, 210
allow outbound, 210
comments, 209
creating new, 205, 229, 230
destination, 205
guaranteed bandwidth, 229
ID, 205
inbound NAT, 210
insert policy before, 206, 338
log traffic, 208, 210
maximum bandwidth, 229, 337, 340
outbound NAT, 210
schedule, 205, 207
service, 205, 207
source, 205
SSL VPN options, 210
traffic priority, 337, 340
traffic shaping, 208, 209
policy-based routing, 183
POP3
service, 222
port 53, 144
port 8888, 144
port 9443, 148
port monitor
HA, 94
port monitoring, 94
PPPoE
service, 222
and IP Pools, 207
PPPoE (Point-to-Point Protocol over Ethernet)
RFC 2516, 66
PPTP
service, 222
predefined services, 220
predefined signature
default action, 257
Pre-shared Key
IPSec VPN, phase 1, 301
pre-shared key
wireless setting, 133
priority
cluster members, 95
private key
importing, 126, 127
product registration, 30
products, family, 13
proposal
  IPSec VPN, phase 2, 305

protocol
  service, 220
  system status, 50
  virtual IP, 232

Protocol Independent Multicast (PIM), 196

proxy ARP, 231
  FortiGate interface, 231
  IP pool, 231
  virtual IP, 231

proxy auto-config
  explicit web proxy, 85

proxy server, 147
  push updates, 147

push update, 143
  configuring, 147
  external IP address changes, 147
  IP address changes, 147
  management IP address changes, 148
  through a proxy server, 147

QUAKE
  service, 223

quarantine files list
  antivirus, 371
  apply, 372
  date, 372
  DC, 372
  download, 372
  duplicates, 372
  file name, 372
  filter, 372
  service, 372
  sorting, 372
  status, 372
  status description, 372
  TTL, 372
  upload status, 372

R

RADIUS
  servers, 327
  viewing server list, 327
  WPA Radius, 133

RADIUS server
  authentication, 117
  wireless setting, 133

RAUDIO
  service, 223
  read & write access level
    administrator account, 39, 40, 115
  read only access level
    administrator account, 39, 40, 115, 117
  real servers
    configuring, 237
    monitoring, 240

recurring schedule
  adding, 226
  creating new, 227
  list, 226
  select, 227
  start, 227
  stop, 227

redundant interface
  adding system settings, 65

redundant mode
  configuring, 77

refresh every
  HA statistics, 95

registering
  Fortinet product, 30
  regular administrator, 114

regular expression, 17

relay
  DHCP, 89, 90

reliable
  delivery of syslog messages, 366

remote administration, 68, 114

remote certificates
  options, 127
  viewing, 127

Remote Gateway
  IPSec manual key setting, 307
  IPSec VPN, manual key, 307
  IPSec VPN, phase 1, 301

remote peer
  manual key configuration, 307

Remote SPI
  IPSec VPN, manual key, 307

remote user authentication, 327

replacement messages, 99

report
  configuring report schedules, 378

resource limits
  dynamic resources, 158
  static resources, 158
  VDOM, 158

resource usage
  VDOM, 159

restoring 3.0 configuration, 171
  using the CLI, 171
  using web-based manager, 171

Reverse Path Forwarding (RPF), 198

REEXEC
  firewall service, 223

RFC 1321, 193
RFC 1771, 195
RFC 2362, 196
RFC 2385, 195
RFC 2516, 66
RFC 3973, 196
RFC 5237, 184

RIP
  authentication, 189
  service, 223
  split horizon, 189
RLOGIN
  service, 223
role
  cluster members, 95
route
  HA, 199
route flapping, 181
router monitor
  HA, 199
routing
  configuring, 88
  monitor, 199
  static, 173
routing policy
  protocol number, 184
routing table, 199
  searching, 200
RSH
  firewall service, 223
RTS threshold
  wireless setting, 133
RTSP
  firewall service, 223

