Conserve mode ................................................. 26
The AV proxy ................................................. 26
Entering and exiting conserve mode ....................... 26
Conserve mode effects ........................................ 26
Configuring the av-failopen command ...................... 27
SSL content scanning and inspection ....................... 27
Setting up certificates to avoid client warnings ........... 28
SSL content scanning and inspection settings .......... 29
Viewing and saving logged packets ......................... 31
Configuring packet logging options ....................... 31
Using wildcards and Perl regular expressions ............ 32

Network defense .............................................. 35
Monitoring .................................................... 35
Blocking external probes ................................... 35
  Address sweeps .......................................... 35
  Port scans ................................................. 36
  Probes using IP traffic options ......................... 36
  Evasion techniques ..................................... 38
Defending against DoS attacks ................................ 39
  The “three-way handshake” ............................... 40
  SYN flood ................................................ 40
  SYN spoofing ............................................ 41
  DDoS SYN flood .......................................... 41
  Configuring the SYN threshold to prevent SYN floods 42
  SYN proxy ................................................ 42
  Other flood types ....................................... 43
Traffic inspection ............................................ 43
  IPS signatures .......................................... 43
  Suspicious traffic attributes ............................ 44
  DoS policies .............................................. 44
  Application control ..................................... 44
Content inspection and filtering ........................... 45
  AntiVirus ................................................ 45
  FortiGuard Web Filtering ............................... 45
  Email filter .............................................. 46
  DLP ....................................................... 46
AntiVirus

Antivirus concepts .......................................................... 47
   How antivirus scanning works ...................................... 47
   Antivirus scanning order ............................................. 48
   Antivirus databases .................................................. 50
   Antivirus techniques .................................................. 51
   FortiGuard Antivirus .................................................. 52
Enable antivirus scanning ............................................... 52
   Viewing antivirus database information ......................... 52
   Changing the default antivirus database ....................... 53
   Overriding the default antivirus database ...................... 53
   Adding the antivirus profile to a firewall policy ............... 54
   Configuring the scan buffer size ................................. 54
   Configuring archive scan depth ................................... 55
   Configuring a maximum allowed file size ........................ 55
   Configuring client comforting ...................................... 56
Enable the file quarantine ................................................ 57
   General configuration steps ........................................ 57
   Configuring the file quarantine .................................... 57
   Viewing quarantined files ......................................... 58
   Downloading quarantined files .................................... 58
Enable file filtering ....................................................... 59
   General configuration steps ........................................ 59
   Creating a file filter list ......................................... 59
   Creating a file pattern ............................................. 60
   Creating a file type ............................................... 60
   Enabling file filtering in a profile ............................... 60
Enable grayware scanning ................................................. 61
Testing your antivirus configuration .................................. 61
Antivirus examples ......................................................... 61
   Configuring simple antivirus protection ......................... 62
   Protecting your network against malicious email attachments . 63

Email filter

Email filter concepts .......................................................... 67
   Email filter techniques .............................................. 67
   Order of spam filtering ............................................. 68
Enable email filter. ............................................................... 69
  Enabling FortiGuard IP address checking ............................. 70
  Enabling FortiGuard URL checking .................................... 70
  Enabling FortiGuard email checksum checking ....................... 70
  Enabling FortiGuard spam submission ................................ 71
  Enabling IP address black/white list checking ....................... 71
  Enabling HELO DNS lookup ............................................. 73
  Enabling email address black/white list checking ................... 73
  Enabling return email DNS checking .................................. 74
  Enabling banned word checking ....................................... 75
How content is evaluated. .................................................. 75
  Configure the spam action ............................................. 78
  Configure the tag location ............................................. 78
  Configure the tag format .............................................. 79
Email filter examples ....................................................... 79
  Configuring simple antispam protection ............................. 79
  Blocking email from a user ............................................ 80

Intrusion protection ......................................................... 83
  IPS concepts ..................................................................... 83
    Anomaly-based defense ............................................... 83
    Signature-based defense .............................................. 83
  Enable IPS scanning ..................................................... 85
    General configuration steps ........................................... 85
    Creating an IPS sensor ................................................. 85
    Creating an IPS filter .................................................. 85
    Updating predefined IPS signatures ................................. 86
    Creating an IPS signature override .................................. 86
    Creating a custom IPS signature ..................................... 87
    Custom signature syntax and keywords ............................. 87
  IPS processing in an HA cluster ........................................ 96
    Active-passive ........................................................... 97
    Active-active ........................................................... 97
  Configure IPS options .................................................... 97
    Configuring the IPS engine algorithm ............................... 97
    Configuring the IPS engine-count .................................... 97
    Configuring fail-open .................................................. 98
    Configuring the session count accuracy ............................ 98
    Configuring the IPS buffer size ...................................... 98
    Configuring protocol decoders ...................................... 98
    Configuring security processing modules ......................... 99
  Enable IPS packet logging .............................................. 99
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS examples</td>
<td>100</td>
</tr>
<tr>
<td>Configuring basic IPS protection</td>
<td>100</td>
</tr>
<tr>
<td>Using IPS to protect your web server</td>
<td>101</td>
</tr>
<tr>
<td>Create and test a packet logging IPS sensor</td>
<td>103</td>
</tr>
<tr>
<td>Creating a custom signature to block access to example.com.</td>
<td>105</td>
</tr>
<tr>
<td>Creating a custom signature to block the SMTP “vrfy” command</td>
<td>106</td>
</tr>
<tr>
<td>Configuring a Fortinet Security Processing module</td>
<td>108</td>
</tr>
<tr>
<td>Web filter</td>
<td>113</td>
</tr>
<tr>
<td>Web filter concepts</td>
<td>113</td>
</tr>
<tr>
<td>Different ways of controlling access</td>
<td>115</td>
</tr>
<tr>
<td>Order of web filtering</td>
<td>115</td>
</tr>
<tr>
<td>Web content filter</td>
<td>115</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>116</td>
</tr>
<tr>
<td>Creating a web filter content list</td>
<td>116</td>
</tr>
<tr>
<td>Configuring a web content filter list</td>
<td>116</td>
</tr>
<tr>
<td>How content is evaluated</td>
<td>117</td>
</tr>
<tr>
<td>Enabling the web content filter and setting the content threshold</td>
<td>118</td>
</tr>
<tr>
<td>URL filter</td>
<td>118</td>
</tr>
<tr>
<td>URL filter actions</td>
<td>119</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>121</td>
</tr>
<tr>
<td>Creating a URL filter list</td>
<td>121</td>
</tr>
<tr>
<td>Configuring a URL filter list</td>
<td>122</td>
</tr>
<tr>
<td>SafeSearch</td>
<td>122</td>
</tr>
<tr>
<td>Advanced web filter configuration</td>
<td>123</td>
</tr>
<tr>
<td>ActiveX filter</td>
<td>123</td>
</tr>
<tr>
<td>Cookie filter</td>
<td>123</td>
</tr>
<tr>
<td>Java applet filter</td>
<td>123</td>
</tr>
<tr>
<td>Web resume download block</td>
<td>123</td>
</tr>
<tr>
<td>Block Invalid URLs</td>
<td>123</td>
</tr>
<tr>
<td>HTTP POST action</td>
<td>124</td>
</tr>
<tr>
<td>Web filtering example</td>
<td>124</td>
</tr>
<tr>
<td>School district</td>
<td>124</td>
</tr>
<tr>
<td>FortiGuard Web Filter</td>
<td>129</td>
</tr>
<tr>
<td>Before you begin</td>
<td>129</td>
</tr>
<tr>
<td>FortiGuard Web Filter and your FortiGate unit</td>
<td>130</td>
</tr>
<tr>
<td>Order of web filtering</td>
<td>130</td>
</tr>
</tbody>
</table>
Enable FortiGuard Web Filter ................................. 132
   General configuration steps .............................. 132
   Configuring FortiGuard Web Filter settings .......... 132
   Configuring FortiGuard Web Filter categories ...... 132
   Configuring FortiGuard Web Filter classifications .. 133
   Configuring FortiGuard Web Filter usage quotas ... 134
   Checking quota usage .................................. 136
Advanced FortiGuard Web Filter configuration .......... 136
   Provide Details for Blocked HTTP 4xx and 5xx Errors . 136
   Rate Images by URL (blocked images will be replaced with blanks) .... 136
   Allow Websites When a Rating Error Occurs ......... 136
   Strict Blocking ....................................... 137
   Rate URLs by Domain and IP Address .................. 137
   Block HTTP Redirects by Rating ....................... 137
   Daily log of remaining quota .......................... 137
Add or change FortiGuard Web Filter ratings .......... 137
Create FortiGuard Web Filter overrides ................. 138
   Understanding administrative and user overrides .. 138
Customize categories and ratings ........................ 139
   Creating local categories ............................ 139
   Customizing site ratings .............................. 139
FortiGuard Web Filter examples ........................... 140
   Configuring simple FortiGuard Web Filter protection .... 140
   School district ..................................... 141

Data leak prevention ........................................ 143
Data leak prevention concepts ............................. 143
   DLP sensor ........................................ 143
   DLP rule .......................................... 143
   DLP compound rule ................................ 144
Enable data leak prevention ................................ 145
   General configuration steps ........................... 145
   Creating a DLP rule ................................ 145
   Understanding the default DLP rules. ................. 148
   Creating a compound DLP rule ......................... 149
   Creating a DLP sensor ................................ 149
   Adding rules to a DLP sensor ........................ 150
   Understanding default DLP sensors ................. 152
DLP archiving ............................................. 153
DLP examples ............................................ 154
   Configuring DLP content archiving .................... 154
   Blocking sensitive email messages .................... 154
### Application control

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application control concepts</td>
<td>157</td>
</tr>
<tr>
<td>Enable application control</td>
<td>157</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>158</td>
</tr>
<tr>
<td>Creating an application control list</td>
<td>158</td>
</tr>
<tr>
<td>Adding applications to an application control list</td>
<td>158</td>
</tr>
<tr>
<td>Understanding the default application control lists</td>
<td>160</td>
</tr>
<tr>
<td>Application traffic shaping</td>
<td>160</td>
</tr>
<tr>
<td>Enabling application control traffic shaping</td>
<td>160</td>
</tr>
<tr>
<td>Reverse direction traffic shaping</td>
<td>161</td>
</tr>
<tr>
<td>Shaper re-use</td>
<td>161</td>
</tr>
<tr>
<td>Application control monitor</td>
<td>162</td>
</tr>
<tr>
<td>Enabling application control monitor</td>
<td>162</td>
</tr>
<tr>
<td>Application control packet logging</td>
<td>163</td>
</tr>
<tr>
<td>Application considerations</td>
<td>164</td>
</tr>
<tr>
<td>IM applications</td>
<td>164</td>
</tr>
<tr>
<td>Skype</td>
<td>164</td>
</tr>
<tr>
<td>Application control examples</td>
<td>164</td>
</tr>
<tr>
<td>Blocking all instant messaging</td>
<td>164</td>
</tr>
<tr>
<td>Allowing only software updates</td>
<td>165</td>
</tr>
</tbody>
</table>

### DoS policy

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS policy concepts</td>
<td>167</td>
</tr>
<tr>
<td>Enable DoS</td>
<td>167</td>
</tr>
<tr>
<td>Creating and configuring a DoS sensor</td>
<td>167</td>
</tr>
<tr>
<td>Creating a DoS policy</td>
<td>169</td>
</tr>
<tr>
<td>Apply an IPS sensor to a DoS policy</td>
<td>170</td>
</tr>
<tr>
<td>DoS example</td>
<td>170</td>
</tr>
</tbody>
</table>

### Sniffer policy

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sniffer policy concepts</td>
<td>173</td>
</tr>
<tr>
<td>The sniffer policy list</td>
<td>173</td>
</tr>
<tr>
<td>Before you begin</td>
<td>174</td>
</tr>
<tr>
<td>Enable one-arm sniffer</td>
<td>175</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>175</td>
</tr>
<tr>
<td>Designating a sniffer interface</td>
<td>176</td>
</tr>
<tr>
<td>Creating a sniffer policy</td>
<td>176</td>
</tr>
</tbody>
</table>
Introduction

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

*FortiOS Handbook: UTM* describes the Unified Threat Management (UTM) features available on your FortiGate unit, including antivirus, intrusion prevention system (IPS), anomaly protection (DoS), one-armed IPS (sniffer policies), web filtering, email filtering, data leak prevention, (DLP) and application control. The guide includes step-by-step instructions showing how to configure each feature. Example scenarios are included, with suggested configurations.

Examples include school scenarios using web filtering to protect students from inappropriate content, using IPS and DoS sensors to protect web servers from attack, and using antivirus scanning to protect your network against viruses and malicious file attachments.

This section contains the following topics:

- Before you begin
- How this chapter is organized
- Document conventions
- Entering FortiOS configuration data
- Registering your Fortinet product
- Fortinet products End User License Agreement
- Training
- Documentation
- Customer service and technical support

Before you begin

Before you begin using this guide, take a moment to note the following:

- Administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.
- Firewall policies limit access, and, while this and other similar features are a vital part of securing your network, they are not covered in this guide.
- If your FortiGate unit supports SSL acceleration, it also supports SSL content scanning and inspection for HTTPS, IMAPS, POP3S, and SMTPS traffic.

How this chapter is organized

This FortiOS Handbook chapter contains the following sections:

**UTM overview**: Describes UTM components and their relation to firewall policies, as well as SSL content scanning and inspection. We recommend starting with this section to become familiar with the different features in your FortiGate unit.

**Network defense**: Explains basic denial of service (DoS) and distributed denial of service (DDOS) concepts and provides an overview of the best practices to use with all the UTM features to defend your network against infection and attack.
**AntiVirus:** Explains how the FortiGate unit scans files for viruses and describes how to configure the antivirus options.

**Email filter:** Explains how the FortiGate unit filters email, describes how to configure the filtering options and the action to take with email detected as spam.

**Intrusion protection:** Explains basic Intrusion Protection System (IPS) concepts and how to configure IPS options; includes guidance and a detailed table for creating custom signatures as well as several examples.

**Web filter and FortiGuard Web Filter:** The first of these sections describes basic web filtering concepts, the order in which the FortiGate unit performs web filtering, and configuration. The second section describes enhanced features of the subscription-based FortiGuard Web Filtering service and explains how to configure them. We recommend reading both sections if you are using FortiGuard Web Filtering because settings you configure in one feature may affect the other.

**Data leak prevention:** Describes the DLP features that allow you to prevent sensitive data from leaving your network and explains how to configure the DLP rules, compound rules, and sensors.

**Application control:** Describes how your FortiGate unit can detect and take action against network traffic based on the application generating the traffic.

**DoS policy:** Describes how to use DoS policies to protect your network from DoS attacks.

**Sniffer policy:** Describes how to use your FortiGate unit as a one-armed intrusion detection system (IDS) to report on attacks.
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.

Most of the examples in this document use the following IP addressing:

- IP addresses are made up of A.B.C.D
- A - can be one of 192, 172, or 10 - the non-public addresses covered in RFC 1918.
- B - 168, or the branch / device / virtual device number.
  - Branch number can be 0xx, 1xx, 2xx - 0 is Head office, 1 is remote, 2 is other.
  - Device or virtual device - allows multiple FortiGate units in this address space (VDOMs).
- Devices can be from x01 to x99.
- C - interface - FortiGate units can have up to 40 interfaces, potentially more than one on the same subnet
  - 001 - 099- physical address ports, and non -virtual interfaces
  - 100-255 - VLANs, tunnels, aggregate links, redundant links, vdom-links, etc.
- D - usage based addresses, this part is determined by what device is doing
  - The following gives 16 reserved, 140 users, and 100 servers in the subnet.
  - 001 - 009 - reserved for networking hardware, like routers, gateways, etc.
  - 010 - 099 - DHCP range - users
  - 100 - 109 - FortiGate devices - typically only use 100
  - 110 - 199 - servers in general (see later for details)
  - 200 - 249 - static range - users
  - 250 - 255 - reserved (255 is broadcast, 000 not used)
  - The D segment servers can be farther broken down into:
    - 110 - 119 - Email servers
    - 120 - 129 - Web servers
    - 130 - 139 - Syslog servers
    - 140 - 149 - Authentication (RADIUS, LDAP, TACACS+, FSAE, etc)
    - 150 - 159 - VoIP / SIP servers / managers
    - 160 - 169 - FortiAnalyzers
    - 170 - 179 - FortiManagers
    - 180 - 189 - Other Fortinet products (FortiScan, FortiDB, etc.)
    - 190 - 199 - Other non-Fortinet servers (NAS, SQL, DNS, DDNS, etc.)
    - Fortinet products, non-FortiGate, are found from 160 - 189.
The following table shows some examples of how to choose an IP number for a device based on the information given. For internal and dmz, it is assumed in this case there is only one interface being used.

Table 1: Examples of the IP numbering

<table>
<thead>
<tr>
<th>Location and device</th>
<th>Internal</th>
<th>Dmz</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head Office, one FortiGate</td>
<td>10.011.101.100</td>
<td>10.011.201.100</td>
<td>172.20.120.191</td>
</tr>
<tr>
<td>Head Office, second FortiGate</td>
<td>10.012.101.100</td>
<td>10.012.201.100</td>
<td>172.20.120.192</td>
</tr>
<tr>
<td>Branch Office, one FortiGate</td>
<td>10.021.101.100</td>
<td>10.021.201.100</td>
<td>172.20.120.193</td>
</tr>
<tr>
<td>Office 7, one FortiGate with 9 VDOMs</td>
<td>10.079.101.100</td>
<td>10.079.101.100</td>
<td>172.20.120.194</td>
</tr>
<tr>
<td>Office 3, one FortiGate, web server</td>
<td>n/a</td>
<td>10.031.201.110</td>
<td>n/a</td>
</tr>
<tr>
<td>Bob in accounting on the corporate user network (dhcp) at Head Office, one FortiGate</td>
<td>10.0.11.101.200</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Router outside the FortiGate</td>
<td>n/a</td>
<td>n/a</td>
<td>172.20.120.195</td>
</tr>
</tbody>
</table>
Example Network configuration

The network configuration shown in Figure 1 or variations on it is used for many of the examples in this document. In this example, the 172.20.120.0 network is equivalent to the Internet. The network consists of a head office and two branch offices.

Figure 1: Example network configuration
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, but 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 2: 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 <em>Minimum log level</em>, select <em>Notification</em>.</td>
</tr>
</tbody>
</table>
| CLI input                                       | `config system dns
       set primary <address_ipv4>
       end`                                                                |
| CLI output                                      | `FGT-602803030703 # get system settings
       comments          : (null)
       opmode            : nat`                                               |
| Emphasis                                        | HTTP connections are *not* secure and can be intercepted by a third party.|
| File content                                    | `<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>
       <BODY><H4>You must authenticate to use this service.</H4>`         |
| Hyperlink                                       | Visit the Fortinet Technical Support web site, [https://support.fortinet.com](https://support.fortinet.com). |
| Keyboard entry                                  | Type a name for the remote VPN peer or client, such as Central_Office_1.|
| Navigation                                      | Go to *VPN > IPSEC > Auto Key (IKE)*.                                  |
| Publication                                     | For details, see the *FortiOS Handbook*.                              |

CLI command syntax conventions

This guide uses the following conventions to describe the 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 `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

### Table 3: Command syntax notation

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| Square brackets `[]` | A non-required word or series of words. For example: `[verbose {1 | 2 | 3}]`
   indicates that you may either omit or type both the `verbose` word and its accompanying option, such as: `verbose 3` |
Table 3: Command syntax notation  (Continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angle brackets &lt; &gt;</td>
<td>A word constrained by data type.</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;retries_int&gt;</code> indicates that you should enter a number of retries, such as 5.</td>
</tr>
<tr>
<td></td>
<td>Data types include:</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_name&gt;</code>: A name referring to another part of the configuration, such as policy_A.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_index&gt;</code>: An index number referring to another part of the configuration, such as 0 for the first static route.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_pattern&gt;</code>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx fqdn&gt;</code>: A fully qualified domain name (FQDN), such as mail.example.com.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_email&gt;</code>: An email address, such as <a href="mailto:admin@mail.example.com">admin@mail.example.com</a>.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_url&gt;</code>: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <a href="http://www.fortinet..com/">http://www.fortinet..com/</a>.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_ipv4&gt;</code>: An IPv4 address, such as 192.168.1.99.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_v4mask&gt;</code>: A dotted decimal IPv4 netmask, such as 255.255.255.0.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_ipv4mask&gt;</code>: A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_ipv4/mask&gt;</code>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as 192.168.1.99/24.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_ipv6&gt;</code>: A colon( : )-delimited hexadecimal IPv6 address, such as 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_v6mask&gt;</code>: An IPv6 netmask, such as /96.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_ipv6mask&gt;</code>: An IPv6 address and netmask separated by a space.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_str&gt;</code>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;xxx_int&gt;</code>: An integer number that is not another data type, such as 15 for the number of minutes.</td>
</tr>
</tbody>
</table>
Entering FortiOS configuration data

The configuration of a FortiGate unit is stored as a series of configuration settings in the FortiOS configuration database. To change the configuration you can use the web-based manager or CLI to add, delete or change configuration settings. These configuration changes are stored in the configuration database as they are made.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable).