S
SAMBA
  service, 223
SCCP
  firewall service, 223

schedule
  antivirus and attack definition updates, 146
  firewall policy, 205, 207
  one-time schedule list, 227
  organizing schedules into groups, 228
  recurring schedule list, 226
schedule group
  adding, 228
scheduled updates
  through a proxy server, 147
screen resolution
  minimum recommended, 21
search
  online help, 32
  online help wildcard, 32
searching
  routing table, 200
Secure Copy (SCP), 123
security
  MAC address filtering, 133
  security certificates. See system certificates
security mode
  wireless setting, 132
select
  recurring schedule, 227
separate server certificates
  importing, 127
server
  DHCP, 89
  server certificate, 312
  server certificates
  importing, 126, 127
Index

service
AH, 220
ANY, 220
AOL, 220
BGP, 220
custom service list, 224
CVSPSERVER, 220
DCE-RPC, 220
DHCP, 90, 221
DHCP6, 221
DNS, 221
ESP, 221
FINGER, 221
firewall policy, 205, 207
FTP, 221
FTP_GET, 221
FTP_PUT, 221
GOPHER, 221
GRE, 221
H323, 221
HTTPS, 221
ICMP_ANY, 221
IKE, 221
IMAP, 221
INFO_ADDRESS, 221
INFO_REQUEST, 221
Internet-Locator-Service, 222
IRC, 222
L2TP, 222
LDAP, 222
MGCP, 222
MS-SQL, 222
MYSQL, 222
NetMeeting, 222
NFS, 222
NNTP, 222
NTP, 222
ONC-RPC, 222
OSPF, 222
PC-Anywhere, 222
PING, 222
PING6, 222
POP3, 222
PPTP, 222
predefined, 220
QUAKE, 223
quarantine files list, 372
RAUDIO, 223
REXEC, 223
RIP, 223
RLOGIN, 223
RSH, 223
RTSP, 223
SAMBA, 223
SCCP, 223
service name, 220
SIP, 223
SIP-MSNMessenger, 223
SMTP, 223
SNMP, 223
SOCKS, 224
SQUID, 224
SSH, 224
SYSLOG, 224
TELNET, 224
TFTP, 224
TIMESTAMP, 224
UDP, 224
UUCP, 224
VDOLIVE, 224
VNC, 224
WAIS, 224
WINFRAME, 224
WINS, 224
X-WINDOWS, 224
service group
create new, 226
service port
virtual IP, 231
session list
viewing, 50
session pickup
HA, 93
set time
time
set the time, 39
settings, 132
administrators, 121
IPv6 support, 122
timeout, 122
sFlow, 73
agent, 73
collector, 73
multiple VDOMs, 74
SIP
service, 223
SIP-MSNMessenger
service, 223
SMTP
service, 223
user, 369
SMTPS, 107
sniffer policy
viewing, 216
SNMP
configuring community, 97
contact information, 98
event, 99
manager, 97
queries, 99
service, 223
traps, 99
v3, 97
SNMP Agent, 98
SNMP communities, 98
SOCKS
explicit web proxy, 85
service, 224
sorting
quarantine files list, 372
source
firewall policy, 205, 206, 211
source IP address
system status, 50
source IP port
  system status, 50
spam filter
  banned word list, 276
spam filter, see email filter, 272
split DNS, 80, 83
split-DNS, 80, 83
SQUID
  service, 224
SSH, 114
  service, 224
SSID
  wireless setting, 132
SSID broadcast
  wireless setting, 132
SSL
  service definition, 221, 222
SSL VPN
  checking client certificates, 312
  configuring settings, 312
  firewall policy, 210
  setting the cipher suite, 312
  specifying server certificate, 312
  specifying timeout values, 313
  web-only mode, 310
SSL VPN Client Certificate, 210
SSL VPN login message, 112
SSL VPN web portal, 313
standalone mode
  modem, 75, 78
start
  IP pool, 233
  one-time schedule, 228
  recurring schedule, 227
static default route, 175
static IP
  monitor, 309
static resources
  VDOM resource limits, 158
static route
  adding, 177
  creating, 173
  default gateway, 175
  default route, 175
  editing, 173
  overview, 173
  policy, 183
  policy list, 184
  viewing, 173
statistics
  viewing HA statistics, 95
status
  HA statistics, 95
  interface, 60
  quarantine files list, 372
status description
  quarantine files list, 372
stop
  one-time schedule, 228
  recurring schedule, 227
string, 17
stub
  OSPF area, 192
subnet
  firewall address, 218
subscription
  expired, 143
  not registered, 143
  valid license, 143
super administrator, 114
switch mode, 63
sync interval
  NTP, 39
synchronize
  with NTP Server, 39
SYSLOG
  service, 224
syslog
  reliable, 366
system administrators, 114
system certificate
  FortiGate unit self-signed security certificate, 28
system certificates
  CA, 128
  CRL, 129
  importing, 126
  requesting, 125
  viewing, 124
system configuration, 92
system DHCP see also DHCP, 89
system idle timeout, 114
system information
  viewing, 37
system maintenance
  backup and restore, 138
  creating scripts, 151
  enabling push updates, 147
  push update through a NAT device, 148
  remote FortiManager options, 139
  remote management options, 139
  updating antivirus and attack definitions, 145
  uploading scripts, 151
  VDOM, 136
system resources
  viewing, 44
system time
  configuring, 39
system wireless. See wireless