**Entering text strings (names)**

Text strings are used to name entities in the configuration. For example, the name of a firewall address, administrative user, and so on. You can enter any character in a FortiGate configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, text strings in FortiGate configuration names cannot include the following characters:

" (double quote), & (ampersand), ' (single quote), < (less than) and > (greater than)

You can determine the limit to the number of characters that are allowed in a text string by determining how many characters the web-based manager or CLI allows for a given name field. From the CLI, you can also use the `tree` command to view the number of characters that are allowed. For example, firewall address names can contain up to 64 characters. When you add a firewall address to the web-based manager you are limited to entering 64 characters in the firewall address name field. From the CLI you can do the following to confirm that the firewall address name field allows 64 characters.

```bash
config firewall address
  tree
    -- [address] --*name (64)
      |-- subnet
      |-- type
      |-- start-ip
      |-- end-ip
```

Table 3: Command syntax notation (Continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Curly braces {</td>
<td>A word or series of words that is constrained to a set of options</td>
</tr>
<tr>
<td></td>
<td>delimited by either vertical bars or spaces. You must enter at least one of</td>
</tr>
<tr>
<td>Options delimited by vertical bars</td>
<td>Mutually exclusive options. For example:</td>
</tr>
<tr>
<td></td>
<td>{enable</td>
</tr>
<tr>
<td></td>
<td>must not enter both.</td>
</tr>
<tr>
<td>Options delimited by spaces</td>
<td>Non-mutually exclusive options. For example:</td>
</tr>
<tr>
<td></td>
<td>{http https ping snmp ssh telnet} indicates that you may enter all or a</td>
</tr>
<tr>
<td></td>
<td>subset of those options, in any order, in a space-delimited list, such as:</td>
</tr>
<tr>
<td></td>
<td>ping https ssh</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To change the options, you must re-type the entire list. For</td>
</tr>
<tr>
<td></td>
<td>example, to add snmp to the previous example, you would type:</td>
</tr>
<tr>
<td></td>
<td>ping https snmp ssh</td>
</tr>
<tr>
<td></td>
<td>If the option adds to or subtracts from the existing list of options,</td>
</tr>
<tr>
<td></td>
<td>instead of replacing it, or if the list is comma-delimited, the exception</td>
</tr>
<tr>
<td></td>
<td>will be noted.</td>
</tr>
</tbody>
</table>
Note that the tree command output also shows the number of characters allowed for other firewall address name settings. For example, the fully-qualified domain name (fqdn) field can contain up to 256 characters.

**Entering numeric values**

Numeric values are used to configure various sizes, rates, numeric addresses, or other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or as in the case of MAC or IPv6 addresses separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again such as MAC addresses) require hexadecimal numbers.

Most web-based manager numeric value configuration fields limit the number of numeric digits that you can add or contain extra information to make it easier to add the acceptable number of digits and to add numbers in the allowed range. CLI help includes information about allowed numeric value ranges. Both the web-based manager and the CLI prevent you from entering invalid numbers.

**Selecting options from a list**

If a configuration field can only contain one of a number of selected options, the web-based manager and CLI present you a list of acceptable options and you can select one from the list. No other input is allowed. From the CLI you must spell the selection name correctly.

**Enabling or disabling options**

If a configuration field can only be on or off (enabled or disabled) the web-based manager presents a check box or other control that can only be enabled or disabled. From the CLI you can set the option to enable or disable.

---

**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](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 Center article Registration Frequently Asked Questions.

---

**Fortinet products End User License Agreement**

See the [Fortinet products End User License Agreement](https://support.fortinet.com/).
Training

Fortinet Training Services provides courses that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email training@fortinet.com.

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 Center.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For 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.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate 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.
UTM overview

Ranging from the FortiGate®-30 series for small businesses to the FortiGate-5000 series for large enterprises, service providers and carriers, the FortiGate line combines a number of security features to protect your network from threats. As a whole, these features, when included in a single Fortinet security appliance, are referred to as Unified Threat Management (UTM). The UTM features your FortiGate model includes are:

- AntiVirus
- Intrusion Prevention System (IPS)
- Anomaly protection (DoS policies)
- One-armed IPS (Sniffer policies)
- Web filtering
- E-mail filtering, including protection against spam and grayware
- Data Leak Prevention (DLP)
- Application Control (for example, IM and P2P).

Firewall policies limit access, and while this and similar features are a vital part of securing your network, they are not covered in this document.

The following topics are included in this section:

- UTM components
- UTM profiles/lists/sensors
- UTM and Virtual domains (VDOMs)
- Conserve mode
- SSL content scanning and inspection
- Viewing and saving logged packets
- Using wildcards and Perl regular expressions

UTM components

AntiVirus

Your FortiGate unit stores a virus signature database that can identify more than 15,000 individual viruses. FortiGate models that support additional virus databases are able to identify hundreds of thousands of viruses. With a FortiGuard AntiVirus subscription, the signature databases are updated whenever a new threat is discovered.

AntiVirus also includes file filtering. When you specify files by type or by file name, the FortiGate unit will stop the matching files from reaching your users.

FortiGate units with a hard drive or configured to use a FortiAnalyzer unit can store infected and blocked files for that you can examine later.
Intrusion Protection System (IPS)

The FortiGate Intrusion Protection System (IPS) protects your network against hacking and other attempts to exploit vulnerabilities of your systems. More than 3,000 signatures are able to detect exploits against various operating systems, host types, protocols, and applications. These exploits can be stopped before they reach your internal network.

You can also write custom signatures, tailored to your network.

Anomaly protection (DoS policies)

A complement to the signature-based IPS, anomaly protection detects unusual network traffic that can be used to attack your network. When you set thresholds for various types of network operations, the FortiGate unit will block any attempt to exceed the thresholds you have defined.

One-armed IDS (sniffer policies)

You can use sniffer policies on the FortiGate unit as a one-arm intrusion detection system (IDS). The unit examines traffic for matches to the configured IPS sensor and application control list. Matches are logged and then all received traffic is dropped. In this way, you can configure a unit to sniff network traffic for attacks without actually processing the packets.

The FortiGate unit can log all detected IPS signatures and anomalies in a traffic stream.

Web filtering

Web filtering includes a number of features you can use to protect or limit your users’ activity on the web.

FortiGuard Web Filtering is a subscription service that allows you to limit access to web sites. More than 60 million web sites and two billion web pages are rated by category. You can choose to allow or block each of the 77 categories.

URL filtering can block your network users from access to URLs that you specify.

Web content filtering can restrict access to web pages based on words and phrases appearing on the web page itself. You can build lists of words and phrases, each with a score. When a web content list is selected in a web filter profile, you can specify a threshold. If a user attempts to load a web page and the score of the words on the page exceeds the threshold, the web page is blocked.

Email filtering

FortiGuard AntiSpam is a subscription service that includes an IP address black list, a URL black list, and an email checksum database. These resources are updated whenever new spam messages are received, so you do not need to maintain any lists or databases to ensure accurate spam detection.

You can use your own IP address lists and email address lists to allow or deny addresses, based on your own needs and circumstances.

Data Leak Prevention (DLP)

Data leak prevention allows you to define the format of sensitive data. The FortiGate unit can then monitor network traffic and stop sensitive information from leaving your network. Rules for U.S. social security numbers, Canadian social insurance numbers, as well as Visa, Mastercard, and American Express card numbers are included.
Application Control (for example, IM and P2P)

Although you can block the use of some applications by blocking the ports they use for communications, many applications do not use standard ports to communicate. Application control can detect the network traffic of more than 1000 applications, improving your control over application communication.

UTM profiles/lists/sensors

A profile is a group of settings that you can apply to one or more firewall policies. Each UTM feature is enabled and configured in a profile, list, or sensor. These are then selected in a firewall policy and the settings apply to all traffic matching the policy. For example, if you create an antivirus profile that enables antivirus scanning of HTTP traffic, and select the antivirus profile in the firewall policy that allows your users to access the World Wide Web, all of their web browsing traffic will be scanned for viruses.

Because you can use profiles in more than one firewall policy, you can configure one profile for the traffic types handled by a set of firewall policies requiring identical protection levels and types, rather than repeatedly configuring those same profile settings for each individual firewall policy.

For example, while traffic between trusted and untrusted networks might need strict protection, traffic between trusted internal addresses might need moderate protection. To provide the different levels of protection, you might configure two separate sets of profiles: one for traffic between trusted networks, and one for traffic between trusted and untrusted networks.

The UTM profiles include:

- antivirus profile
- IPS sensor
- Web filter profile
- Email filter profile
- Data Leak Prevention profile
- Application Control list
- VoIP profile

Although they’re called profiles, sensors, and lists, they’re functionally equivalent. Each is used to configure how the feature works.

UTM and Virtual domains (VDOMs)

If you enable virtual domains (VDOMs) on your FortiGate unit, all UTM configuration is limited to the VDOM in which you configure it.

While configuration is not shared, the various databases used by UTM features are shared. The FortiGuard antivirus and IPS databases and database updates are shared. The FortiGuard web filter and spam filter features contact the FortiGuard distribution network and access the same information when checking email for spam and web site categories and classification.
Conserve mode

FortiGate units perform all UTM processing in physical RAM. Since each model has a limited amount of memory, conserve mode is activated when the remaining free memory is nearly exhausted or the AV proxy has reached the maximum number of sessions it can service. While conserve mode is active, the AV proxy does not accept new sessions.

The AV proxy

Most content inspection the FortiGate unit performs requires that the files, email messages, URLs, and web pages be buffered and examined as a whole. The AV proxy performs this function, and because it may be buffering many files at the same time, it uses a significant amount of memory. Conserve mode is designed to prevent all the component features of the FortiGate unit from trying to use more memory than it has. Because the AV proxy uses so much memory, conserve mode effectively disables it in most circumstances. As a result, the content inspection features that use the AV proxy are also disabled in conserve mode.

All of the UTM features use the AV proxy with the exception of IPS, application control, flow-based antivirus scanning, and DoS. These features continue to operate normally when the FortiGate unit enters conserve mode.

Entering and exiting conserve mode

A FortiGate unit will enter conserve mode because it is nearly out of physical memory, or because the AV proxy has reached the maximum number of sessions it can service. The memory threshold that triggers conserve mode varies by model, but it is about 20% free memory. When memory use rises to the point where less than 20% of the physical memory is free, the FortiGate unit enters conserve mode.

The FortiGate unit will leave conserve mode only when the available physical memory exceeds about 30%. When exiting conserve mode, all new sessions configured to be scanned with features requiring the AV proxy will be scanned as normal, with the exception of a unit configured with the one-shot option.

Conserve mode effects

What happens when the FortiGate unit enters conserve mode depends on how you have configured. There are four options:

off

The off setting forces the FortiGate unit to stop all traffic that is configured for content inspection by UTM features that use the AV proxy. New sessions are not allowed but current sessions continue to be processed normally unless they request more memory. Sessions requesting more memory are terminated.

For example, if a firewall policy is configured to use antivirus scanning, the traffic it permits is blocked while in conserve mode. A policy with IPS scanning enabled continues as normal. A policy with both IPS and antivirus scanning is blocked because antivirus scanning requires the AV proxy.

Use the off setting when security is more important than a loss of access while the problem is rectified.
pass
The pass setting allows traffic to bypass the AV proxy and continue to its destination. Since the traffic is bypassing the proxy, no UTM scanning that requires the AV proxy is performed. UTM scanning that does not require the AV proxy continues normally. Use the pass setting when access is more important than security while the problem is rectified.
Pass is the default setting.

one-shot
The one-shot setting is similar to pass in that traffic is allowed when conserve mode is active. The difference is that a system configured for one-shot will force new sessions to bypass the AV proxy even after it leaves conserve mode. The FortiGate unit resumes use of the AV proxy only when the av-failopen setting is changed or the unit is restarted.

idledrop
The idledrop setting will recover memory and session space by terminating all the sessions associated with the host that has the most sessions open. The FortiGate may force this session termination a number of times, until enough memory is available to allow it to leave conserve mode.
The idledrop setting is primarily designed for situations in which malware may continue to open sessions until the AV proxy cannot accept more new sessions, triggering conserve mode. If your FortiGate unit is barely able to handle the traffic of your network, this setting could cause the termination of valid sessions. Use this option with caution.

Configuring the av-failopen command
You can configure the av-failopen command using the CLI.

    config system global
    set av-failopen {off | pass | one-shot | idledrop}
    end
The default setting is pass.

SSL content scanning and inspection
If your FortiGate model supports SSL content scanning and inspection, you can apply antivirus scanning, web filtering, FortiGuard Web Filtering, and email filtering to encrypted traffic. You can also apply DLP and DLP archiving to HTTPS, IMAPS, POP3S, and SMTPS traffic. To perform SSL content scanning and inspection, the FortiGate unit does the following:

• intercepts and decrypts HTTPS, IMAPS, POP3S, and SMTPS sessions between clients and servers (FortiGate SSL acceleration speeds up decryption)
• applies content inspection to decrypted content, including:
  • HTTPS, IMAPS, POP3S, and SMTPS Antivirus, DLP, and DLP archiving
  • HTTPS web filtering and FortiGuard web filtering
  • IMAPS, POP3S, and SMTPS email filtering
• encrypts the sessions and forwards them to their destinations.
Setting up certificates to avoid client warnings

To use SSL content scanning and inspection, you need to set up and use a certificate that supports it. FortiGate SSL content scanning and inspection intercepts the SSL keys that are passed between clients and servers during SSL session handshakes and then substitutes spoofed keys. Two encrypted SSL sessions are set up, one between the client and the FortiGate unit, and a second one between the FortiGate unit and the server. Inside the FortiGate unit the packets are decrypted.

While the SSL sessions are being set up, the client and server communicate in clear text to exchange SSL session keys. The session keys are based on the client and server certificates. The FortiGate SSL decrypt/encrypt process intercepts these keys and uses a built-in signing CA certificate named Fortinet_CA_SSLProxy to create keys to send to the client and the server. This signing CA certificate is used only by the SSL decrypt/encrypt process. The SSL decrypt/encrypt process then sets up encrypted SSL sessions with the client and server and uses these keys to decrypt the SSL traffic to apply content scanning and inspection.

Some client programs (for example, web browsers) can detect this key replacement and will display a security warning message. The traffic is still encrypted and secure, but the security warning indicates that a key substitution has occurred.

You can stop these security warnings by importing the signing CA certificate used by the server into the FortiGate unit SSL content scanning and inspection configuration. Then the FortiGate unit creates keys that appear to come from the server and not the FortiGate unit.

Note: You can add one signing CA certificate for SSL content scanning and inspection. The CA certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported for SSL content scanning and encryption.
You can replace the default signing CA certificate, Fortinet_CA_SSLProxy, with another signing CA certificate. To do this, you need the signing CA certificate file, the CA certificate key file, and the CA certificate password.

All SSL content scanning and inspection uses the same signing CA certificate. If your FortiGate unit is operating with virtual domains enabled, the same signing CA certificate is used by all virtual domains.

**To add a signing CA certificate for SSL content scanning and inspection**

1. Obtain a copy of the signing CA certificate file, the CA certificate key file, and the password for the CA certificate.
2. Go to System > Certificates > Local Certificates and select Import.
3. Set Type to Certificate.
4. For Certificate file, use the Browse button to select the signing CA certificate file.
5. For Key file, use the Browse button to select the CA certificate key file.
6. Enter the CA certificate Password.
7. Select OK.
8. Add the imported signing CA certificate to the SSL content scanning and inspection configuration. Use the following CLI command if the certificate name is Example_CA.

   ```
   config firewall ssl setting
   set caname Example_CA
   end
   ```

The Example_CA signing CA certificate will now be used by SSL content scanning and inspection for establishing encrypted SSL sessions.

**SSL content scanning and inspection settings**

If SSL content scanning and inspection is available on your FortiGate unit, you can configure SSL settings. The following table provides an overview of the options available and where to find further instruction:

### Table 4: SSL content scanning and inspection settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined firewall services</td>
<td>The IMAPS, POP3S and SMTPS predefined services. You can select these services in a firewall policy and a DoS policy.</td>
</tr>
<tr>
<td>Protocol recognition</td>
<td>The TCP port numbers that the FortiGate unit inspects for HTTPS, IMAPS, POP3S, and SMTPS. Go to Firewall &gt; Protocol Options. Add or edit a protocol options profile, configure HTTPS, IMAPS, POP3S, and SMTPS. Using Protocol Options, you can also configure the FortiGate unit to perform URL filtering of HTTPS or to use SSL content scanning and inspection to decrypt HTTPS so that the FortiGate unit can also apply antivirus and DLP content inspection and DLP archiving to HTTPS. Using SSL content scanning and inspection to decrypt HTTPS also allows you to apply more web filtering and FortiGuard Web Filtering options to HTTPS. To enable full SSL content scanning of web filtering, select Enable Deep Scanning under HTTPS in the protocol options profile.</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Antivirus options including virus scanning and file filtering for HTTPS, IMAPS, POP3S, and SMTPS. Go to UTM AntiVirus &gt; Profile. Add or edit a profile and configure Virus Scan for HTTPS, IMAPS, POP3S, and SMTPS.</td>
</tr>
</tbody>
</table>
### SSL content scanning and inspection (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Antivirus quarantine</strong></td>
<td>Antivirus quarantine options to quarantine files in HTTPS, IMAPS, POP3S, and SMTPS sessions.</td>
</tr>
<tr>
<td></td>
<td>Go to UTM &gt; AntiVirus &gt; Quarantine. You can quarantine infected files, suspicious files, and blocked files found in HTTPS, IMAPS, POP3S, and SMTPS sessions.</td>
</tr>
<tr>
<td><strong>Web filtering</strong></td>
<td>Web filtering options for HTTPS:</td>
</tr>
<tr>
<td></td>
<td>• Web Content Filter</td>
</tr>
<tr>
<td></td>
<td>• Web URL Filter</td>
</tr>
<tr>
<td></td>
<td>• ActiveX Filter</td>
</tr>
<tr>
<td></td>
<td>• Cookie Filter</td>
</tr>
<tr>
<td></td>
<td>• Java Applet Filter</td>
</tr>
<tr>
<td></td>
<td>• Web Resume Download Block</td>
</tr>
<tr>
<td></td>
<td>• Block invalid URLs</td>
</tr>
<tr>
<td></td>
<td>Go to UTM &gt; Web Filter &gt; Profile. Add or edit a web filter profile and configure web filtering for HTTPS.</td>
</tr>
<tr>
<td><strong>FortiGuard Web Filtering</strong></td>
<td>FortiGuard Web Filtering options for HTTPS:</td>
</tr>
<tr>
<td></td>
<td>• Enable FortiGuard Web Filtering</td>
</tr>
<tr>
<td></td>
<td>• Enable FortiGuard Web Filtering Overrides</td>
</tr>
<tr>
<td></td>
<td>• Provide Details for Blocked HTTP 4xx and 5xx Errors</td>
</tr>
<tr>
<td></td>
<td>• Rate Images by URL (Blocked images will be replaced with blanks)</td>
</tr>
<tr>
<td></td>
<td>• Allow Websites When a Rating Error Occurs</td>
</tr>
<tr>
<td></td>
<td>• Strict Blocking</td>
</tr>
<tr>
<td></td>
<td>• Rate URLs by Domain and IP Address</td>
</tr>
<tr>
<td></td>
<td>• Block HTTP Redirects by Rating</td>
</tr>
<tr>
<td></td>
<td>Go to UTM &gt; Web Filter &gt; Profile. Add or edit a profile and configure FortiGuard Web Filtering for HTTPS.</td>
</tr>
<tr>
<td><strong>Email filtering</strong></td>
<td>Email filtering options for IMAPS, POP3S, and SMTPS:</td>
</tr>
<tr>
<td></td>
<td>• FortiGuard Email Filtering IP Address Check, URL check, E-mail Checksum Check, and Spam Submission</td>
</tr>
<tr>
<td></td>
<td>• IP Address BWL Check</td>
</tr>
<tr>
<td></td>
<td>• E-mail Address BWL Check</td>
</tr>
<tr>
<td></td>
<td>• Return S-mail DNS Check</td>
</tr>
<tr>
<td></td>
<td>• Banned Word Check</td>
</tr>
<tr>
<td></td>
<td>• Spam Action</td>
</tr>
<tr>
<td></td>
<td>• Tag Location</td>
</tr>
<tr>
<td></td>
<td>• Tag Format</td>
</tr>
<tr>
<td></td>
<td>Go to UTM &gt; Email Filter &gt; Profile. Add or edit a profile and configure email filtering for IMAPS, POP3S, and SMTPS.</td>
</tr>
<tr>
<td><strong>Data Leak Prevention</strong></td>
<td>DLP for HTTPS, IMAPS, POP3S, and SMTPS. To apply DLP, follow the steps below:</td>
</tr>
<tr>
<td></td>
<td>• Go to UTM &gt; Data Leak Prevention &gt; Rule to add DLP rules. For HTTPS, add an HTTP rule and select HTTPS POST and HTTPS GET. For IMAPS, POP3S, and SMTPS, add an Email rule and select IMAPS, POP3S, and SMTPS.</td>
</tr>
<tr>
<td></td>
<td>• Go to UTM &gt; Data Leak Prevention &gt; Sensor, create a new DLP sensor or edit an existing one and then add the DLP rules to a DLP sensor.</td>
</tr>
<tr>
<td></td>
<td>• Go to Firewall &gt; Protocol Options. Add or edit a profile and select Enable Deep Scan under HTTPS.</td>
</tr>
<tr>
<td></td>
<td>• Go to Firewall &gt; Policy, edit the required policy, enable UTM, select Enable DLP Sensor and select the DLP sensor.</td>
</tr>
<tr>
<td></td>
<td>• Go to Firewall &gt; Policy, edit the required policy, enable Protocol Options and select a profile that has Enable Deep Scan selected under HTTPS. Note: If no protocol options profile is selected, or if Enable Deep Scan is not selected within the protocol options profile, DLP rules cannot inspect HTTPS.</td>
</tr>
</tbody>
</table>
Viewing and saving logged packets

The FortiGate unit supports packet logging for IPS and application control. The packets that trigger a signature match for IPS or application recognition for application control are saved for later viewing when packet logging is enabled.

For information on how to enable packet logging, see “Enable IPS packet logging” on page 99 and “Application control packet logging” on page 163.

Once the FortiGate unit has logged packets, you can view or save them.

To view and save logged packets
2. Depending on where the logs are configured to be stored, select the appropriate option:
   - Memory: Select if logs are stored in the FortiGate unit memory.
   - Disk: Select if the FortiGate unit has an internal hard disk and logs are stored there.
   - Remote: Select if logs are sent to a FortiAnalyzer unit or to the FortiGuard Analysis and Management Service.
3. Select the Packet Log icon of the log entry you want to view. The IPS Packet Log Viewer window appears.
4. Select the packet to view the packet in binary and ASCII. Each table row represents a captured packet.
5. Select Save to save the packet data in a PCAP formatted file.
   PCAP files can be opened and examined in network analysis software such as Wireshark.

Configuring packet logging options
You can use a number of CLI commands to further configure packet logging.

Limiting memory use
When logging to memory, you can define the maximum amount of memory used to store logged packets.

```
config ips settings
  set packet-log-memory 256
end
```

The acceptable range is from 64 to 8192 kilobytes. This command affects only logging to memory.
Limiting disk use

When logging to the FortiGate unit internal hard disk, you can define the maximum amount of space used to store logged packets.

```plaintext
config ips settings
  set ips-packet-quota 256
end
```

The acceptable range is from 0 to 4294967295 megabytes. This command affects only logging to disk.

Configuring how many packets are captured

Since the packet containing the signature is sometimes not sufficient to troubleshoot a problem, you can specify how many packets are captured before and after the packet containing the IPS signature match.

```plaintext
config ips settings
  packet-log-history
  packet-log-post-attack
end
```

The `packet-log-history` command specifies how many packets are captured before and including the one in which the IPS signature is detected. If the value is more 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 equalling the `packet-log-history` setting.

For example, if `packet-log-history` is set to 7, the FortiGate unit will save the packet containing the IPS signature match and the six before it.

The acceptable range for `packet-log-history` is from 1 to 255. The default is 1.

Note: Setting `packet-log-history` to a value larger than 1 can affect the performance of the FortiGate unit because network traffic must be buffered. The performance penalty depends on the model, the setting, and the traffic load.

The `packet-log-post-attack` command specifies how many packets are logged after the one in which the IPS signature is detected. For example, if `packet-log-post-attack` is set to 10, the FortiGate unit will save the ten packets following the one containing the IPS signature match.

The acceptable range for `packet-log-post-attack` is from 0 to 255. The default is 0.

Using wildcards and Perl regular expressions

Many UTM feature list entries can include wildcards or Perl regular expressions.

For more information about using Perl regular expressions, see [http://perldoc.perl.org/perlretut.html](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 Fortinet 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.\*\.*\.`.

Word boundary

In Perl regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression “test” not only matches the word “test” but also any word that contains “test” such as “atest”, “mytest”, “testimony”, “atestb”. The notation “\b” specifies the word boundary. To match exactly the word “test”, the expression should be `\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 5 lists and describes some example Perl regular expressions.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td>“abc” (the exact character sequence, but anywhere in the string)</td>
</tr>
<tr>
<td>^abc</td>
<td>“abc” at the beginning of the string</td>
</tr>
<tr>
<td>abc$</td>
<td>“abc” at the end of the string</td>
</tr>
<tr>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>^abc</td>
<td>abc$</td>
</tr>
<tr>
<td>ab(2,4)c</td>
<td>“a” followed by two, three or four “b”s followed by a “c”</td>
</tr>
<tr>
<td>ab(2,)c</td>
<td>“a” followed by at least two “b”s followed by a “c”</td>
</tr>
<tr>
<td>ab+c</td>
<td>“a” followed by any number (zero or more) of “b”s followed by a “c”</td>
</tr>
<tr>
<td>ab?c</td>
<td>“a” followed by an optional “b” followed by a “c”; that is, either “abc” or “ac”</td>
</tr>
<tr>
<td>a.c</td>
<td>“a” followed by any single character (not newline) followed by a” c</td>
</tr>
<tr>
<td>a\c</td>
<td>“a.c” exactly</td>
</tr>
<tr>
<td>[abc]</td>
<td>Any one of “a”, “b” and “c”</td>
</tr>
<tr>
<td>[Aa]bc</td>
<td>Either of “Abc” and “abc”</td>
</tr>
</tbody>
</table>
Table 5: Perl regular expression formats (Continued)

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[abc]+</td>
<td>Any (nonempty) string of “a”, “b” and “c” (such as “a”, “abba”, “acbabcacaa”)</td>
</tr>
<tr>
<td>[^abc]+</td>
<td>Any (nonempty) string which does not contain any of “a”, “b”, and “c” (such as “defg”)</td>
</tr>
<tr>
<td>\d\d</td>
<td>Any two decimal digits, such as 42; same as <code>\d{2}</code></td>
</tr>
<tr>
<td>/i</td>
<td>Makes the pattern case insensitive. For example, <code>/bad language/i</code> blocks any instance of “bad language” regardless of case.</td>
</tr>
<tr>
<td>/w+</td>
<td>A “word”: 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>“abc” when followed by a word boundary (for example, in “abc!” but not in “abcd”)</td>
</tr>
<tr>
<td>perl\B</td>
<td>“perl” when not followed by a word boundary (for example, in “perlert” but not in “perl stuff”)</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 (‘i’, ‘x’, 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>

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.*$/i`

`/cr[ééèèé][\+\-\*=<>\,\;\!\?\%\$\^°\$£€\{\}()\[\]\|\_01]dit/i`

Block common spam phrases

The following phrases are some examples of common phrases found in spam messages.

`/try it for free/i`

`/student loans/i`

`/you’re already approved/i`

`/special[\+\-\*=<>\,\;\!\?\%\$\^°\$£€\{\}()\[\]\|\_1]offer/i`
Network defense

This section describes in general terms the means by which attackers can attempt to compromise your network and steps you can take to protect it. The goal of an attack can be as complex as gaining access to your network and the privileged information it contains, or as simple as preventing customers from accessing your web server. Even allowing a virus onto your network can cause damage, so you need to protect against viruses and malware even if they are not specifically targeted at your network.

The following topics are included in this section:

- Monitoring
- Blocking external probes
- Defending against DoS attacks
- Traffic inspection
- Content inspection and filtering

Monitoring

Monitoring, in the form of logging, alert email, and SNMP, does not directly protect your network. But monitoring allows you to review the progress of an attack, whether afterwards or while in progress. How the attack unfolds may reveal weaknesses in your preparations. The packet archive and sniffer policy logs can reveal more details about the attack. Depending on the detail in your logs, you may be able to determine the attackers location and identity.

While log information is valuable, you must balance the log information with the resources required to collect and store it.

Blocking external probes

Protection against attacks is important, but attackers often use vulnerabilities and network tools to gather information about your network to plan an attack. It is often easier to prevent an attacker from learning important details about your network than to defend against an attack designed to exploit your particular network.

Attacks are often tailored to the hardware or operating system of the target, so reconnaissance is often the first step. The IP addresses of the hosts, the open ports, and the operating systems the hosts are running is invaluable information to an attacker. Probing your network can be as simple as an attacker performing an address sweep or port scan to a more involved operation like sending TCP packets with invalid combinations of flags to see how your firewall reacts.

Address sweeps

An address sweep is a basic network scanning technique to determine which addresses in an address range have active hosts. A typical address sweep involves sending an ICMP ECHO request (a ping) to each address in an address range to attempt to get a response. A response signifies that there is a host at this address that responded to the ping. It then becomes a target for more detailed and potentially invasive attacks.
Address sweeps do not always reveal all the hosts in an address range because some systems may be configured to ignore ECHO requests and not respond, and some firewalls and gateways may be configured to prevent ECHO requests from being transmitted to the destination network. Despite this shortcoming, Address sweeps are still used because they are simple to perform with software tools that automate the process.

Use the `icmp_sweep` anomaly in a DoS sensor to protect against address sweeps.

There are a number of IPS signatures to detect the use of ICMP probes that can gather information about your network. These signatures include `AddressMask`, `Traceroute`, `ICMP.Invalid.Packet.Size`, and `ICMP.Oversized.Packet`. Include ICMP protocol signatures in your IPS sensors to protect against these probes/attacks.

### Port scans

Potential attackers may run a port scan on one or more of your hosts. This involves trying to establish a communication session to each port on a host. If the connection is successful, a service may be available that the attacker can exploit.

Use the DoS sensor anomaly `tcp_port_scan` to limit the number of sessions (complete and incomplete) from a single source IP address to the configured threshold. If the number of sessions exceed the threshold, the configured action is taken.

Use the DoS sensor anomaly `udp_scan` to limit UDP sessions in the same way.

### Probes using IP traffic options

Every TCP packet has space reserved for eight flags or control bits. They are used for communicating various control messages. Although space in the packet is reserved for all eight, there are various combinations of flags that should never happen in normal network operation. For example, the SYN flag, used to initiate a session, and the FIN flag, used to end a session, should never be set in the same packet.

Attackers may create packets with these invalid combinations to test how a host will react. Various operating systems and hardware react in different ways, giving a potential attackers clues about the components of your network.

The IPS signature `TCP.Bad.Flags` detects these invalid combinations. The default action is pass though you can override the default and set it to `Block` in your IPS sensor.

### Configure packet reply and TCP sequence checking

The anti-reply CLI command allows you to set the level of checking for packet replay and TCP sequence checking (or TCP Sequence (SYN) number checking). All TCP packets contain a Sequence Number (SYN) and an Acknowledgement Number (ACK). The TCP protocol uses these numbers for error free end-to-end communications. TCP sequence checking can also be used to validate individual packets.

FortiGate units use TCP sequence checking to make sure that a packet is part of a TCP session. By default, if a packet is received with sequence numbers that fall out of the expected range, the FortiGate unit drops the packet. This is normally a desired behavior, since it means that the packet is invalid. But in some cases you may want to configure different levels of anti-replay checking if some of your network equipment uses non-RFC methods when sending packets.

Configure the anti-reply CLI command:

```plaintext
config system global
  anti-reply {disable | loose | strict}
end
```
You can set anti-replay protection to the following settings:

- **disable** — No anti-replay protection.
- **loose** — Perform packet sequence checking and ICMP anti-replay checking with the following criteria:
  - The SYN, FIN, and RST bit cannot appear in the same packet.
  - The FortiGate unit does not allow more than one ICMP error packet through before it receives a normal TCP or UDP packet.
  - If the FortiGate unit receives an RST packet, and check-reset-range is set to strict, the FortiGate unit checks to determine if its sequence number in the RST is within the un-ACKed data and drops the packet if the sequence number is incorrect.
  - **strict** — Performs all of the loose checking but for each new session also checks to determine of the TCP sequence number in a SYN packet has been calculated correctly and started from the correct value for each new session. Strict anti-replay checking can also help prevent SYN flooding.

If any packet fails a check it is dropped.

**Configure ICMP error message verification**

```text
check-reset-range {disable | strict}
```

Enable ICMP error message verification to ensure an attacker cannot send an invalid ICMP error message.

```text
config system global
  check-reset-range {disable | strict}
end
```

- **disable** — the FortiGate unit does not validate ICMP error messages.
- **strict** — enable ICMP error message checking.

If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. Strict checking also affects how the anti-replay option checks packets.

**Protocol header checking**

Select the level of checking performed on protocol headers.

```text
config system global
  check-protocol-header {loose | strict}
end
```

- **loose** — the FortiGate unit performs basic header checking to verify that a packet is part of a session and should be processed. Basic header checking includes verifying that the layer-4 protocol header length, the IP header length, the IP version, the IP checksum, IP options are correct, etc.
- **strict** — the FortiGate unit does the same checking as above plus it verifies that ESP packets have the correct sequence number, SPI, and data length.

If the packet fails header checking it is dropped by the FortiGate unit.
Evasion techniques

Attackers employ a wide range of tactics to try to disguise their techniques. If an attacker disguises a known attack in such a way that it is not recognized, the attack will evade your security and possibly succeed. FortiGate security recognizes a wide variety of evasion techniques and normalizes data traffic before inspecting it.

Packet fragmentation

Information sent across local networks and the Internet is encapsulated in packets. There is a maximum allowable size for packets and this maximum size varies depending on network configuration and equipment limitations. If a packet arrives at a switch or gateway and it is too large, the data it carries is divided among two or more smaller packets before being forwarded. This is called fragmentation.

When fragmented packets arrive at their destination, they are reassembled and read. If the fragments do not arrive together, they must be held until all of the fragments arrive. Reassembly of a packet requires all of the fragments.

The FortiGate unit automatically reassembles fragmented packets before processing them because fragmented packets can evade security measures. Both IP packets and TCP packets are reassembled by the IPS engine before examination.

For example, you have configured the FortiGate unit to block access to the example.org web site. Any checks for example.com will fail if a fragmented packet arrives and one fragment contains http://www.exa while the other contains mple.com/. Viruses and malware can be fragmented and avoid detection in the same way. The FortiGate unit will reassemble fragmented packets before examining network data to ensure that inadvertent or deliberate packet fragmentation does not hide threats in network traffic.

Non-standard ports

Most traffic is sent on a standard port based on the traffic type. The FortiGate unit recognizes most traffic by packet content rather than the TCP/UDP port and uses the proper IPS signatures to examine it. Protocols recognized regardless of port include DHCP, DNP3, FTP, HTTP, IMAP, MS RPC, NNTP, POP3, RSTP, SIP, SMTP, and SSL, as well as the supported IM/P2P application protocols.

In this way, the FortiGate unit will recognize HTTP traffic being sent on port 25 as HTTP rather than SMTP, for example. Because the protocol is correctly identified, the FortiGate unit will examine the traffic for any enabled HTTP signatures.

Negotiation codes

Telnet and FTP servers and clients support the use of negotiation information to allow the server to report what features it supports. This information has been used to exploit vulnerable servers. To avoid this problem, the FortiGate unit removes negotiation codes before IPS inspection.

HTTP URL obfuscation

Attackers encode HTML links using various formats to evade detection and bypass security measures. For example, the URL www.example.com/cgi.bin could be encoded in a number of ways to avoid detection but still work properly, and be interpreted the same, in a web browser.

The FortiGate prevents the obfuscation by converting the URL to ASCII before inspection.
Network defense

Defending against DoS attacks

A denial of service is the result of an attacker sending an abnormally large amount of network traffic to a target system. Having to deal with the traffic flood slows down or disables the target system so that legitimate users can not use it for the duration of the attack.

HTTP header obfuscation

The headers of HTTP requests or responses can be modified to make the discovery of patterns and attacks more difficult. To prevent this, the FortiGate unit will:

- remove junk header lines
- reassemble an HTTP header that's been folded onto multiple lines
- move request parameters to HTTP POST body from the URL

The message is scanned for any enabled HTTP IPS signatures once these problems are corrected.

HTTP body obfuscation

The body content of HTTP traffic can be hidden in an attempt to circumvent security scanning. HTTP content can be GZipped or deflated to prevent security inspection. The FortiGate unit will uncompress the traffic before inspecting it.

Another way to hide the contents of HTTP traffic is to send the HTTP body in small pieces, splitting signature matches across two separate pieces of the HTTP body. The FortiGate unit reassembles these ‘chunked bodies’ before inspection.

Microsoft RPC evasion

Because of its complexity, the Microsoft Remote Procedure Call protocol suite is subject to a number of known evasion techniques, including:

- SMB-level fragmentation
- DCERPC-level fragmentation
- DCERPC multi-part fragmentation
- DCERPC UDP fragmentation
- Multiple DCERPC fragments in one packet

The FortiGate unit reassembles the fragments into their original form before inspection.

Table 6: HTTP URL obfuscation types

<table>
<thead>
<tr>
<th>Encoding type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>No encoding</td>
<td><a href="http://www.example.com/cgi.bin/">http://www.example.com/cgi.bin/</a></td>
</tr>
<tr>
<td>Decimal encoding</td>
<td><a href="http://www.example.com/&amp;#99;&amp;#103;&amp;#105;&amp;#46;&amp;#98;&amp;#105;&amp;#110;&amp;#47">http://www.example.com/&amp;#99;&amp;#103;&amp;#105;&amp;#46;&amp;#98;&amp;#105;&amp;#110;&amp;#47</a>;</td>
</tr>
<tr>
<td>URL encoding</td>
<td><a href="http://www.example.com/%43%47%49%2E%42%49%4E%2F">http://www.example.com/%43%47%49%2E%42%49%4E%2F</a></td>
</tr>
<tr>
<td>ANSI encoding</td>
<td><a href="http://www.example.com/%u0063%u0067%u0069%u002E%u0062%u0069%u006E/">http://www.example.com/%u0063%u0067%u0069%u002E%u0062%u0069%u006E/</a></td>
</tr>
<tr>
<td>Directory traversal</td>
<td><a href="http://www.example.com/cgi.bin/test/../">http://www.example.com/cgi.bin/test/../</a></td>
</tr>
</tbody>
</table>

Defending against DoS attacks

A denial of service is the result of an attacker sending an abnormally large amount of network traffic to a target system. Having to deal with the traffic flood slows down or disables the target system so that legitimate users can not use it for the duration of the attack.
Any network traffic the target system receives has to be examined, and then accepted or rejected. TCP, UDP, and ICMP traffic is most commonly used, but a particular type of TCP traffic is the most effective. TCP packets with the SYN flag are the most efficient DoS attack tool because of how communication sessions are started between systems.

The “three-way handshake”

Communication sessions between systems start with establishing a TCP/IP connection. This is a simple three step process, sometimes called a “three-way handshake,” initiated by the client attempting to open the connection.

1. The client sends a TCP packet with the SYN flag set. With the SYN packet, the client informs the server of its intention to establish a connection.

2. If the server is able to accept the connection to the client, it sends a packet with the SYN and the ACK flags set. This simultaneously acknowledges the SYN packet the server has received, and informs the client that the server intends to establish a connection.

3. To acknowledge receipt of the packet and establish the connection, the client sends an ACK packet.

![Figure 3: Establishing a TCP/IP connection](image)

The three-way handshake is a simple way for the server and client to each agree to establish a connection and acknowledge the other party expressing its intent. Unfortunately, the three-way handshake can be used to interfere with communication rather than facilitate it.

**SYN flood**

When a client sends a SYN packet to a server, the server creates an entry in its session table to keep track of the connection. The server then sends a SYN+ACK packet expecting an ACK reply and the establishment of a connection.

An attacker intending to disrupt a server with a denial of service (DoS) attack can send a flood of SYN packets and not respond to the SYN+ACK packets the server sends in response. Networks can be slow and packets can get lost so the server will continue to send SYN+ACK packets until it gives up, and removes the failed session from the session table. If an attacker sends enough SYN packets to the server, the session table will fill completely, and further connection attempts will be denied until the incomplete sessions time out. Until this happens, the server is unavailable to service legitimate connection requests.
Figure 4: A single client launches a SYN flood attack

SYN floods are seldom launched from a single address so limiting the number of connection attempts from a single IP address is not usually effective.