T
TACACS+
  configuring server, 331
TACACS+ server
  authentication, 118
TALK
  service, 224
TCP
  service, 224
technical support, 18
TELNET
  service, 224
<table>
<thead>
<tr>
<th><strong>Index</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TFTP</strong> <strong>service</strong>, 224</td>
</tr>
<tr>
<td><strong>time</strong> configuring, 39</td>
</tr>
<tr>
<td><strong>timeout</strong> settings, 122</td>
</tr>
<tr>
<td><strong>timeout values</strong> specifying for SSL VPN, 313</td>
</tr>
<tr>
<td><strong>TIMESTAMP</strong> <strong>service</strong>, 224</td>
</tr>
<tr>
<td><strong>top attacks</strong> viewing, 51</td>
</tr>
<tr>
<td><strong>top sessions</strong> viewing, 49</td>
</tr>
<tr>
<td><strong>top viruses</strong> viewing, 51</td>
</tr>
<tr>
<td><strong>total bytes</strong> HA statistics, 96</td>
</tr>
<tr>
<td><strong>total packets</strong> HA statistics, 96</td>
</tr>
<tr>
<td><strong>traffic history</strong> viewing, 51</td>
</tr>
<tr>
<td><strong>Traffic Priority</strong>, 337, 340</td>
</tr>
<tr>
<td><strong>traffic priority</strong> firewall policy, 337, 340</td>
</tr>
<tr>
<td><strong>traffic shaping</strong> firewall policy, 208, 209</td>
</tr>
<tr>
<td><strong>maximum bandwidth</strong>, 229</td>
</tr>
<tr>
<td><strong>traffic priority</strong>, 337, 340</td>
</tr>
<tr>
<td><strong>transparent mode</strong> WAN optimization, 339</td>
</tr>
<tr>
<td><strong>troubleshooting</strong> FDN connectivity, 145</td>
</tr>
<tr>
<td><strong>trusted host</strong> administrators options, 117</td>
</tr>
<tr>
<td><strong>security issues</strong>, 119</td>
</tr>
<tr>
<td><strong>TTL</strong> quarantine files list, 372</td>
</tr>
<tr>
<td><strong>tunnel mode</strong> SSL VPN, SSL VPN tunnel mode, 310</td>
</tr>
<tr>
<td><strong>Tunnel Name</strong> IPSec VPN, manual key, 307</td>
</tr>
<tr>
<td><strong>Tx Power</strong> wireless setting, 131</td>
</tr>
<tr>
<td><strong>type</strong> virtual IP, 232</td>
</tr>
<tr>
<td><strong>U</strong> <strong>UDP service</strong>, 224</td>
</tr>
<tr>
<td><strong>unit</strong> HA statistics, 95</td>
</tr>
<tr>