**SYN spoofing**

With a flood of SYN packets coming from a single attacker, you can limit the number of connection attempts from the source IP address or block the attacker entirely. To prevent this simple defense from working, or to disguise the source of the attack, the attacker may spoof the source address and use a number of IP addresses to give the appearance of a distributed denial of service (DDoS) attack. When the server receives the spoofed SYN packets, the SYN+ACK replies will go to the spoofed source IP addresses which will either be invalid, or the system receiving the reply will not know what to do with it.

Figure 5: A client launches a SYN spoof attack

**DDoS SYN flood**

The most severe form of SYN attack is the distributed SYN flood, one variety of distributed denial of service attack (DDoS). Like the SYN flood, the target receives a flood of SYN packets and the ACK+SYN replies are never answered. The attack is distributed across multiple sources sending SYN packets in a coordinated attack.
Defending against DoS attacks

The distributed SYN flood is more difficult to defend against because multiple clients are capable of creating a larger volume of SYN packets than a single client. Even if the server can cope, the volume of traffic may overwhelm a point in the network upstream of the targeted server. The only defence against this is more bandwidth to prevent any choke-points.

Configuring the SYN threshold to prevent SYN floods

The preferred primary defence against any type of SYN flood is the DoS sensor \texttt{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 \texttt{Pass}, the FortiGate unit will allow the SYN packets that exceed the threshold. If the action is set to \texttt{Block}, the FortiGate 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 when 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 \texttt{Block}.

For more information, see "Creating and configuring a DoS sensor" on page 167. For recommendations on how to configure DoS policies, see “DoS policy recommendations” on page 44.

SYN proxy

FortiGate units with Fortinet security processing modules installed offer a third action for the \texttt{tcp_syn_flood} threshold when a module is installed. Instead of \texttt{Block} and \texttt{Pass}, you can choose to \texttt{Proxy} the incomplete connections that exceed the threshold value.

When the \texttt{tcp_syn_flood} threshold action is set to \texttt{Proxy}, incomplete TCP connections are allowed as normal as long as the configured threshold is not exceeded. If the threshold is exceeded, the FortiGate unit will intercept incoming SYN packets from clients and respond with a SYN+ACK packet. If the FortiGate 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.
Other flood types

UDP and ICMP packets can also be used for DoS attacks, though they are less common. TCP SYN packets are so effective because the target receives them and maintains a session table entry for each until they time out. Attacks using UDP or ICMP packets do not require the same level of attention from a target, rendering them less effective. The target will usually drop the offending packets immediately, closing the session.

Use the `udp_flood` and `icmp_flood` thresholds to defend against these DoS attacks.

Traffic inspection

When the FortiGate unit examines network traffic one packet at a time for IPS signatures, it is performing traffic analysis. This is unlike content analysis where the traffic is buffered until files, email messages, web pages, and other files are assembled and examined as a whole.

DoS policies use traffic analysis by keeping track of the type and quantity of packets, as well as their source and destination addresses.

Application control uses traffic analysis to determine which application generated the packet.

Although traffic inspection doesn't involve taking packets and assembling files they are carrying, the packets themselves can be split into fragments as they pass from network to network. These fragments are reassembled by the FortiGate unit before examination.

No two networks are the same and few recommendations apply to all networks. This topic offers suggestions on how you can use the FortiGate unit to help secure your network against content threats.

IPS signatures

IPS signatures can detect malicious network traffic. For example, the Code Red worm attacked a vulnerability in the Microsoft IIS web server. Your FortiGate’s IPS system can detect traffic attempting to exploit this vulnerability. IPS may also detect when infected systems communicate with servers to receive instructions.

IPS recommendations

- Enable IPS scanning at the network edge for all services.
- Use FortiClient endpoint IPS scanning for protection against threats that get into your network.
- Subscribe to FortiGuard IPS Updates and configure your FortiGate unit to receive push updates. This will ensure you receive new IPS signatures as soon as they are available.
- Your FortiGate unit includes IPS signatures written to protect specific software titles from DoS attacks. Enable the signatures for the software you have installed and set the signature action to `Block`.
  
  You can view these signatures by going to `UTM > Intrusion Protection > Predefined` and sorting by, or applying a filter to, the `Group` column.
- Because it is critical to guard against attacks on services that you make available to the public, configure IPS signatures to block matching signatures. For example, if you have a web server, configure the action of web server signatures to `Block`. 
Suspicious traffic attributes

Network traffic itself can be used as an attack vector or a means to probe a network before an attack. For example, SYN and FIN flags should never appear together in the same TCP packet. The SYN flag is used to initiate a TCP session while the FIN flag indicates the end of data transmission at the end of a TCP session.

The FortiGate unit has IPS signatures that recognize abnormal and suspicious traffic attributes. The SYN/FIN combination is one of the suspicious flag combinations detected in TCP traffic by the `TCP.BAD.FLAGS` signature.

The signatures that are created specifically to examine traffic options and settings, begin with the name of the traffic type they are associated with. For example, signatures created to examine TCP traffic have signature names starting with TCP.

DoS policies

DDoS attacks vary in nature and intensity. Attacks aimed at saturating the available bandwidth upstream of your service can only be countered by adding more bandwidth. DoS policies can help protect against DDoS attacks that aim to overwhelm your server resources.

DoS policy recommendations

- Use and configure DoS policies to appropriate levels based on your network traffic and topology. This will help drop traffic if an abnormal amount is received.
- It is important to set a good threshold. The threshold defines the maximum number of sessions/packets per second of normal traffic. If the threshold is exceeded, the action is triggered. Threshold defaults are general recommendations, although your network may require very different values.

One way to find the correct values for your environment is to set the action to Pass and enable logging. Observe the logs and adjust the threshold values until you can determine the value at which normal traffic begins to generate attack reports. Set the threshold above this value with the margin you want. Note that the smaller the margin, the more protected your system will be from DoS attacks, but your system will also be more likely to generate false alarms.

Application control

While applications can often be blocked by the ports they use, application control allows convenient management of all supported applications, including those that do not use set ports.

Application control recommendations

- Some applications behave in an unusual manner in regards to application control. For more information, see “Application considerations” on page 164.
- By default, application control allows the applications not specified in the application control list. For high security networks, you may want to change this behavior so that only the explicitly allowed applications are permitted.
Content inspection and filtering

When the FortiGate unit buffers the packets containing files, email messages, web pages, and other similar files for reassembly before examining them, it is performing content inspection. Traffic inspection, on the other hand, is accomplished by the FortiGate unit examining individual packets of network traffic as they are received.

No two networks are the same and few recommendations apply to all networks. This topic offers suggestions on how you can use the FortiGate unit to help secure your network against content threats. Be sure to understand the effects of the changes before using the suggestions.

AntiVirus

The FortiGate antivirus scanner can detect viruses and other malicious payloads used to infect machines. The FortiGate unit performs deep content inspection. To prevent attempts to disguise viruses, the antivirus scanner will reassemble fragmented files and uncompress content that has been compressed. Patented Compact Pattern Recognition Language (CPRL) allows further inspection for common patterns, increasing detection rates of virus variations in the future.

AntiVirus recommendations

- Enable antivirus scanning at the network edge for all services.
- Use FortiClient endpoint antivirus scanning for protection against threats that get into your network.
- Subscribe to FortiGuard AntiVirus Updates and configure your FortiGate unit to receive push updates. This will ensure you receive new antivirus signatures as soon as they are available.
- Enable the Extended Virus Database if your FortiGate unit supports it.
- Examine antivirus logs periodically. Take particular notice of repeated detections. For example, repeated virus detection in SMTP traffic could indicate a system on your network is infected and is attempting to contact other systems to spread the infection using a mass mailer.
- The *builtin-patterns* file filter list contains nearly 20 file patterns. Many of the represented files can be executed or opened with a double-click. If any of these file patterns are not received as a part of your normal traffic, blocking them may help protect your network. This also saves resources since files blocked in this way do not need to be scanned for viruses.
- To conserve system resources, avoid scanning email messages twice. Scan messages as they enter and leave your network or when clients send and retrieve them, rather than both.

FortiGuard Web Filtering

The web is the most popular part of the Internet and, as a consequence, virtually every computer connected to the Internet is able to communicate using port 80, HTTP. Botnet communications take advantage of this open port and use it to communicate with infected computers. FortiGuard Web Filtering can help stop infections from malware sites and help prevent communication if an infection occurs.
**FortiGuard Web Filtering recommendations**

- Enable FortiGuard Web Filtering at the network edge.
- Install the FortiClient application and use FortiGuard Web Filtering on any systems that bypass your FortiGate unit.
- Block categories such as Pornography, Malware, Spyware, and Phishing. These categories are more likely to be dangerous.
- In the email filter profile, enable **IP Address Check** in **FortiGuard Email Filtering**. Many IP addresses used in spam messages lead to malicious sites; checking them will protect your users and your network.

**Email filter**

Spam is a common means by which attacks are delivered. Users often open email attachments they should not, and infect their own machine. The FortiGate email filter can detect harmful spam and mark it, alerting the user to the potential danger.

**Email filter recommendations**

- Enable email filtering at the network edge for all types of email traffic.
- Use FortiClient endpoint scanning for protection against threats that get into your network.
- Subscribe to the FortiGuard AntiSpam Service.

**DLP**

Most security features on the FortiGate unit are designed to keep unwanted traffic out of your network while DLP can help you keep sensitive information from leaving your network. For example, credit card numbers and social security numbers can be detected by DLP sensors.

**DLP recommendations**

- Rules related to HTTP posts can be created, but if the requirement is to block all HTTP posts, a better solution is to use application control or the **HTTP POST Action** option in the web filter profile.
- While DLP can detect sensitive data, it is more efficient to block unnecessary communication channels than to use DLP to examine it. If you don’t use instant messaging or peer-to-peer communication in your organization, for example, use application control to block them entirely.
AntiVirus

This section describes how to configure the antivirus options. From an antivirus profile you can configure the FortiGate unit to apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, IM, and NNTP sessions. If your FortiGate unit supports SSL content scanning and inspection, you can also configure antivirus protection for HTTPS, IMAPS, POP3S, and SMTPS sessions.

The following topics are included in this section:

- Antivirus concepts
- Enable antivirus scanning
- Enable the file quarantine
- Enable file filtering
- Enable grayware scanning
- Testing your antivirus configuration
- Antivirus examples

Antivirus concepts

The word “antivirus” refers to a group of features that are designed to prevent unwanted and potentially malicious files from entering your network. These features all work in different ways, which include checking for a file size, name, or type, or for the presence of a virus or grayware signature.

The antivirus scanning routines your FortiGate unit uses are designed to share access to the network traffic. This way, each individual feature does not have to examine the network traffic as a separate operation, and the overhead is reduced significantly. For example, if you enable file filtering and virus scanning, the resources used to complete these tasks are only slightly greater than enabling virus scanning alone. Two features do not require twice the resources.

How antivirus scanning works

Antivirus scanning examines files for viruses, worms, trojans, and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.

The most thorough scan requires that the FortiGate unit have the whole file for the scanning procedure. To achieve this, the antivirus proxy buffers the file as it arrives. Once the transmission is complete, the virus scanner examines the file. If no infection is present, it is sent to the destination. If an infection is present, a replacement message is set to the destination.

During the buffering and scanning procedure, the client must wait. With a default configuration, the file is released to the client only after it is scanned. You can enable client comforting in the protocol options profile to feed the client a trickle of data to prevent them from thinking the transfer is stalled, and possibly cancelling the download.
Buffering the entire file allows the FortiGate unit to eliminate the danger of missing an infection due to fragmentation because the file is reassembled before examination. Archives can also be expanded and the contents scanned, even if archives are nested.

Since the FortiGate unit has a limited amount of memory, files larger than a certain size do not fit within the memory buffer. The default buffer size is 10 MB. You can use the `uncompsizelimit` CLI command to adjust the size of this memory buffer.

Files larger than the buffer are passed to the destination without scanning. You can use the `Oversize File/Email` setting to block files larger than the antivirus buffer if allowing files that are too large to be scanned is an unacceptable security risk.

**Flow-based antivirus scanning**

If your FortiGate unit supports flow-based antivirus scanning, you can choose to select it instead of proxy-based antivirus scanning. Flow-based antivirus scanning uses the FortiGate IPS engine to examine network traffic for viruses, worms, trojans, and malware, without the need to buffer the file being checked.

The advantages of flow-based scanning include faster scanning and no maximum file size. Flow-based scanning doesn’t require the file be buffered so it is scanned as it passes through the FortiGate unit, packet-by-packet. This eliminates the maximum file size limit and the client begins receiving the file data immediately.

The trade-off for these advantages is that flow-based scans detect a smaller number of infections. Viruses in documents, packed files, and some archives are less likely to be detected because the scanner can only examine a small portion of the file at any moment.

Note however that your choice of flow-based or proxy-based scans only affects antivirus scans. Although you enable file filtering in the antivirus profile, it requires that files be proxied. Therefore, if you enable both flow-based antivirus scanning and file filtering, files will not be proxied for antivirus scans, but they will be proxied for file filtering.

**Antivirus scanning order**

The antivirus scanning function includes various modules and engines that perform separate tasks.

**Proxy-based antivirus scanning order**

Figure 7 on page 49 illustrates the antivirus scanning order when using proxy-based scanning (i.e. the normal, extended, or extreme databases). The first check for oversized files/email is to determine whether the file exceeds the configured size threshold. The `uncompsizelimit` check is to determine if the file can be buffered for file type and antivirus scanning. If the file is too large for the buffer, it is allowed to pass without being scanned. For more information, see the `config antivirus service` command in the FortiGate CLI Reference. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.

Note: File filtering includes file pattern and file type scans which are applied at different stages in the antivirus process.
Figure 7: Antivirus scanning order when using the normal, extended, or extreme database

If a file fails any of the tasks of the antivirus scan, no further scans are performed. For example, if the file `fakefile.EXE` is recognized as a blocked file pattern, the FortiGate unit will send the end user a replacement message, and delete or quarantine the file. The unit will not perform virus scan, grayware, heuristics, and file type scans because the previous checks have already determined that the file is a threat and have dealt with it.

Flow-based antivirus scanning order

Figure 8 on page 50 illustrates the antivirus scanning order when using flow-based scanning (i.e. the flow-based database). The antivirus scan takes place before any other antivirus-related scan. If file filter is not enabled, the file is not buffered. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.

Note: File filtering includes file pattern and file type scans which are applied at different stages in the antivirus process.
Antivirus databases

The antivirus scanning engine relies on a database to detail the unique attributes of each infection. The antivirus scan searches for these signatures, and when one is discovered, the FortiGate unit determines the file is infected and takes action.

All FortiGate units have the normal antivirus signature database but some models have additional databases you can select for use. Which you choose depends on your network and security needs.

<table>
<thead>
<tr>
<th>Database</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.</td>
</tr>
<tr>
<td>Extended</td>
<td>Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.</td>
</tr>
<tr>
<td>Extreme</td>
<td>Includes the extended database in addition to a large collection of ‘zoo’ viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.</td>
</tr>
<tr>
<td>Flow</td>
<td>The flow-based database is a subset of the extreme database. Flow-based scans can not detect polymorphic and packed-file viruses so those signatures and not included in the flow-based database. Note that flow-based scanning is not just another database, but a different type of scanning. For more information, see “How antivirus scanning works” on page 47.</td>
</tr>
</tbody>
</table>

Figure 8: Antivirus scanning order when using the flow-based database
Antivirus techniques

The antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first four features have specific functions, the fifth, heuristics, protects against any new, previously unknown virus threats. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The features are discussed in the order that they are applied, followed by FortiGuard antivirus.

File size

This task checks if files and email messages exceed configured size thresholds. You enable this check by editing your protocol options profiles and setting the Oversized File/Email option to Block for each protocol. The maximum size you can set varies by model.

File pattern

Once a file is accepted, the FortiGate unit applies the file pattern recognition filter. The unit will check the file name against the file pattern setting you have configured. If the file name matches a blocked pattern, “.EXE” for example, then it is stopped and a replacement message is sent to the end user. No other levels of protection are applied. If the file name does not match a blocked pattern, the next level of protection is applied.

Virus scan

If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN). For more information, see “FortiGuard Antivirus” on page 52.

Grayware

If the file passes the virus scan, it will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information, see “Enable grayware scanning” on page 61.

Heuristics

After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results.

Note: You can configure heuristics only through the CLI. See the FortiGate CLI Reference.

File type

Finally, the FortiGate unit applies the file type recognition filter. The FortiGate unit will check the file against the file type setting you have configured. If the file is a blocked type, then it is stopped and a replacement message is sent to the end user. No other levels of protection are applied.
FortiGuard Antivirus

FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.

The connection between the FortiGate unit and FortiGuard Center is configured in System > Maintenance > FortiGuard.

Enable antivirus scanning

Antivirus scanning is enabled in the antivirus profile. Once the antivirus profile is enabled and selected in one or more firewall policies, all the traffic controlled by those firewall policies will scanned according to your settings.

To enable antivirus scanning — web-based manager

1. Go to UTM > AntiVirus > Profile.
2. Select Create New to create a new antivirus profile, or select an existing antivirus profile and choose Edit.
3. In the row labeled Virus Scan, select the check boxes associated with the traffic you want scanned for viruses.
4. Select OK.

To enable antivirus scanning — CLI

You need to configure the scan option for each type of traffic you want scanned. In this example, antivirus scanning of HTTP traffic is enabled in the profile.

```
config antivirus profile
edit my_av_profile
config http
    set options scan
end
end
```

Viewing antivirus database information

The FortiGate antivirus scanner relies on up-to-date virus signatures to detect the newest threats. To view the information about the FortiGate unit virus signatures, check the status page or the Virus Database information page:

- **Status page**: Go to System > Dashboard > Dashboard. In the License Information section under FortiGuard Services, the AV Definitions field shows the regular antivirus database version as well as when it was last updated.

  If your FortiGate unit supports extended and extreme virus database definitions, the database versions and date they were last updated is displayed in the Extended set and Extreme DB fields.

  The flow-based virus database is distributed as part of the IPS signature database. Its database version and date it was last updated is displayed in the IPS Definitions field.
**Virus Database**

Go to **UTM > AntiVirus > Virus Database**. This page shows the version number, number of included signatures, and a description of the regular virus database. If your FortiGate unit supports extended, extreme, or flow-based virus database definitions, the version numbers, number of included signatures, and descriptions of those databases are also displayed.

**Changing the default antivirus database**

If your FortiGate unit supports extended, extreme, or flow-based virus database definitions, you can select the virus database most suited to your needs.

In most circumstances, the regular virus database provides sufficient protection. Viruses known to be active are included in the regular virus database. The extended database includes signatures of the viruses that have become rare within the last year in addition to those in the normal database. The extreme database includes legacy viruses that have not been seen in the wild in a long time in addition to those in the extended database.

The flow-based database contains a subset of the virus signatures in the extreme database. Unlike the other databases, selecting the flow-based database also changes the way the FortiGate unit scans your network traffic for viruses. Instead of the standard proxy-based scan, network traffic is scanned as it streams through the FortiGate unit. For more information on the differences between flow-based and proxy-based antivirus scanning, see “How antivirus scanning works” on page 47.

If you require the most comprehensive antivirus protection, enable the extended virus database. The additional coverage comes at a cost, however, because the extra processing requires additional resources.

**To change the antivirus database — web-based manager**

1. Go to **UTM > AntiVirus > Virus Database**.
2. Select the antivirus database the FortiGate unit will use as the default database to perform antivirus scanning of your network traffic.
3. Select **Apply**.

**To change the antivirus database — CLI**

```
config antivirus settings
  set default-db extended
end
```

**Overriding the default antivirus database**

The default antivirus database is used for all antivirus scanning. If you have a particular policy or traffic type that requires scanning using a different antivirus database, you can override the default database. Antivirus database overrides are applied to individual traffic types in an antivirus profile. The override will affect only the traffic types to which the override is applied for the traffic handled by the firewall policy the antivirus profile is applied to. Antivirus database overrides can be set using only the CLI.

In this example, a database override is applied to HTTP traffic in a protocol options profile named `web_traffic`. The flow-based database is specified.
To override the default antivirus database — CLI

```
config antivirus profile
  edit web-traffic
    config http
      set avdb flow-based
    end
  end
end
```

With this configuration, the flow-based database is used for antivirus scans on HTTP traffic controlled by firewall policies in which this antivirus profile is selected. Other traffic types will use the default database, as specified in UTM > AntiVirus > Virus Database.

Adding the antivirus profile to a firewall policy

This procedure is required only if your antivirus profile does not yet belong to a firewall policy. You need to add the antivirus profile to a policy before any antivirus profile settings can take effect.

To add the antivirus profile to a policy

1. Go to Firewall > Policy.
2. Select Create New to add a new policy, or select the Edit icon of the firewall policy to which you want to add the profile.
3. Enable UTM.
4. Select Enable AntiVirus and select the antivirus profile that contains the quarantine configuration.
5. Select OK to save the firewall policy.

Configuring the scan buffer size

When checking files for viruses using the proxy-based scanning method, there is a maximum file size that can be buffered. Files larger than this size are passed without scanning. The default size for all FortiGate models is 10 megabytes. Archived files are extracted and email attachments are decoded before the FortiGate unit determines if they can fit in the scan buffer. For example, a 7 megabyte ZIP file containing a 12 megabyte EXE file will be passed without scanning with the default buffer size. Although the archive would fit within the buffer, the uncompressed file size will not.

In this example, the `uncompsizelimit` CLI command is used to change the scan buffer size to 20 megabytes for files found in HTTP traffic:

```
config antivirus service http
  set uncompsizelimit 20
end
```

The maximum buffer size varies by model. Enter `set uncompsizelimit ?` to display the buffer size range for your FortiGate unit.

Note: Flow-based scanning does not use a buffer and therefore has no file-size limit. File data is scanned as it passes through the FortiGate unit. The `uncompsizelimit` setting has no effect for flow-based scanning.
Configuring archive scan depth

The antivirus scanner will open archives and scan the files inside. Archives within other archives, or nested archives, are also scanned to a default depth of twelve nestings. You can adjust the number of nested archives to which the FortiGate unit will scan with the uncompnestlimit CLI command. Further, the limit is configured separately for each traffic type.

For example, this CLI command sets the archive scan depth for SMTP traffic to 5. That is, archives within archives will be scanned five levels deep.

```
config antivirus service smtp
  set uncompnestlimit 5
end
```

You can set the nesting limit from 2 to 100.

Configuring a maximum allowed file size

The protocol option profile allows you to enforce a maximum allowed file size for each of the network protocols in the profile. They are HTTP, FTP, IMAP, POP3, SMTP, IM, and NNTP. If your FortiGate unit supports SSL content scanning and inspection, you can also configure a maximum file size for HTTPS, IMAPS, POP3S, and SMTPS.

The action you set determines what the FortiGate unit does with a file that exceeds the oversized file threshold. Two actions are available:

<table>
<thead>
<tr>
<th>Block</th>
<th>Files that exceed the oversize threshold are dropped and a replacement message is sent to the user instead of the file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>Files exceed the oversized threshold are allowed through the FortiGate unit to their destination. Note that passed files are not scanned for viruses. File Filtering, both file pattern and file type, are applied, however.</td>
</tr>
</tbody>
</table>

You can also use the maximum file size to help secure your network. If you’re using a proxy-based virus scan, the proxy scan buffer size limits the size of the files that can be scanned for infection. Files larger than this limit are passed without scanning. If you configure the maximum file size to block files larger than the scan buffer size, large infected files will not by-pass antivirus scanning.

In this example, the maximum file size will be configured to block files larger than 10 megabytes, the largest file that can be antivirus scanned with the default settings. You will need to configure a protocol options profile and add it to a firewall policy.

Create a protocol options profile to block files larger than 10 MB

1. Go to Firewall > Policy > Protocol Options.
2. Select Create New.
3. Enter 10MB_Block for the protocol options policy name.
4. For the comment, enter Files larger than 10MB are blocked.
5. Expand each protocol listed and select Block for the Oversized File/Email setting. Also confirm that the Threshold is set to 10.
6. Select OK.

The protocol options profile is configured, but to block files, you must select it in the firewall profiles handling the traffic that contains the files you want blocked.
To select the protocol options profile in a firewall policy

1. Go to Firewall > Policy > Policy.
2. Select a firewall policy.
3. Select the Edit icon.
4. Enable UTM.
5. Select Protocol Options.
6. Select 10MB_Block from the Protocol Options list.
7. Select OK to save the firewall policy.

Once you complete these steps, any files in the traffic handled by this policy that are larger than 10MB will be blocked. If you have multiple firewall policies, examine each to determine if you want to apply similar file blocking the them as well.

Configuring client comforting

When proxy-based antivirus scanning is enabled, the FortiGate unit buffers files as they are downloaded. Once the entire file is captured, the FortiGate unit scans it. If no infection is found, the file is sent along to the client. The client initiates the file transfer and nothing happens until the FortiGate finds the file clean, and releases it. Users can be impatient, and if the file is large or the download slow, they may cancel the download, not realizing that the transfer is in progress.

The client comforting feature solves this problem by allowing a trickle of data to flow to the client so they can see the file is being transferred. The default client comforting transfer rate sends one byte of data to the client every ten seconds. This slow transfer continues while the FortiGate unit buffers the file and scans it. If the file is infection-free, it is released and the client will receive the remainder of the transfer at full speed. If the file is infected, the FortiGate 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, 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.

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.

Client comforting is available for HTTP and FTP traffic. If your FortiGate unit supports SSL content scanning and inspection, you can also configure client comforting for HTTPS traffic.

Enable and configure client comforting

1. Go to Firewall > Policy > Protocol Options.
2. Select a protocol options profile and choose Edit, or select Create New to make a new one.
3. Expand HTTP, FTP, and if your FortiGate unit supports SSL content scanning and inspection, expand HTTPS as well.
4. To enable client comforting, select Comfort Clients for each of the protocols in which you want it enabled.
5. Select OK to save the changes.
6. Select this protocol options profile in any firewall policy for it to take effect on all traffic handled by the policy.

The default values for Interval and Amount are 10 and 1, respectively. This means that when client comforting takes effect, 1 byte of the file is sent to the client every 10 seconds. You can change these values to vary the amount and frequency of the data transferred by client comforting.

Enable the file quarantine

You can quarantine blocked and infected files if you have a FortiGate unit with a local hard disk. You can view the file name and status information about the file in the Quarantined Files list and submit specific files and add file patterns to the AutoSubmit list so they will automatically be uploaded to the FortiGuard AntiVirus service for analysis.

FortiGate units can also quarantine blocked and infected files to a FortiAnalyzer unit. Files stored on the FortiAnalyzer unit can also be viewed from the Quarantined Files list in the FortiGate unit.

General configuration steps

The following steps provide an overview of the file quarantine configuration. For best results, follow the procedures in the order given. Note that if you perform any additional actions between procedures, your configuration may have different results.

1. Go to UTM > AntiVirus > Quarantine to configure the quarantine service and destination.
2. Go to UTM > AntiVirus > Profile and edit an existing antivirus profile or create a new one. In the Quarantine row, select the check boxes of the protocols for which you want the quarantine enabled. The Quarantine option only appears if your FortiGate unit has a local disk or if your FortiGate unit is configured to use a FortiAnalyzer unit to quarantine files.

   Note: Antivirus profiles also have a configurable feature called Quarantine Virus Sender (to Banned User List). This is a different feature unrelated to the Quarantine option.

3. If you have not previously done so, go to Firewall > Policy and add the antivirus profile to a firewall policy.

Configuring the file quarantine

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.
To configure the file quarantine

1. Go to UTM > AntiVirus > Quarantine.

2. In the options table, select the files to quarantine.
   - The options table lists three detection methods used to find potentially problematic files, as well as the types of traffic scanned for these files. Select one or more check boxes for the following traffic types to enable quarantine for detected files:
     - Infected Files: files in which the FortiGate unit detects virus signatures
     - Suspicious Files: files detected by the heuristics scanner
     - Blocked Files: files matching patterns or types defined in a file filter.

3. In the Max Filesize to Quarantine field, enter the maximum file size to quarantine, in megabytes. Files that exceed this size limit are not quarantined.

4. In the Age Limit field, enter the number of hours quarantined files will be saved. Files older than the specified number of hours are deleted.

5. Select OK.

Viewing quarantined files

The Quarantined Files list displays information about each quarantined file. You can sort the files by file name, date, service, status, duplicate count (DC), or time to live (TTL). You can also filter the list to view only quarantined files from a specific service.

To view quarantined files, go to Log&Report > Quarantined Files.

Downloading quarantined files

You can download any non-expired file from the quarantine. You may want to do so if it was quarantined as the result of a false positive or if you want to examine the contents.

To download a quarantined file

1. Go to Log&Report > Quarantined Files.

2. In the quarantine file list, find the file you want to download.
   - To find the file more quickly, use the Sort by function to change the sort order. Available sort criteria include status, services, file name, date, TTL, and duplicate count. You can also use the Filter function to display the files quarantined from an individual traffic type.

3. Select the Download icon to save a copy of the quarantined file on your computer.
Enable file filtering

Enable file filtering is a feature that allows you to block files based on their file name or their type.

- **File patterns** are a means of filtering based purely on the names of files. They may include wildcards (*). For example, blocking *.scr will stop all files with an scr file extension, which is commonly used for Windows screen saver files. Files trying to pass themselves off as Windows screen saver files by adopting the file-naming convention will also be stopped.

  Files can specify the full or partial file name, the full or partial file extension, or any combination. File pattern entries are not case sensitive. For example, adding *.exe to the file pattern list also blocks any files ending with .EXE.

  Files are compared to the enabled file patterns from top to bottom, in list order.

  In addition to the built-in patterns, you can specify more file patterns to block. For details, see "Creating a file filter list" on page 59.

- **File types** are a means of filtering based on an examination of the file contents, regardless of the file name. If you were to block the file type Archive (zip), all zip archives would be blocked even if they were renamed to have a different file extension. The FortiGate examines the file contents to determine what type of file it is and then acts accordingly.

  The FortiGate unit can take either of the following actions toward the files that match a configured file pattern or type:

  - **Block**: the file will be blocked and a replacement messages will be sent to the user. If both file pattern filtering and virus scan are enabled, the FortiGate unit blocks files that match the enabled file filter and does not scan these files for viruses.

  - **Allow**: the file will be allowed to pass.

  The FortiGate unit also writes a message to the virus log and sends an alert email message if configured to do so.

  **Note**: File filter does not detect files within archives. You can use file filter to block or allow the archives themselves, but not the contents of the archives.

General configuration steps

The following steps provide an overview of the file filtering configuration. For best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create a file filter list.
2. Create one or more file patterns or file types to populate the file filter list.
3. Enable the file filter list by adding it to a firewall policy.

Creating a file filter list

Before your FortiGate unit can filter files by pattern or type, you must create a file filter list.

**To create a file filter list**

1. Go to **UTM > AntiVirus > File Filter**.
2. Select **Create New**.
3. Enter a **Name** for the new file filter list.
4. Select **OK**.
The new list is created and the edit file filter list window appears. The new list is empty. You need to populate it with one or more file patterns or file types.

**Creating a file pattern**

A file pattern allows you to block or allow files based on the file name. File patterns are created within file filter lists.

*To create a file pattern*

1. Go to UTM > AntiVirus > File Filter.
2. Select a file filter list.
3. Select the Edit icon.
4. Select Create New.
5. Select File Name Pattern as the Filter Type.
6. Enter the pattern in the Pattern field. The file pattern can be an exact file name or can include wildcards (*). The file pattern is limited to a maximum of 80 characters.
7. Select the action the FortiGate unit will take when it discovers a matching file: Allow or Block.
8. The filter is enabled by default. Clear the Enable check box if you want to disable the filter.
9. Select OK.

**Creating a file type**

A file type allows you to block or allow files based on the kind of file. File types are created within file filter lists.

*To create a file type*

1. Go to UTM > AntiVirus > File Filter.
2. Select the Edit icon of the file filter list to which you will add the file type.
3. Select Create New.
4. Select File Type as the Filter Type.
5. Select the kind of file from the File Type list.
6. Select the action the FortiGate unit will take when it discovers a matching file: Allow or Block.
7. The filter is enabled by default. Clear the Enable check box if you want to disable the filter.
8. Select OK.

**Enabling file filtering in a profile**

You need to add a file filter list to an antivirus profile to enable file filtering.

*To enable file filtering*

1. Go to UTM > AntiVirus > Profile.
2. Select Create New to add an antivirus profile or select the Edit icon of an existing one for which you want to enable file filtering.
3. In the row labeled File Filter, select the check boxes associated with the traffic you want scanned for files.
4. At the end of the File Filter row, select the file filter list containing the file types and patterns that the FortiGate unit will scan.

5. Select OK.

You also need to add the antivirus profile to a firewall policy for all settings to take effect. For more information, see “Adding the antivirus profile to a firewall policy” on page 54.

Enable grayware scanning

Grayware programs are unsolicited software programs installed on computers, often without the user’s consent or knowledge. Grayware programs are generally considered an annoyance, but they can also cause system performance problems or be used for malicious purposes.

To allow the FortiGate unit to scan for known grayware programs, you must enable both antivirus scanning and grayware detection. By default, grayware detection is disabled. To enable antivirus scanning, see “Enable antivirus scanning” on page 52.

To enable grayware detection — web-based manager

1. Go to UTM > AntiVirus > Virus Database.
2. Select Enable Grayware Detection.

To enable grayware detection — CLI

```
config antivirus settings
  set grayware enable
end
```

With grayware detection enabled, the FortiGate unit will scan for grayware any time it checks for viruses.

Testing your antivirus configuration

You have configured your FortiGate unit to stop viruses, but you’d like to confirm your settings are correct. Even if you have a real virus, it would be dangerous to use for this purpose. An incorrect configuration will allow the virus to infect your network.

To solve this problem, the European Institute of Computer Anti-virus Research has developed a test file that allows you to test your antivirus configuration. The EICAR test file is not a virus. It cannot infect computers, nor can it spread or cause any damage. It’s a very small file that contains a sequence of characters. Your FortiGate unit recognizes the EICAR test file as a virus so you can safely test your FortiGate unit antivirus configuration.

Go to http://www.fortiguard.com/antivirus/eicartest.html to download the test file (eicar.com) or the test file in a ZIP archive (eicar.zip).

If the antivirus profile applied to the firewall policy that allows you access to the Web is configured to scan HTTP traffic for viruses, any attempt to download the test file will be blocked. This indicates that you are protected.

Antivirus examples

The following examples provide a sample antivirus configuration scenario for a fictitious company.
Configuring simple antivirus protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable antivirus protection on a FortiGate unit located in a satellite office. The satellite office does not have an internal email server. To send and retrieve email, the employees connect to an external mail server.

Creating an antivirus profile

Most antivirus settings are configured in an antivirus profile. Antivirus profiles are selected in firewall policies. This way, you can create multiple antivirus profiles, and tailor them to the traffic controlled by the firewall policy in which they are selected. In this example, you will create one antivirus profile.

To create an antivirus profile — web-based manager

1. Go to UTM > AntiVirus > Profile.
2. Select Create New.
3. In the Name field, enter basic_antivirus.
4. In the Comments field, enter Antivirus protection for web and email traffic.
5. Select the Virus Scan check boxes for the HTTP, IMAP, POP3, and SMTP traffic types.
6. Select OK to save the antivirus profile.

To create an antivirus profile — CLI

```
config antivirus profile
edit basic_antivirus
   set comment "Antivirus protection for web and email traffic"
config http
   set options scan
end
config imap
   set options scan
end
config pop3
   set options scan
end
config smtp
   set options scan
end
end
```

Selecting the antivirus profile in a firewall policy

An antivirus profile directs the FortiGate unit to scan network traffic only when it is selected in a firewall policy. When an antivirus profile is selected in a firewall policy, its settings are applied to all the traffic the firewall policy handles.

To select the antivirus profile in a firewall policy — web-based manager

1. Go to Firewall > Policy > Policy.
2. Select a policy.
3. Select the Edit icon.
4 Enable UTM.

5 Select default from the Protocol Options list.
   UTM can not be enabled without selecting a protocol options profile. A default profile is provided.

6 Select the Enable AntiVirus option.

7 Select the basic_antivirus profile from the list.

8 Select OK to save the firewall policy.

To select the antivirus profile in a firewall policy — CLI

```
config firewall policy
edit 1
   set utm-status enable
   set profile-protocol-options default
   set av-profile basic_antivirus
end
```

HTTP, IMAP, POP3, and SMTP traffic handled by the firewall policy you modified will be scanned for viruses. A small office may have only one firewall policy configured. If you have multiple policies, consider enabling antivirus scanning for all of them.

Protecting your network against malicious email attachments

Viruses and grayware are commonly delivered by email or the web. The Example.com corporation has been the victim of multiple virus infections in the past. Now that the company has a FortiGate unit protecting its network, you (Example.com’s system administrator) can configure the unit to scan email and web traffic to filter out harmful attachments. Example.com’s FortiGate unit supports SSL content scanning and inspection.

Enabling antivirus scanning in the antivirus profile

The primary means to avoid viruses is to configure the FortiGate unit to scan email and web traffic for virus signatures. You enable virus scanning in the antivirus profile and then select the antivirus profile in firewall policies that control email traffic.

To enable antivirus scanning in the antivirus profile

1 Go to UTM > AntiVirus > Profile.

2 Select Create New to add a new antivirus profile, or select the Edit icon of an existing antivirus profile.

3 Select the Virus Scan check box for HTTP to scan web traffic for viruses.

4 Select the Virus Scan check box for IMAP, POP3, and SMTP to scan all email protocols for viruses.

5 Select OK to save the antivirus profile.
Enabling grayware scanning

Grayware can also threaten Example.com’s network. Viruses, email messages and the web are often the means by which grayware infections are delivered.

To enable grayware scanning

1. Go to UTM > AntiVirus > Virus Database.
2. Select Enable Grayware Detection.
3. Select Apply.

When Enable Grayware Detection is selected, virus scanning will also include grayware scanning. Any traffic scanned for viruses will also be scanned for grayware.

Configuring and enabling file filtering

Executable files are never sent or received at Example.com. Since many executable files attached to spam messages install malware or infect the system with viruses, Example.com decided to stop all executable files attached to email messages by using file filters.

Creating the file filtering list

1. Go to UTM > AntiVirus > File Filter.
2. Select Create New.
3. Enter a name for the new file filter list.
4. Optionally, enter a descriptive comment for the list.
5. Select OK to save the new list.
6. Select Create New to add an entry to the file pattern list.
7. For Filter Type, select File Type.
8. For File Type, select Executable (exe).
9. For Action, select Block.
10. Select OK to save the new file filter list entry.
11. Select OK to save the file filter list.

With the file filter list created, you must now enable file filtering in the antivirus profile and select the list.

Enabling file filter

1. Go to UTM > AntiVirus > Profile.
2. Select the antivirus profile in which you already enabled virus scanning and choose Edit.
3. Select the File Filter check box for IMAP, POP3, and SMTP to scan all email protocols for viruses.
4. At the end of the File Filter row, select the file filter list you created.
5. Select OK.

To complete the example, you also need to add the antivirus profile to a firewall policy for all settings to take effect.
Selecting the antivirus profile in a firewall policy

An antivirus profile directs the FortiGate unit to scan network traffic only when it is selected in a firewall policy. When an antivirus profile is selected in a firewall policy, its settings are applied to all the traffic the firewall policy handles.

To select the antivirus profile in a firewall policy

1. Go to Firewall > Policy > Policy.
2. Select the policy that controls the network traffic controlling email traffic.
3. Select the Edit icon.
4. Enable UTM.
5. Select default from the Protocol Options list.
   UTM can not be enabled without selecting a protocol options profile. A default profile is provided.
6. Select the Enable AntiVirus option.
7. Select the antivirus profile from the list.
8. Select OK to save the firewall policy.
Email filter

This section describes how to configure FortiGate email filtering for IMAP, POP3, and SMTP email. Email filtering includes both spam filtering and filtering for any words or files you want to disallow in email messages. If your FortiGate unit supports SSL content scanning and inspection, you can also configure spam filtering for IMAPS, POP3S, and SMTPS email traffic.

The following topics are included in this section:

- Email filter concepts
- Enable email filter
- Configure the spam action
- Configure the tag location
- Configure the tag format
- Email filter examples

Email filter concepts

You can configure the FortiGate unit to manage unsolicited commercial email by detecting and 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 Antispam email filter profile settings, you can enable IP address checking, URL checking, email checksum checking, and spam submission. Updates to the IP reputation and spam signature databases are provided continuously via the global FortiGuard Distribution Network.

From the FortiGuard Antispam Service page in the FortiGuard Center, you can find out 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.

Email filter techniques

The FortiGate unit has a number of techniques available to help detect spam. Some use the FortiGuard Antispam Service and require a subscription. The remainder use your DNS servers or use lists that you must maintain.

FortiGuard IP address check

The FortiGate unit queries the FortiGuard Antispam Service to determine if the IP address of the client delivering the email is blacklisted. A match will cause the FortiGate unit to treat delivered messages as spam.

The default setting of the `smtp-spamhdrip` CLI command is `disable`. If enabled, the FortiGate unit will check all the IP addresses in the header of SMTP email against the FortiGuard Antispam Service. For more information, see the FortiGate CLI Reference.
**FortiGuard URL check**

The FortiGate unit queries the FortiGuard Antispam service to determine if any URL in the message body is associated with spam. If any URL is blacklisted, the FortiGate unit determines that the email message is spam.