<td><strong>unit operation</strong> viewing, 43</td>
</tr>
<tr>
<td><strong>up time</strong> HA statistics, 95</td>
</tr>
<tr>
<td><strong>update</strong> push, 147</td>
</tr>
<tr>
<td><strong>upgrading</strong> 3.0 using web-based manager, 165</td>
</tr>
<tr>
<td>4.0 using the CLI, 166</td>
</tr>
<tr>
<td>backing up using the CLI, 3.0, 162</td>
</tr>
<tr>
<td>FortiGate unit to 3.0, 165</td>
</tr>
<tr>
<td>using the web-based manager, 165</td>
</tr>
<tr>
<td>using web-based manager, 3.0, 162</td>
</tr>
<tr>
<td><strong>upload status</strong> quarantine files list, 372</td>
</tr>
<tr>
<td><strong>URL</strong> <strong>block</strong> adding a URL to the web filter block list, 265</td>
</tr>
<tr>
<td><strong>web filter</strong>, 265</td>
</tr>
<tr>
<td><strong>URL formats</strong>, 267</td>
</tr>
<tr>
<td><strong>USB</strong> disk, 138</td>
</tr>
<tr>
<td><strong>backup and restore configuration</strong>, 136</td>
</tr>
<tr>
<td><strong>user authentication</strong> PKI, 333</td>
</tr>
<tr>
<td>remote, 327</td>
</tr>
<tr>
<td><strong>user groups</strong> configuring, 324</td>
</tr>
<tr>
<td>Directory Service, 326</td>
</tr>
<tr>
<td>firewall, 325</td>
</tr>
<tr>
<td>SSL VPN, 326</td>
</tr>
<tr>
<td><strong>UTF-8</strong> character set, 265</td>
</tr>
<tr>
<td><strong>UTM</strong> explicit web proxy, 86</td>
</tr>
<tr>
<td>web proxy, 86</td>
</tr>
<tr>
<td><strong>UUCP</strong> service, 224</td>
</tr>
<tr>
<td><strong>valid license</strong>, 143</td>
</tr>
<tr>
<td><strong>value parse error</strong>, 17</td>
</tr>
<tr>
<td><strong>VDOLIVE</strong> <strong>service</strong>, 224</td>
</tr>
<tr>
<td><strong>VDOM</strong> dynamic resource limits, 158</td>
</tr>
<tr>
<td>license key, 152</td>
</tr>
<tr>
<td>resource limits, 158</td>
</tr>
<tr>
<td>resource usage, 159</td>
</tr>
<tr>
<td>static resource limits, 158</td>
</tr>
<tr>
<td>system maintenance, 136</td>
</tr>
<tr>
<td><strong>VDOM partitioning</strong> HA, 94</td>
</tr>
<tr>
<td><strong>verifying</strong> downgrade to 2.80 MR11, 169</td>
</tr>
<tr>
<td>upgrade to 4.0, 167</td>
</tr>
</tbody>
</table>
Index