**FortiGuard email checksum check**

The FortiGate unit sends a hash of an email to the FortiGuard Antispam server, which compares the hash to hashes of known spam messages stored in the FortiGuard Antispam database. If the hash results match, the email is flagged as spam.

**FortiGuard spam submission**

Spam submission is a way you can inform the FortiGuard AntiSpam service of non-spam messages incorrectly marked as spam. When you enable this setting, the FortiGate unit adds a link to the end of every message marked as spam. You then select this link to inform the FortiGuard AntiSpam service when a message is incorrectly marked.

**IP address black/white list check**

The FortiGate unit compares the IP address of the client delivering the email to the addresses in the IP address black/white list specified in the email filter profile. If a match is found, the FortiGate unit will take the action configured for the matching black/white list entry against all delivered email.

The default setting of the `smtp-spamhdr` CLI command is `disable`. If enabled, the FortiGate unit will check all the IP addresses in the header of SMTP email against the specified IP address black/white list. For more information, see the [FortiGate CLI Reference](http://docs.fortinet.com/).

**HELO DNS lookup**

The FortiGate unit takes the domain name specified by the client in the HELO greeting sent when starting the SMTP session and does a DNS lookup to determine if the domain exists. If the lookup fails, the FortiGate unit determines that any messages delivered during the SMTP session are spam.

**Email address black/white list check**

The FortiGate unit compares the sender email address, as shown in the message envelope `MAIL FROM`, to the addresses in the email address black/white list specified in the email filter profile. If a match is found, the FortiGate unit will take the action configured for the matching black/white list entry.

**Return email DNS check**

The FortiGate unit performs a DNS lookup on the reply-to domain to see if there is an A or MX record. If no such record exists, the message is treated as spam.

**Banned word check**

The FortiGate unit blocks email messages based on matching the content of the message with the words or patterns in the selected spam filter banned word list.

**Order of spam filtering**

The FortiGate unit checks for spam using various filtering techniques. The order in which the FortiGate 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 spam filter passes the email to the next if no matches or problems are found. If the action in the filter is *Mark as Spam*, the FortiGate unit tags the email as spam 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 spam filtering**

The FortiGate unit scans SMTP and SMTPS email for spam in the order given below. SMTPS spam filtering is available on FortiGate units that support SSL content scanning and inspection.

1. IP address black/white list (BWL) check on last hop IP
2. DNSBL & ORDBL check on last hop IP, FortiGuard Antispam IP check on last hop IP, HELO DNS lookup
3. MIME headers check, E-mail address BWL check
4. Banned word check on email subject
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Banned word check on email body
7. Return email DNS check, FortiGuard Antispam email checksum check, FortiGuard Antispam URL check, DNSBL & ORDBL check on public IP extracted from header.

**Order of IMAP, POP3, IMAPS and POP3S spam filtering**

The FortiGate unit scans IMAP, POP3, IMAPS and POP3S email for spam in the order given below. IMAPS and POP3S spam filtering is available on FortiGate units that support SSL content scanning and inspection.

1. MIME headers check, E-mail address BWL check
2. Banned word check on email subject
3. IP BWL check
4. Banned word check on email body
5. Return email DNS check, FortiGuard Antispam email checksum check, FortiGuard Antispam URL check, DNSBL & ORDBL check.

**Enable email filter**

Unlike antivirus protection, no single control enables all email filtering. Your FortiGate unit uses many techniques to detect spam; some may not be appropriate for every situation.

To enable any of the email filtering options, however, you must allow the FortiGate unit to inspect email traffic.
To enable email traffic inspection
1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to enable email traffic inspection and choose Edit.
3. The top row lists each type of email traffic the FortiGate unit is capable of inspecting. Select the check box for the traffic types you want the FortiGate unit to inspect.
4. Select OK.

Once you allow the FortiGate unit to examine one or more types of email traffic, you can enable any of the individual email filtering techniques.

Enabling FortiGuard IP address checking
When you enable FortiGuard IP address checking, your FortiGate unit will submit the IP address of the client to the FortiGuard service for checking. If the IP address exists in the FortiGuard IP address black list, your FortiGate unit will treat the message as spam.

To enable FortiGuard IP address checking
1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to enable FortiGuard IP address checking and choose Edit.
3. Under the heading FortiGuard Email Filtering, the IP Address Check row has check boxes for each email traffic type. Select the types of traffic you want scanned.
4. Select OK.

Select the edited email filter profile in a firewall policy, and the traffic controlled by the firewall policy will be scanned according to the settings you configured. You may select the email filter profile in more than one firewall policy if required.

Enabling FortiGuard URL checking
When you enable FortiGuard IP address checking, your FortiGate unit will submit all URLs appearing in the email message body to the FortiGuard service for checking. If a URL exists in the FortiGuard URL black list, your FortiGate unit will treat the message as spam.

To enable FortiGuard URL checking
1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to enable FortiGuard URL checking and choose Edit.
3. Under the heading FortiGuard Email Filtering, the URL Check row has check boxes for each email traffic type. Select the types of traffic you want scanned.
4. Select OK.

Select the edited email filter profile in a firewall policy, and the traffic controlled by the firewall policy will be scanned according to the settings you configured. You may select the email filter profile in more than one firewall policy if required.

Enabling FortiGuard email checksum checking
When you enable FortiGuard email checksum checking, your FortiGate unit will submit a checksum of each email message to the FortiGuard service for checking. If a checksum exists in the FortiGuard checksum black list, your FortiGate unit will treat the message as spam.
To enable FortiGuard checksum checking

1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to enable FortiGuard checksum checking and choose Edit.
3. Under the heading FortiGuard Email Filtering, the E-mail Checksum Check row has check boxes for each email traffic type. Select the types of traffic you want scanned.
4. Select OK.

Select the edited email filter profile in a firewall policy, and the traffic controlled by the firewall policy will be scanned according to the settings you configured. You may select the email filter profile in more than one firewall policy if required.

Enabling FortiGuard spam submission

When you enable FortiGuard email checksum checking, your FortiGate unit will append a link to the end of every message detected as spam. This link allows email users to “correct” the FortiGuard service by informing it that the message is not spam.

**Note:** Carefully consider the use of the Spam submission option on email leaving your network. Users not familiar with the feature may click the link on spam messages because they are curious. This will reduce the accuracy of the feature.

To enable FortiGuard Spam submission

1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to enable FortiGuard spam submission and choose Edit.
3. Under the heading FortiGuard Email Filtering, the Spam Submission row has check boxes for each email traffic type. Select the types of traffic you want processed.
4. Select OK.

Select the edited email filter profile in a firewall policy, and the traffic controlled by the firewall policy will be scanned according to the settings you configured. You may select the email filter profile in more than one firewall policy if required.

Enabling IP address black/white list checking

When you enable IP address black/white list checking, your FortiGate unit will compare the client IP address with the IP address black/white list specified in the email filter profile. If the client IP address exists, the FortiGate unit acts according to the action configured for the IP address in the list: allow the message, reject it, or mark it as spam.

The next two topics describe adding and configuring the IP address black/white list that you will need before you can enable the checking. If you already have this list, go to “Enabling the IP address black/white list checking” on page 72.

Creating an IP address black/white list

Before you can enable IP address black/white list spam filtering in the email filter profile, you must create an IP address black/white list.

To create an IP address black/white list

1. Go to UTM > Email Filter > IP Address.
2. Select Create New.
3. Enter a name for the IP address list.
4 Optionally, enter a description or comments about the list.
5 Select OK to save the IP address black/white list.

When a new IP address back/white list is created, it is empty. To perform any actions, you must add IP addresses to the list.

Adding addresses to an IP address black/white list

Each IP address black/white list contains a number of IP addresses, each having a specified action. When the FortiGate unit accepts mail from a client with an IP address on the IP address black/white list specified in the active email filter profile, it performs the action specified for the address.

To add an address to an IP address black/white list
1 Go to UTM > Email Filter > IP Address.
2 Select the list to which you want to add an address and choose Edit.
3 Select Create New.
4 Enter the address or netmask in the IP/netmask field.
5 Select the action:
   • Mark as Clear: Messages from clients with matching IP addresses will be allowed, bypassing further email filtering.
   • Mark as Reject: Messages from clients with matching IP addresses will be rejected. The FortiGate unit will return a reject message to the client. Mark as Reject only applies to mail delivered by SMTP. If an IP address black/white list is used with POP3 or IMAP mail, addresses configured with the Mark as Reject action will be marked as spam.
   • Mark as Spam: Messages from clients with matching IP addresses will be treated as spam, subject to the action configured in the applicable email filter profile. For more information, see “Configure the spam action” on page 78.
6 By default, the address is enabled and the FortiGate unit will perform the action if the address is detected. To disable checking for the address, clear the Enable check box.
7 Select OK.

Enabling the IP address black/white list checking

Once you have created a black/white list and added the IP addresses, you can enable the checking.

To enable IP address black/white list checking
1 Go to UTM > Email Filter > Profile.
2 Select the email filter profile in which you want to enable IP address black/white list checking and choose Edit.
3 The IP Address BWL Check row has check boxes for each email traffic type. Select the types of traffic you want scanned.
4 Select the IP address black/white list to use from the drop-down list at the end of the row.
5 Select OK.

Select the edited email filter profile in a firewall policy, and the traffic controlled by the firewall policy will be scanned according to the settings you configured. You may select the email filter profile in more than one firewall policy if required.
Enabling HELO DNS lookup

Whenever a client opens an SMTP session with a server, the client sends a HELO command with the client domain name. When you enable HELO DNS lookup, your FortiGate unit will take the domain the client submits as part of the HELO greeting and send it to the configured DNS. If the domain does not exist, your FortiGate unit will treat all messages the client delivers as spam.

The HELO DNS lookup is available only for SMTP traffic.

To enable HELO DNS lookup

1. Go to UTM > Email Filter > Profile.
2. Select the Edit icon of the email filter profile in which you want to enable HELO DNS lookup.
3. The HELO DNS Lookup row has a check box for the SMTP traffic type. Select the check box to enable HELO DNS lookup.
4. Select OK.

Select the edited email filter profile in a firewall policy, and the traffic controlled by the firewall policy will be scanned according to the settings you configured. You may select the email filter profile in more than one firewall policy if required.

Enabling email address black/white list checking

When you enable email address black/white list checking, your FortiGate unit will compare the sender email address with the email address black/white list specified in the email filter profile. If the sender email address exists, the FortiGate unit acts according to the action configured for the email address in the list: allow the message or mark it as spam.

The next two topics describe adding and configuring the email address black/white list that you will need before you can enable the checking. If you already have this list, go to "Enabling email address black/white list checking" on page 74.

Creating an email address black/white list

Before you can enable email address black/white list spam filtering in the email filter profile, you must create an email address black/white list.

To create an email address black/white list

1. Go to UTM > Email Filter > E-mail Address.
2. Select Create New.
3. Enter a name for the email address list.
4. Optionally, enter a description or comments about the list.
5. Select OK to save the email address black/white list.

When a new IP address back/white list is created, it is empty. To perform any actions, you must add email addresses to the list.

Adding addresses to an email address black/white list

Each email address black/white list may contain a number of email addresses, each having a specified action. When the FortiGate unit accepts an email message from a client with a reply-to address that appears in the email address black/white list specified in the active email filter profile, it performs the action specified for the email message.
To add an address to an email address black/white list

1. Go to UTM > Email Filter > E-mail Address.
2. Select the Edit icon of the list to which you want to add an address.
3. Select Create New.
4. Enter the email address in the Email Address field.
5. If you need to enter a pattern in the Email Address field, select whether to use wildcards or regular expressions to specify the pattern.
   - Wildcard uses an asterisk ("*"), to match any number of any character. For example, *@example.com will match all addresses ending in @example.com.
   - Regular expressions use Perl regular expression syntax. See http://perldoc.perl.org/perlretut.html for detailed information about using Perl regular expressions.
6. Select the action:
   - Mark as Spam: Messages with matching reply-to email addresses will be treated as spam, subject to the action configured in the applicable email filter profile. For more information, see "Configure the spam action" on page 78.
   - Mark as Clear: Messages with matching reply-to addresses will be allowed, bypassing further email filtering.
7. By default, the address is enabled and the FortiGate unit will perform the action if the address is detected. To disable checking for the address, clear the Enable check box.
8. Select OK to save the address.

Enabling email address black/white list checking

Once you have created a black/white list and added the email addresses, you can enable the checking.

To enable email address black/white list checking

1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to enable email address black/white list checking and choose Edit.
3. The E-mail Address BWL Check row has check boxes for each email traffic type. Select the types of traffic you want scanned.
4. Select the email address black/white list to use from the drop-down list at the end of the row.
5. Select OK.

Select the edited email filter profile in a firewall policy, and the traffic controlled by the firewall policy will be scanned according to the settings you configured. You may select the email filter profile in more than one firewall policy if required.

Enabling return email DNS checking

When you enable return email DNS checking, your FortiGate unit will take the domain in the reply-to email address and send it to the configured DNS. If the domain does not exist, your FortiGate unit will treat the message as spam.
To enable return email DNS check

1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to enable return email DNS checking and choose Edit.
3. The Return E-mail DNS Check row has check boxes for each email traffic type. Select the types of traffic you want checked.
4. Select OK.

Select the edited email filter profile in a firewall policy, and the traffic controlled by the firewall policy will be scanned according to the settings you configured. You may select the email filter profile in more than one firewall policy if required.

Enabling banned word checking

When you enable banned word checking, your FortiGate unit will examine the email message for words appearing in the banned word list specified in the email filter profile. If the total score of the banned word discovered in the email message exceeds the threshold value set in the email filter profile, your FortiGate unit will treat the message as spam.

When determining the banned word score total for an email message, each banned word score is added once no matter how many times the word appears in the message.

The next two topics describe adding and configuring the banned word list that you will need before you can enable the checking. If you already have this list, go to “Enabling banned word checking” on page 77.

How content is evaluated

Every time the banned word filter detects a pattern in an email message, it adds the pattern score to the sum of scores for the message. You set this score when you create a new pattern to block content. The score can be any number from zero to 99999. Higher scores indicate more offensive content. When the total score equals or exceeds the threshold, the email message is considered as spam and treated according to the spam action configured in the email filter profile. The score for each pattern is counted only once, even if that pattern appears many times in the email message. The default score for banned word patterns is 10 and the default threshold is 10. This means that by default, an email message is blocked by a single match.

A pattern can be part of a word, a whole word, or a phrase. Multiple words entered as a pattern are treated as a phrase. The phrase must appear as entered to match. You can also use wildcards or regular expressions to have a pattern match multiple words or phrases.

For example, the FortiGate unit scans an email message that contains only this sentence: “The score for each word or phrase is counted only once, even if that word or phrase appears many times in the email message.”
In this example, the message is treated as spam if the banned word threshold is set to 60 or less.

Creating a banned word list

Before you can enable IP address black/white list spam filtering in the email filter profile, you must create an IP address black/white list.

To create an IP address black/white list

1. Go to UTM > Email Filter > Banned Word.
2. Select Create New.
3. Enter a name for the banned word list.
4. Optionally, enter a description or comments about the list.
5. Select OK to save the banned word list.

When a new banned word list is created, it is empty. To perform any actions, you must add words to the list.

Adding words to a banned word list

Each banned word list contains a number of words, each having a score, and specifying whether the email FortiGate unit will search for the word in the message subject, message body, or both.

When the FortiGate unit accepts an email message containing one or more words in the banned word list specified in the active email filter profile, it totals the scores of the banned words in the email message. If the total is higher than the threshold set in the email filter profile, the email message will be detected as spam. If the total score is lower than the threshold, the message will be allowed to pass as normal.

The score of a banned word present in the message will be counted toward the score total only once, regardless of how many times the word appears in the message.

<table>
<thead>
<tr>
<th>Banned word pattern</th>
<th>Pattern type</th>
<th>Assigned score</th>
<th>Score added to the sum for the entire page</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>word</td>
<td>Wildcard</td>
<td>20</td>
<td>20</td>
<td>The pattern appears twice but multiple occurrences are only counted once.</td>
</tr>
<tr>
<td>word phrase</td>
<td>Wildcard</td>
<td>20</td>
<td>0</td>
<td>Although each word in the phrase appears in the message, the words do not appear together as they do in the pattern. There are no matches.</td>
</tr>
<tr>
<td>word*phrase</td>
<td>Wildcard</td>
<td>20</td>
<td>20</td>
<td>The wildcard represents any number of any character. A match occurs as long as “word” appears before “phrase” regardless of what is in between them.</td>
</tr>
<tr>
<td>mail*age</td>
<td>Wildcard</td>
<td>20</td>
<td>20</td>
<td>Since the wildcard character can represent any characters, this pattern is a match because “email message” appears in the message.</td>
</tr>
</tbody>
</table>
To add words to a banned word list
1. Go to UTM > Email Filter > Banned Word.
2. Select the Edit icon of the list to which you want to add a word.
3. Select Create New.
4. Enter the word or the pattern in the Pattern field.
5. In the Pattern Type field, select whether you use wildcards or regular expressions. 
   * Wildcard uses an asterisk ("*") to match any number of any character. For example, re* will match all words starting with “re”.
6. In the Language field, select the language.
7. Select where the FortiGate unit will check for the banned word. The options are Body, Subject, or All, which combines the other two options.
8. Enter a score. If the word appears in the message as determined by the Where setting, the score is added to the scores of all the other banned words appearing in the email message. If the score total is higher than the threshold set in the email filter profile, the email message will be detected as spam. If the total score is lower than the threshold, the message will be allowed to pass as normal.
9. By default, the banned word is enabled and will appear in the list. To disable checking for the banned word, clear the Enable check box.
10. Select OK to save the banned word.

Enabling banned word checking
Once you have created a black/white list and added the email addresses, you can enable the checking.

To enable banned word checking
1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to enable banned word checking and choose Edit.
3. The Banned Word Check row has check boxes for each email traffic type. Select the types of traffic you want scanned.
4. Select the banned word list to use from the drop-down list at the end of the row.
5. Enter a threshold value. If the total score of the banned words appearing in the message exceeds this threshold, the FortiGate unit treats the message as spam.
6. Select OK.
Select the edited email filter profile in a firewall policy, and the traffic controlled by the firewall policy will be scanned according to the settings you configured. You may select the email filter profile in more than one firewall policy if required.
Configure the spam action

When spam is detected, the FortiGate unit will deal with it according to the Spam Action setting in the email filter profile. Note that POP3S, IMAPS and SMTPS spam filtering is available only on FortiGate units that support SSL content scanning and inspection. POP3, IMAP, POP3S and IMAPS mail can only be tagged. SMTP and SMTPS mail can be set to Discard or Tagged:

- **Discard**: When the spam action is set to Discard, messages detected as spam are deleted. No notification is sent to the sender or recipient.
- **Tagged**: When the spam action is set to Tagged, messages detected as spam are labelled and delivered normally. The text used for the label is set in the Tag Format field and the label is placed in the subject or the message header, as set with the Tag Location option.

**To configure the spam action**

1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to configure the spam action and choose Edit.
3. The Spam Action row has a drop-down selection under the SMTP and SMTPS traffic type. Select Discard or Tagged.
   
   No selection is available for POP3, IMAP, POP3S or IMAPS traffic. Tagged is the only applicable action for those traffic types.
   
   By default, the tag location for any traffic set to Tagged is Subject and the tag format is Spam. If you want to change these settings, continue with “Configure the tag location” on page 78 and “Configure the tag format” on page 79.
4. Select OK.

Select the edited email filter profile in a firewall policy, and the traffic controlled by the firewall policy will be scanned according to the settings you configured. You may select the email filter profile in more than one firewall policy if required.

Configure the tag location

When the spam action is set to Tagged, the Tag Location setting determines where the tag is applied in the message.

**To configure the tag location**

1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to configure the tag location action and choose Edit.
3. The Tag Location row has two options for SMTP traffic. Select the tag location:
   
   - **Subject**: The FortiGate unit inserts the tag at the beginning of the message subject. For example, if the message subject is "Buy stuff!" and the tag is "[spam]", the new message subject is "[spam] Buy stuff!" if the message is detected as spam.
   
   - **MIME**: The FortiGate unit inserts the tag into the message header. With most mail readers and web-based mail services, the tag will not be visible. Despite this, you can still set up a rule based on the presence or absence of the tag.
4. Select OK.
Configure the tag format

When the spam action is set to Tagged, the Tag Format setting determines what text is used as the tag applied to the message.

To configure the tag format
1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile in which you want to configure the tag format and choose Edit.
3. The Tag Format row has a field for each traffic type. Enter the text the FortiGate unit will use as the tag for each traffic type.
4. Select OK.

Email filter examples

Configuring simple antispam protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable antispam protection on a FortiGate unit located in a satellite office.

Creating an email filter profile

Most email filter settings are configured in an email filter profile. Email filter profiles are selected in firewall policies. This way, you can create multiple email filter profiles, and tailor them to the traffic controlled by the firewall policy in which they are selected. In this example, you will create one email filter profile.

To create an email filter profile — web-based manager
1. Go to UTM > Email Filter > Profile.
2. Select Create New.
3. In the Name field, enter basic_emailfilter.
4. Ensure that IMAP, POP3, and SMTP are selected in the header row.
   These header row selections enable or disable examination of each email traffic type. When disabled, the email traffic of that type is ignored by the FortiGate unit and no email filtering options are available.
5. Under FortiGuard Email Filtering, enable IP Address Check for the IMAP, POP3, and SMTP email traffic types.
6. Under FortiGuard Email Filtering, enable URL Check for the IMAP, POP3, and SMTP email traffic types.
7. Under FortiGuard Email Filtering, enable E-mail Checksum Check for the IMAP, POP3, and SMTP email traffic types.
8. Select OK to save the email filter profile.
To create an email filter profile — CLI

```
config spamfilter profile
  edit basic_emailfilter
    config imap
      set options spamfsip spamfsurl spamfschksum
    end
    config pop3
      set options spamfsip spamfsurl spamfschksum
    end
    config smtp
      set options spamfsip spamfsurl spamfschksum
    end
  end
end
```

Selecting the email filter profile in a firewall policy

An email filter profile directs the FortiGate unit to scan network traffic only when it is selected in a firewall policy. When an email filter profile is selected in a firewall policy, its settings are applied to all the traffic the firewall policy handles.

To select the email filter profile in a firewall policy — web-based manager

1. Go to Firewall > Policy > Policy.
2. Select a policy.
3. Select the Edit icon.
4. Enable UTM.
5. Select default from the Protocol Options list.
   UTM can not be enabled without selecting a protocol options profile. A default profile is provided.
6. Select the Enable Email Filter option.
7. Select the basic_emailfilter profile from the list.
8. Select OK to save the firewall policy.

To select the email filter profile in a firewall policy — CLI

```
config firewall policy
  edit 1
    set utm-status enable
    set profile-protocol-options default
    set spamfilter-profile basic_emailfilter
  end
```

IMAP, POP3, and SMTP email traffic handled by the firewall policy you modified will be scanned for spam. Spam messages have the text “Spam” added to their subject lines. A small office may have only one firewall policy configured. If you have multiple policies, consider enabling spam scanning for all of them.

Blocking email from a user

Employees of the Example.com corporation have been receiving unwanted email messages from a former client at a company called example.net. All ties between the company and the client have been severed, but the messages continue. The FortiGate unit can be configured to prevent these messages from being delivered.
To create the email address list
1. Go to UTM > Email Filter > E-mail Address.
2. Select Create New.
3. Enter a name for the new email address list.
4. Optionally, enter a descriptive comment for the email address list.
5. Select OK to create the list.
6. Select Create New to add a new entry to the email address list.
7. Enter *@example.net in the E-mail Address field.
8. Leave Pattern Type set to the default, Wildcard.
9. Leave Action as Mark as Spam to have the FortiGate unit mark all messages from example.net as spam.

Now that the email address list is created, you must enable the email filter in the email filter profile.

To enable Email Filter
1. Go to UTM > Email Filter > Profile.
2. Select the email filter profile that is used by the firewall policies handling email traffic and choose Edit.
3. Select the check boxes labeled IMAP, POP3, and SMTP in the table header row immediately above the FortiGuard Email Filtering heading.
4. In the row E-mail Address BWL Check, select all three check boxes.
5. At the end of the E-mail address BWL check row, select the email address list you created in the previous procedure.
6. In the row Tag Location, select Subject for all three mail protocols.
7. In the row Tag Format, enter SPAM: in all three fields.
8. Select OK.

With these changes, the FortiGate unit will add “SPAM:” to the subject of any email message from an address ending with @example.net. Recipients can ignore the message or they can configure their email clients to automatically delete messages with “SPAM:” in the subject.
Intrusion protection

The FortiGate Intrusion Protection system combines signature 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 any firewall policy.

This section describes how to configure the FortiGate Intrusion Protection settings.

If you enable virtual domains (VDOMs) on the FortiGate unit, intrusion protection is configured separately for each virtual domain.

The following topics are included:

- IPS concepts
- Enable IPS scanning
- Configure IPS options
- Enable IPS packet logging
- IPS examples

IPS concepts

The FortiGate intrusion protection system protects your network from outside attacks. Your FortiGate unit has two techniques to deal with these attacks: anomaly- and signature-based defense.

Anomaly-based defense

Anomaly-based defense is used when network traffic itself is used as a weapon. A host can be flooded with far more traffic than it can handle, making the host inaccessible. The most common example is the denial of service (DoS) attack, in which an attacker directs a large number of computers to attempt normal access of the target system. If enough access attempts are made, the target is overwhelmed and unable to service genuine users. The attacker does not gain access to the target system, but it is not accessible to anyone else.

The FortiGate DoS feature will block traffic above a certain threshold from the attacker and allow connections from other legitimate users.

Signature-based defense

Signature-based defense is used against known attacks or vulnerability exploits. These often involve an attacker attempting to gain access to your network. The attacker must communicate with the host in an attempt to gain access and this communication will include particular commands or sequences of commands and variables. The IPS signatures include these command sequences, allowing the FortiGate unit to detect and stop the attack.
Signatures

IPS signatures are the basis of signature-based intrusion protection. Every attack can be reduced to a particular string of commands or a sequence of commands and variables. Signatures include this information so your FortiGate unit knows what to look for in network traffic.

Signatures also include characteristics about the attack they describe. These characteristics include the network protocol in which the attack will appear, the vulnerable operating system, and the vulnerable application.

To view the complete list of predefined signatures, go to UTM > Intrusion Protection > Predefined.

Protocol decoders

Before examining network traffic for attacks, the IPS engine uses protocol decoders to identify each protocol appearing in the traffic. Attacks are protocol-specific, so your FortiGate unit conserves resources by looking for attacks only in the protocols used to transmit them. For example, the FortiGate unit will only examine HTTP traffic for the presence of a signature describing an HTTP attack.

To view the protocol decoders, go to UTM > Intrusion Protection > Protocol Decoder.

IPS engine

Once the protocol decoders separate the network traffic by protocol, the IPS engine examines the network traffic for the attack signatures.

IPS sensors

The IPS engine does not examine network traffic for all signatures, however. You must first create an IPS sensor and specify which signatures are included. You do not have to choose each signature you want to include individually. Instead, filters are used to define the included signatures.

To view the IPS sensors, go to UTM > Intrusion Protection > IPS Sensor.

IPS filters

IPS sensors contain one or more IPS 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.

For example, if your FortiGate unit protects a Linux server running the Apache web server software, you could create a new filter to protect it. By setting OS to Linux, and Application to Apache, the filter will include only the signatures that apply to both Linux and Apache. If you wanted to scan for all the Linux signatures and all the Apache signatures, you would create two filters, one for each.

To view the filters in an IPS sensor, go to UTM > Intrusion Protection > IPS Sensor, select the IPS sensor containing the filters you want to view, and choose Edit.

Policies

To use an IPS sensor, you must select it in a firewall policy or an interface policy. An IPS sensor that is not selected in a policy will have no effect on network traffic.

IPS is most often configured as part of a firewall policy. Unless stated otherwise, discussion of IPS sensor use will be in regards to firewall policies in this document.
Enable IPS scanning

Enabling IPS scanning involves two separate parts of the FortiGate unit:

- The firewall policy allows certain network traffic based on the sender, receiver, interface, traffic type, and time of day. Firewall policies can also be used to deny traffic, but those policies do not apply to IPS scanning.
- The IPS sensor contains filters, overrides, or both. These specify which signatures are included in the IPS sensor.

When IPS is enabled, an IPS sensor is selected in a firewall policy, and all network traffic matching the policy will be checked for the signatures in the IPS sensor.

General configuration steps

For best results in configuring IPS scanning, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create an IPS sensor.
2. Create filters and/or overrides in the IPS sensor. The filters and overrides specify which signatures the IPS engine will look for in the network traffic.
3. Select a firewall policy or create a new one.
4. In the firewall policy, enable UTM protection and select Enable IPS and select the IPS sensor from the list.

All the network traffic controlled by this firewall policy will be processed according to the settings in the policy. These settings include the IPS sensor you specify in the policy.

Creating an IPS sensor

You need to create an IPS sensor and save it before configuring it with filters and override settings.

To create a new IPS sensor

1. Go to UTM > Intrusion Protection > IPS Sensor.
2. Select Create New.
3. Enter the name of the new IPS sensor.
4. Optionally, you can also enter a comment. The comment will appear in the IPS sensor list and can remind you of the details of the sensor.
5. Select OK.

The IPS sensor is created and the sensor configuration window appears. A newly created sensor is empty and contains no filters or overrides. You need to create one or more filters or overrides before the sensor can take effect.

Creating an IPS filter

Filters determine which signatures are included in an IPS sensor. Rather than choosing each signature, you choose the characteristics of the signatures you want included in the IPS sensor by configuring a filter. You can create multiple filters in an IPS sensor.

To create a new IPS filter

1. Go to UTM > Intrusion Protection > IPS Sensor.
2. Select the Edit icon of the IPS sensor to which you want to add the filter.
3 Select Add Filter.
4 Enter the name of the new filter.
5 Configure the filter that you require. Signatures matching all of the characteristics you specify in the filter will be included in the IPS sensor.
6 Select OK.

The filter is created and added to the filter list. The number of signatures included in the filter is listed in the Count column. You can view a list of the included signatures by selecting the View Rules icon.

Note: Signature overrides are checked before filters.

Updating predefined IPS signatures

The FortiGuard Service periodically updates the pre-defined signatures and adds new signatures to counter emerging threats as they appear.

Because 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.

Creating an IPS signature override

Pre-defined and custom signature overrides are configured and work largely the same as filters, except they define the behavior of only one signature.

You can use overrides in two ways:

• To change the behavior of a signature already included in a filter.
  
  For example, to protect a web server, you can create a filter that includes and enables all signatures related to servers. If you want to disable one of those signatures, the simplest way is to create an override and mark the signature as disabled.

• To add an individual signature, 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 of the signature are ignored. These settings must be explicitly set when creating the override.

Note: Before an override can affect network traffic, you must add it to a filter, and you must select the filter in a firewall policy. An override does not have the ability to affect network traffic until these steps are taken. For more information, see “Enable IPS scanning” on page 85.

To create an IPS signature override

1 Go to UTM > Intrusion Protection > IPS Sensor.
2 Select the IPS sensor to which you want to add the override and select the Edit icon.
3 Select either Add Pre-defined Override or Add Custom Override, depending on the type of IPS signature override you require.
4 For the Action, select Pass, Block, or Reset. When the override is enabled, the action determines what the FortiGate will do with traffic containing the specified signature.
5 Select Logging to log all occurrences of the signature.
6 Select Packet Log to save the packets containing the specified signature. For more information, see “Enable IPS packet logging” on page 99.

7 Select the Browse icon and choose the signature to include in the override.

8 Select Enable.

9 Select OK.

Creating a custom IPS signature

The FortiGate predefined signatures cover common attacks. If you use an unusual or specialized application or an uncommon platform, add custom signatures based on the security alerts released by the application and platform vendors.

You can add or edit custom signatures using the web-based manager or the CLI.

To create a custom signature

1 Go to UTM > Intrusion Protection > Custom.

2 Select Create New to add a new custom signature.

3 Enter a Name for the custom signature.

4 Enter the Signature. For information about completing this field, see “Custom signature syntax and keywords”.

5 Select OK.

Custom signature syntax and keywords

All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.

Custom signature syntax

A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.

A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis ([ ]). The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)

You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to UTM > Intrusion Protection > Signature > Custom and enter the data directly into the Signature field, following the guidance in the next topics.

Table 7 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 88.
Table 7: Valid syntax for custom signature fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Valid Characters</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEADER</td>
<td>F-SBID</td>
<td>The header for an attack definition signature. Each custom signature must begin with this header.</td>
</tr>
<tr>
<td>KEYWORD</td>
<td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td>
<td>The keyword is used to identify a parameter. See “Custom signature keywords” on page 88 for tables of supported keywords.</td>
</tr>
<tr>
<td>VALUE</td>
<td>Double quotes (”) must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td>
<td>The value is set specifically for a parameter identified by a keyword.</td>
</tr>
</tbody>
</table>

Custom signature keywords

Table 8: Information keywords

<table>
<thead>
<tr>
<th>Keyword and value</th>
<th>Description</th>
</tr>
</thead>
</table>
| --attack_id <id_int>; | Use this optional value to identify the signature. It cannot be the same value as any other custom rules. If an attack ID is not specified, the FortiGate automatically assigns an attack ID to the signature. If you are using VDOMs, custom signatures appear only in the VDOM in which you create them. You can use the same attack ID for signatures in different VDOMs. An attack ID you assign must be between 1000 and 9999. Example:  
  --attack_id 1234; |
| --name <name_str>; | Enter the name of the rule. A rule name must be unique. If you are using VDOMs, custom signatures appear only in the VDOM in which you create them. You can use the same rule name for signatures in different VDOMs. The name you assign must be a string greater than 0 and less than 64 characters in length. Example:  
  --name "Buffer_Overflow"; |
Table 9: Session keywords

<table>
<thead>
<tr>
<th>Keyword and value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--flow</td>
<td>Specify the traffic direction and state to be inspected. They can be used for all IP traffic. Example: --src_port 41523; --flow bi_direction; The signature checks traffic to and from port 41523. If you enable &quot;quarantine attacker&quot;, the optional reversed keyword allows you to change the side of the connection to be quarantined when the signature is detected. For example, a custom signature written to detect a brute-force log in attack is triggered when &quot;Login Failed&quot; is detected from_server more than 10 times in 5 seconds. If the attacker is quarantined, it is the server that is quarantined in this instance. Adding reversed corrects this problem and quarantines the actual attacker. Previous FortiOS versions used to_client and to_server values. These are now deprecated, but still function for backwards compatibility.</td>
</tr>
<tr>
<td>{from_client[,reversed]</td>
<td>from_server[,reversed]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>--service {HTTP</th>
<th>TELNET</th>
<th>FTP</th>
<th>DNS</th>
<th>SMTP</th>
<th>POP3</th>
<th>IMAP</th>
<th>SNMP</th>
<th>RADIUS</th>
<th>LDAP</th>
<th>MSSQL</th>
<th>RPC</th>
<th>SIP</th>
<th>H323</th>
<th>NBSS</th>
<th>DCERP</th>
<th>SSH</th>
<th>SSL};</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 10: Content keywords

<table>
<thead>
<tr>
<th>Keyword and value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--byte_jump</td>
<td>Use the byte_jump option to extract a number of bytes from a packet, convert them to their numeric representation, and jump the match reference up that many bytes (for further pattern matching or byte testing). This keyword allows relative pattern matches to take into account numerical values found in network data. The available keyword options include:</td>
</tr>
</tbody>
</table>

| <bytes_to_convert>: The number of bytes to examine from the packet. |
| <offset>: The number of bytes into the payload to start processing. |
| relative: Use an offset relative to last pattern match. |
| big: Process the data as big endian (default). |
| little: Process the data as little endian. |
| string: The data is a string in the packet. |
| hex: The converted string data is represented in hexadecimal notation. |
| dec: The converted string data is represented in decimal notation. |
| oct: The converted string data is represented in octal notation. |
| align: Round up the number of converted bytes to the next 32-bit boundary. |
Table 10: Content keywords (Continued)

<table>
<thead>
<tr>
<th>Keyword and value</th>
<th>Description</th>
</tr>
</thead>
</table>
| --byte_test <bytes_to_convert>, <operator>, <value>, <offset>[, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct]; | Use the `byte_test` keyword to compare a byte field against a specific value (with operator). This keyword is capable of testing binary values or converting representative byte strings to their binary equivalent and testing them. The available keyword options include:  
• `<bytes_to_convert>`: The number of bytes to compare.  
• `<operator>`: The operation to perform when comparing the value (`<`, `>`, `=`, `!`, `&`).  
• `<value>`: The value to compare the converted value against.  
• `<offset>`: The number of bytes into the payload to start processing.  
• `relative`: Use an offset relative to last pattern match.  
• `big`: Process the data as big endian (default).  
• `little`: Process the data as little endian.  
• `string`: The data is a string in the packet.  
• `hex`: The converted string data is represented in hexadecimal notation.  
• `dec`: The converted string data is represented in decimal notation.  
• `oct`: The converted string data is represented in octal notation. |
| --depth <depth_int>; | Use the `depth` keyword to search for the contents within the specified number of bytes after the starting point defined by the `offset` keyword. If no `offset` is specified, the `offset` is assumed to be equal to 0.  
If the value of the `depth` keyword is smaller than the length of the value of the `content` keyword, this signature will never be matched.  
The `depth` must be between 0 and 65535. |
| --distance <dist_int>; | Use the `distance` keyword to search for the contents within the specified number of bytes relative to the end of the previously matched contents. If the `within` keyword is not specified, continue looking for a match until the end of the payload.  
The `distance` must be between 0 and 65535. |
| --content [!]"<content_str>"; | Deprecated, see `pattern` and `context` keywords. Use the `content` keyword to search for the content string in the packet payload. The content string must be enclosed in double quotes.  
To have the FortiGate search for a packet that does not contain the specified context string, add an exclamation mark (!) before the content string.  
Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character.  
The double quote ("), pipe sign(|) and colon(;) characters must be escaped using a back slash if specified in a content string.  
If the value of the `content` keyword is greater than the length of the value of the `depth` keyword, this signature will never be matched. |
Table 10: Content keywords (Continued)

<table>
<thead>
<tr>
<th>Keyword and value</th>
<th>Description</th>
</tr>
</thead>
</table>
| **--context {uri | header | body | host};** | Specify the protocol field to look for the pattern. If context is not specified for a pattern, the FortiGate unit searches for the pattern anywhere in the packet buffer. The available context variables are:  
  - **uri**: Search for the pattern in the HTTP URI line.  
  - **header**: Search for the pattern in HTTP header lines or SMTP/POP3/SMTP control messages.  
  - **body**: Search for the pattern in HTTP body or SMTP/POP3/SMTP email body.  
  - **host**: Search for the pattern in HTTP HOST line.  
  Example:  
  ```  
  --pattern "GET "  
  --context uri  
  --pattern "yahoo.com"  
  --context host  
  --no_case  
  --pcre "/DESCRIBE\s+\/\s+RTSP\//i"  
  --context header  
  ```
| **--no_case;** | Use the **no-case** keyword to force the FortiGate unit to perform a case-insensitive pattern match. |
| **--offset <offset_int>;** | Use the **offset** keyword to look for the contents after the specified number of bytes into the payload. The specified number of bytes is an absolute value in the payload. Follow the **offset** keyword with the **depth** keyword to stop looking for a match after a specified number of bytes. If no **depth** is specified, the FortiGate unit continues looking for a match until the end of the payload.  
  The **offset** must be between 0 and 65535. |
| **--pattern [!]"<pattern_str>";** | The FortiGate unit will search for the specified pattern.  
  A **pattern** keyword normally is followed by a **context** keyword to define where to look for the pattern in the packet.  
  If a **context** keyword is not present, the FortiGate unit looks for the pattern anywhere in the packet buffer.  
  To have the FortiGate search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI.  
  Example:  
  ```  
  --pattern "/level/"  
  --pattern "|E8 D9FF FFFF|/bin/sh"  
  --pattern !"|20|RTSP/"  
  ```
Similarly to the `pattern` keyword, use the `pcre` keyword to specify a pattern using Perl-compatible regular expressions (PCRE). A `pcre` keyword can be followed by a `context` keyword to define where to look for the pattern in the packet. If no `context` keyword is present, the FortiGate unit looks for the pattern anywhere in the packet buffer. For more information about PCRE syntax, go to [http://www.pcre.org](http://www.pcre.org).

The switches include:
- `i`: Case insensitive.
- `s`: Include newlines in the dot metacharacter.
- `m`: By default, the string is treated as one big line of characters. `^` and `$` match at the beginning and ending of the string. When `m` is set, `^` and `$` match immediately following or immediately before any newline in the buffer, as well as the very start and very end of the buffer.
- `x`: White space data characters in the pattern are ignored except when escaped or inside a character class.
- `A`: The pattern must match only at the start of the buffer (same as `^`).
- `E`: Set `$` to match only at the end of the subject string. Without `E`, `$` also matches immediately before the final character if it is a newline (but not before any other newlines).
- `G`: Invert the “greediness” of the quantifiers so that they are not greedy by default, but become greedy if followed by `?`.
- `R`: Match relative to the end of the last pattern match. (Similar to `distance:0;`).
- `U`: Deprecated, see the `context` keyword. Match the decoded URI buffers.