viewing
  admin profiles list, 119
  administrators, 40
  administrators list, 115
  Alert Message Console, 45
  antispam IP address list catalog, 276
  antivirus list, 247
  antivirus quarantined files list, 371
  banned word list, 276
  banned word list catalog, 275
  CA certificates, 128
  certificates, 124
  cluster members list, 94
  CRL (Certificate Revocation List), 129
  custom service list, firewall service, 224
  DHCP address leases, 92
  DLP archive, 47
  firewall service list, 220
  FortiGuard support contract, 142
  HA statistics, 95
  hostname, 39
  IP pool list, 233
  IPSec VPN auto key list, 300
  IPSec VPN concentrator list, 309
  IPSec VPN manual key list, 306
  IPSec VPN monitor list, 309
  LDAP server list, 329
  licenses, 41
  modem status, 79
  one-time schedule list, 227
  operational history, 45
  RADIUS server list, 327
  recurring schedule list, 226
  remote certificates, 127
  routing information, 199
  session list, 50
  static route, 173
  system information, 37
  system resources, 44
  TACACS+ server, 331
  top attacks, 51
  top sessions, 49
  top viruses, 51
  traffic history, 51
  unit operation, 43
  virtual IP list, 231
  virtual IP pool list, 233
  web content filter list catalog, 261
  wireless monitor, 134
virtual IP, 231
  configuring, 231
  create new, 231, 233
  external interface, 232
  external IP address, 232
  external service port, 232
  IP, 231
  list, 231
  map to IP, 232
  map to port, 232
  protocol, 232
  service port, 231
  type, 232
virtual IPSec
  configuring interface, 68
virtual servers
  configuring, 234
virus detected
  HA statistics, 96
virus list, 247
virus name, 102
virus protection. See antivirus
VLAN
  jumbo frames, 70
  OSPF, 194
VNC
  service, 224
VPN IPSec (see also IPSec VPN), 299
VPN SSL. See SSL VPN
VPN tunnel
  IPSec VPN, firewall policy, 210
VPN, IPSec
  firewall policy, 210
W
WAIS
  service, 224
WAN optimization
  explicit mode, 339
  monitoring, 341
  transparent mode, 339
WAN optimization peer
  configuring, 340
WAN optimization rule
  configuring, 337
web category block
  changing the host name, 271
  CLI configuration, 271
web equivalent privacy, 132
web filter, 259
  adding a URL to the web URL block list, 265
  character set, 265
  configuring the web URL block list, 267
  URL block, 265
  URL category, 144
web filtering service, 102
web portal
  SSL VPN, SSL VPN web portal
customize, 313
web proxy
  UTM, 86
web site, content category, 101
Web UI. See web-based manager
web URL block
  configuring the web URL block list, 267
web_ftgd_quota, 271
web-based manager, 21
changing the language, 29
connecting to the CLI, 30
idle timeout, 29
IPv6 support, 122
language, 29, 122
logging out, 30
online help, 30
pages, 21
screen resolution, 21
using the menu, 23
using web-based manager lists, 23
web-only mode
SSL VPN, 310
WEP, 132
WEP128, 130, 132
WEP64, 130, 132
WiFi protected access, 132
wild cards, 17
wildcard
online help search, 32
Windows Active Directory, 331
WINFRAME
service, 224
WINS
service, 224
wireless
band, 131
beacon interval, 131
channel, 131
configuration, 129
data encryption, 133
fragmentation threshold, 133
geography, 131
interface, 130
key, 132
MAC filter, 133
operation mode, 131
pre-shared key, 133
RADIUS server, 133
RTS threshold, 133
security, 132
security mode, 132
settings FortiWiFi-50B, 130
settings FortiWiFi-60A, 130
settings FortiWiFi-60AM, 130
settings FortiWiFi-60B, 130
SSID, 132
SSID broadcast, 132
Tx power, 131
viewing monitor, 134
WLAN
interface, 130
WLAN interface
adding to a FortiWiFi-50B, 132
adding to a FortiWiFi-60A, 132
adding to a FortiWiFi-60AM, 132
adding to a FortiWiFi-60B, 132
WPA, 130, 132
WPA Radius
wireless security, 133
WPA2, 130, 132
WPA2 Auto, 130, 132
WPA2 Radius
wireless security, 133
X
X.509 security certificates. See system certificates
X-Forwarded-For (XFF), 88
X-WINDOWS
service, 224
Z
zones
configuring, 74