**Table 10: Content keywords (Continued)**

<table>
<thead>
<tr>
<th>Keyword and value</th>
<th>Description</th>
</tr>
</thead>
</table>
| `--pcre` [!]"(/<regex>/|m<delim><regex><delim>){ismxAEURGB}"; | Similarly to the `pattern` keyword, use the `pcre` keyword to specify a pattern using Perl-compatible regular expressions (PCRE). A `pcre` keyword can be followed by a `context` keyword to define where to look for the pattern in the packet. If no `context` keyword is present, the FortiGate unit looks for the pattern anywhere in the packet buffer. For more information about PCRE syntax, go to [http://www.pcre.org](http://www.pcre.org). The switches include:  
  - `i`: Case insensitive.  
  - `s`: Include newlines in the dot metacharacter.  
  - `m`: By default, the string is treated as one big line of characters. `^` and `$` match at the beginning and ending of the string. When `m` is set, `^` and `$` match immediately following or immediately before any newline in the buffer, as well as the very start and very end of the buffer.  
  - `x`: White space data characters in the pattern are ignored except when escaped or inside a character class.  
  - `A`: The pattern must match only at the start of the buffer (same as `^`).  
  - `E`: Set `$` to match only at the end of the subject string. Without `E`, `$` also matches immediately before the final character if it is a newline (but not before any other newlines).  
  - `G`: Invert the “greediness” of the quantifiers so that they are not greedy by default, but become greedy if followed by `?`.  
  - `R`: Match relative to the end of the last pattern match. (Similar to `distance:0;`).  
  - `U`: Deprecated, see the `context` keyword. Match the decoded URI buffers. |
| `--uri` [!]"<uri_str>"; | Deprecated, see `pattern` and `context` keywords. Use the `uri` keyword to search for the URI in the packet payload. The URI must be enclosed in double quotes ("), To have the FortiGate unit search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI. Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character. The double quote ("), pipe sign (|) and colon (: characters must be escaped using a back slash (\) if specified in a URI string. |
| `--within <within_int>;` | Use this together with the `distance` keyword to search for the contents within the specified number of bytes of the payload. The `within` value must be between 0 and 65535. |
### Table 11: IP header keywords

<table>
<thead>
<tr>
<th>Keyword and Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--dst_addr [!]&lt;ipv4&gt;;</code></td>
<td>Use the <code>dst_addr</code> keyword to search for the destination IP address. To have the FortiGate search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets. <strong>Example:</strong> <code>dst_addr [172.20.0.0/16, 10.1.0.0/16, 192.168.0.0/16]</code></td>
</tr>
<tr>
<td><code>--ip_id &lt;field_int&gt;;</code></td>
<td>Check the IP ID field for the specified value.</td>
</tr>
<tr>
<td>`--ip_option {rr</td>
<td>eol</td>
</tr>
<tr>
<td><code>--ip_tos &lt;field_int&gt;;</code></td>
<td>Check the IP TOS field for the specified value.</td>
</tr>
<tr>
<td>`--ip_ttl [&lt;</td>
<td>&gt;] &lt;ttl_int&gt;;`</td>
</tr>
<tr>
<td>`--protocol {&lt;protocol_int&gt;</td>
<td>tcp</td>
</tr>
<tr>
<td><code>--src_addr [!]&lt;ipv4&gt;;</code></td>
<td>Use the <code>src_addr</code> keyword to search for the source IP address. To have the FortiGate unit search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets. <strong>Example:</strong> <code>src_addr 192.168.13.0/24</code></td>
</tr>
</tbody>
</table>
### Table 12: TCP header keywords

<table>
<thead>
<tr>
<th>Keyword and Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ack &lt;ack_int&gt;;</td>
<td>Check for the specified TCP acknowledge number.</td>
</tr>
</tbody>
</table>
| --dst_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>}; | Use the dst_port keyword to specify the destination port number. You can specify a single port or port range:  
• <port_int> is a single port.  
• :<port_int> includes the specified port and all lower numbered ports.  
• <port_int>: includes the specified port and all higher numbered ports.  
• <port_int>:<port_int> includes the two specified ports and all ports in between. |
| --src_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>}; | Use the src_port keyword to specify the source port number. You can specify a single port or port range:  
• <port_int> is a single port.  
• :<port_int> includes the specified port and all lower numbered ports.  
• <port_int>: includes the specified port and all higher numbered ports.  
• <port_int>:<port_int> includes the two specified ports and all ports in between. |
| --tcp_flags <SAFRUP120>][!|*|+] [!,<SAFRUP120>]; | Specify the TCP flags to match in a packet.  
• S: Match the SYN flag.  
• A: Match the ACK flag.  
• F: Match the FIN flag.  
• R: Match the RST flag.  
• U: Match the URG flag.  
• P: Match the PSH flag.  
• 1: Match Reserved bit 1.  
• 2: Match Reserved bit 2.  
• 0: Match No TCP flags set.  
• !: Match if the specified bits are not set.  
• *: Match if any of the specified bits are set.  
• +: Match on the specified bits, plus any others.  
The first part if the value (<SAFRUP120>) defines the bits that must be present for a successful match. For example:  
--tcp_flags AP  
only matches the case where both A and P bits are set.  
The second part ([!,<SAFRUP120>]) is optional, and defines the additional bits that can be present for a match. For example:  
tcp_flags S,12  
matches the following combinations of flags: S, S and 1, S and 2, S and 1 and 2.  
The modifiers !, * and + cannot be used in the second part. |
| --window_size [!]<window_int>; | Check for the specified TCP window size. You can specify the window size as a hexadecimal or decimal integer. A hexadecimal value must be preceded by Ox.  
To have the FortiGate search for the absence of the specified window size, add an exclamation mark (!) before the window size. |
### Table 13: UDP header keywords

<table>
<thead>
<tr>
<th>Keyword and Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dst_port [!]</td>
<td>Specify the destination port number.</td>
</tr>
<tr>
<td>&lt;port_int&gt;</td>
<td>You can specify a single port or port range:</td>
</tr>
<tr>
<td>:&lt;port_int&gt;</td>
<td>• &lt;port_int&gt; is a single port.</td>
</tr>
<tr>
<td>&lt;port_int&gt;:</td>
<td>• :&lt;port_int&gt; includes the specified port and all lower numbered ports.</td>
</tr>
<tr>
<td>&lt;port_int&gt;:&lt;port_int&gt;;</td>
<td>• &lt;port_int&gt;: includes the specified port and all higher numbered ports.</td>
</tr>
<tr>
<td>--src_port [!]</td>
<td>Specify the source port number.</td>
</tr>
<tr>
<td>&lt;port_int&gt;</td>
<td>You can specify a single port or port range:</td>
</tr>
<tr>
<td>:&lt;port_int&gt;</td>
<td>• &lt;port_int&gt; is a single port.</td>
</tr>
<tr>
<td>&lt;port_int&gt;:</td>
<td>• :&lt;port_int&gt; includes the specified port and all lower numbered ports.</td>
</tr>
<tr>
<td>&lt;port_int&gt;:&lt;port_int&gt;;</td>
<td>• &lt;port_int&gt;: includes the specified port and all higher numbered ports.</td>
</tr>
</tbody>
</table>

### Table 14: ICMP keywords

<table>
<thead>
<tr>
<th>Keyword and Value</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>--icmp_code &lt;code_int&gt;;</td>
<td>Specify the ICMP code to match.</td>
</tr>
<tr>
<td>--icmp_id &lt;id_int&gt;;</td>
<td>Check for the specified ICMP ID value.</td>
</tr>
<tr>
<td>--icmp_seq &lt;seq_int&gt;;</td>
<td>Check for the specified ICMP sequence value.</td>
</tr>
<tr>
<td>--icmp_type &lt;type_int&gt;;</td>
<td>Specify the ICMP type to match.</td>
</tr>
</tbody>
</table>

### Table 15: Other keywords

<table>
<thead>
<tr>
<th>Keyword and Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--data_size {&lt;size_int&gt;</td>
<td>Test the packet payload size. With data_size specified, packet reassembly is turned off automatically. So a signature with data_size and only_stream values set is wrong.</td>
</tr>
<tr>
<td>&lt;=&lt;size_int&gt;</td>
<td>• &lt;size_int&gt; is a particular packet size.</td>
</tr>
<tr>
<td>&gt;=&lt;size_int&gt;</td>
<td>• &lt;=&lt;size_int&gt; is a packet smaller than the specified size.</td>
</tr>
<tr>
<td>&lt;port_int&gt;&lt;&gt;port_int};</td>
<td>• &gt;=&lt;size_int&gt; is a packet larger than the specified size.</td>
</tr>
<tr>
<td>--data_at &lt;offset_int&gt;[,</td>
<td>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</td>
</tr>
<tr>
<td>relative];</td>
<td>• &lt;size_int&gt;&lt;&gt;&lt;size_int&gt; is a packet within the range between the specified sizes.</td>
</tr>
</tbody>
</table>
IPS processing in an HA cluster

IPS processing in an HA cluster is no different than with a single FortiGate unit, from the point of view of the network user. The difference appears when a secondary unit takes over from the primary, and what happens depends on the HA mode.
Active-passive

In an active-passive HA cluster, the primary unit processes all traffic just as it would in a stand-alone configuration. Should the primary unit fail, a secondary unit will assume the role of the primary unit and begin to process network traffic. By default, the state of active communication sessions are not shared with secondary units and will not survive the failover condition. Once the sessions are reestablished however, traffic processing will continue as normal.

If your network requires that active sessions are taken over by the new primary unit, select Enable Session Pick-up in your HA configuration. Because session information must be sent to all subordinate units on a regular basis, session pick-up is a resource-intensive feature and is not enabled by default.

Active-active

The fail-over process in an active-active cluster is similar to an active-passive cluster. When the primary unit fails, a secondary unit takes over and traffic processing continues. The load-balancing schedule used to distribute sessions to the cluster members is used by the new primary unit to redistribute sessions among the remaining subordinate units. If session pick-up is not enabled, the sessions active on the failed primary are lost, and the sessions redistributed among the secondary units may also be lost. If session pick-up is enabled, all sessions are handled according to their last-known state.

For more information about HA options and settings, see the FortiGate High Availability Handbook.

Configure IPS options

There are a number of CLI commands that influence how IPS functions.

Configuring the IPS engine algorithm

The IPS engine is able to search for signature matches in two ways. One method is faster but uses more memory, the other uses less memory but is slower. Use the algorithm CLI command to select one method:

```plaintext
config ips global
  set algorithm {high | low | engine-pick}
end
```

Specify high to use the faster more memory intensive method or low for the slower memory efficient method. The default setting is engine-pick, which allows the IPS engine to choose the best method on the fly.

Configuring the IPS engine-count

FortiGate units with multiple processors can run more than one IPS engine concurrently. The engine-count CLI command allows you to specify how many IPS engines are used at the same time:

```plaintext
config ips global
  set engine-count <int>
end
```

The recommended and default setting is 0, which allows the FortiGate unit to determine the optimum number of IPS engines.
Configuring fail-open

If the IPS engine fails for any reason, it will fail open by default. This means that traffic continues to flow without IPS scanning. If IPS protection is more important to your network than the uninterrupted flow of network traffic, you can disable this behavior using the fail-open CLI command:

```
config ips global
    set fail-open {enable | disable}
end
```

The default setting is enable.

Configuring the session count accuracy

The IPS engine can keep track of the number of open session in two ways. An accurate count uses more resources than a less accurate heuristic count.

```
config ips global
    set session-limit-mode {accurate | heuristic}
end
```

The default is heuristic.

Configuring the IPS buffer size

Set the size of the IPS buffer.

```
config ips global
    set socket-size <int>
end
```

The acceptable range is from 1 to 64 megabytes. The default size varies by model.

Configuring protocol decoders

The FortiGate 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.

To view the decoders and the port numbers that each protocol decoder monitors, go to UTM > Intrusion Protection > Protocol Decoder. The port or ports monitored by each decoder are listed. Many decoders are able to recognize traffic by type rather than by port. These decoders have their port listed as auto because the traffic will be recognized automatically, regardless of the port.

To change the ports a decoder examines, you must use the CLI. In this example, the ports examined by the DNS decoder are changed from the default 53 to 100, 200, and 300.

```
config ips decoder dns_decoder
    set port_list "100,200,300"
end
```

You cannot assign specific ports to decoders that are set to auto by default. These decoders can detect their traffic on any port. Specifying individual ports is not necessary.
Configuring security processing modules

FortiGate Security Processing Modules, such as the CE4, XE2, and FE8, can increase overall system performance by accelerating some security and networking processing on the interfaces they provide. They also allow the FortiGate unit to offload the processing to the security module, thereby freeing up its own processor for other tasks. The security module performs its own IPS and firewall processing, but you can configure it to favor IPS in hostile high-traffic environments.

If you have a security processing module, use the following CLI commands to configure it to devote more resources to IPS than firewall. This example shows the CLI commands required to configure a security module in slot 1 for increased IPS performance.

```
config system amc-slot
  edit sw1
    set optimization-mode fw-ips
    set ips-weight balanced
    set ips-p2p disable
    set ips-fail-open enable
    set fp-disable none
    set ipsec-inb-optimization enable
    set syn-proxy-client-timer 3
    set syn-proxy-server-timer 3
  end
```

In addition to offloading IPS processing, security processing modules provide a hardware accelerated SYN proxy to defend against SYN flood denial of service attacks. When using a security module, configure your DoS sensor `tcp_syn_flood` anomaly with the `Proxy` action. The `Proxy` action activates the hardware accelerated SYN proxy.

**Note:** Because DoS sensors are configured before being applied to an interface, you can assign a DoS sensor with the `Proxy` action to an interface that does not have hardware SYN proxy support. In this circumstance, the `Proxy` action is invalid and a `Pass` action will be applied.

Enable IPS packet logging

Packet logging saves the network packets containing the traffic matching an IPS signature to the attack log. The FortiGate unit will save the logged packets to wherever the logs are configured to be stored, whether memory, internal hard drive, a FortiAnalyzer unit, or the FortiGuard Analysis and Management Service.

You can enable packet logging only in signature overrides or in filters. Use caution in enabling packet logging in a filter. Filters configured with few restrictions can contain thousands of signatures, potentially resulting in a flood of saved packets. This would take up a great deal of space, require time to sort through, and consume considerable system resources to process. Packet logging is designed as a focused diagnostic tool and is best used with a narrow scope.

**Caution:** Although logging to multiple FortiAnalyzer units is supported, packet logs are not sent to the secondary and tertiary FortiAnalyzer units. Only the primary unit receives packet logs.
IPS examples

Configuring basic IPS protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable IPS protection on a FortiGate unit located in a satellite office. The satellite office contains only Windows clients.

Creating an IPS sensor

Most IPS settings are configured in an IPS sensor. IPS sensors are selected in firewall policies. This way, you can create multiple IPS sensors, and tailor them to the traffic controlled by the firewall policy in which they are selected. In this example, you will create one IPS sensor.

To create an IPS sensor—web-based manager

1. Go to UTM > Intrusion Protection > IPS Sensor.
2. Select Create New.
3. In the Name field, enter basic_ips.
4. In the Comments field, enter IPS protection for Windows clients.
5. Select OK.
6. In the Filters section, select Create New.
7. In the Name field, enter windows_clients.
8. For Target, select Specify and Client.
9. For OS, select Specify and Windows.
10. Select OK to save the filter.
11. Select OK to save the IPS sensor.
To create an IPS sensor — CLI

```plaintext
config ips sensor
edit basic_ips
  set comment "IPS protection for Windows clients"
config filter
  edit windows_clients
    set location client
    set os windows
  end
end
```

Selecting the antivirus profile in a firewall policy

An antivirus profile directs the FortiGate unit to scan network traffic only when it is selected in a firewall policy. When an antivirus profile is selected in a firewall policy, its settings are applied to all the traffic the firewall policy handles.

To select the IPS sensor in a firewall policy — web-based manager

1. Go to Firewall > Policy > Policy.
2. Select a policy.
3. Select the Edit icon.
4. Enable UTM.
5. Select the Enable IPS option.
6. Select the basic_ips profile from the list.
7. Select OK to save the firewall policy.

To select the antivirus profile in a firewall policy — CLI

```plaintext
config firewall policy
edit 1
  set utm-status enable
  set ips-sensor basic_ips
end
```

All traffic handled by the firewall policy you modified will be scanned for attacks against Windows clients. A small office may have only one firewall policy configured. If you have multiple policies, consider enabling antivirus scanning for all of them.

Using IPS to protect your web server

Many companies have web servers and they must be protected from attack. Since web servers must be accessible, protection is not as simple as blocking access. IPS is one tool your FortiGate unit has to allow you to protect your network.

In this example, we will configure IPS to protect a web server. As shown in Figure 9 on page 102, a FortiGate unit protects a web server and an internal network. The internal network will have its own policies and configuration but we will concentrate on the web server in this example.
The FortiGate unit is configured with:
- a virtual IP to give the web server a unique address accessible from the Internet.
- a firewall policy to allow access to the web server from the Internet using the virtual IP.

To protect the web server using intrusion protection, you need to create an IPS sensor, populate it with filters, then enable IPS scanning in the firewall policy.

**To create an IPS sensor**
1. Go to UTM > Intrusion Protection > IPS Sensor and select Create New.
2. Enter web_server as the name of the new IPS sensor.
3. Select OK.

The new IPS sensor is created but it has no filters, and therefore no signatures are included.

The web server operating system is Linux, so you need to create a filter for all Linux server signatures.

**To create the Linux server filter**
1. Go to UTM > Intrusion Protection > IPS Sensor and select the web_server IPS sensor and select the Edit icon.
2. Select Add Filter.
3. Enter Linux Server as the name of the new filter.
4. For Target, select Specify and choose server.
5. For OS, select Specify and choose Linux.
6. Select OK.
The filter is saved and the IPS sensor page reappears. In the filter list, find the Linux Server filter and look at the value in the Count column. This shows how many signatures match the current filter settings. You can select the View Rules icon to see a listing of the included signatures.

The web server software is Apache, so you need to create a second filter for all Apache signatures.

**To create the Apache filter**

1. Go to UTM > Intrusion Protection > IPS Sensor and select the web_server IPS sensor and select the Edit icon.
2. Select Add Filter.
3. Enter Apache as the name of the new filter.
4. For Application, select Specify and choose Apache from the Available list.
5. Select the right-arrow to move Apache to the Selected list.
6. Select OK.

The filter is saved and the IPS sensor page reappears.

It might seem that you can skip a step and create one filter that specifies both Linux server and Apache signatures. However, this would include a smaller number of filters. It would not include signatures to detect attacks against the operating system directly, for example.

You have created the IPS sensor and the two filters that include the signatures you need. To have it start scanning traffic, you must edit the firewall policy.

**To edit the firewall policy**

1. Go to Firewall > Policy > Policy, select firewall policy that allows access to the web server, and select the Edit icon.
2. Enable UTM.
3. Select the Enable IPS option and choose the web_server IPS sensor from the list.
4. Select OK.

Since IPS is enabled and the web_server IPS sensor is specified in the firewall policy controlling the web server traffic, the IPS sensor examines the web server traffic for matches to the signatures it contains.

**Create and test a packet logging IPS sensor**

In this example, you create a new IPS sensor and include a filter that detects the EICAR test file and saves a packet log when it is found. This is an ideal first experience with packet logging because the EICAR test file can cause no harm, and it is freely available for testing purposes.

**Create an IPS sensor**

1. Go to UTM > Intrusion Protection > IPS Sensor.
2. Select Create New.
3. Name the new IPS sensor EICAR test.
4. Select OK.

**Create an Override**

1. Select Add Pre-defined Override.
2. Select the signature browse icon.
3 Rather than search through the signature list, use the name filter by selecting the filter icon in the header of the Name column.
4 In the Filters list, select Name.
5 Select Enable.
6 In the Field selection, choose Contains.
7 Enter EICAR in the Text field.
8 Select OK.
9 Select the EICAR.AV.Test.File.Download signature.
10 Select OK.
11 Select Enable, Logging, and Packet Log.
12 Select OK.
13 Select Block as the Action.
14 Select OK to save the IPS sensor.

You are returned to the IPS sensor list. The EICAR test sensor appears in the list.

Add the IPS sensor to the firewall policy allowing Internet access
1 Go to Firewall > Policy > Policy.
2 Select the firewall policy that allows you to access the Internet.
3 Select the Edit icon.
4 Enable Log Allowed Traffic.
5 Enable UTM.
6 Select Enable IPS.
7 Choose EICAR test from the available IPS sensors.
8 Select OK.

With the IPS sensor configured and selected in the firewall policy, the FortiGate unit should block any attempt to download the EICAR test file.

Test the IPS sensor
1 Using your web browser, go to http://www.eicar.org/anti_virus_test_file.htm.
2 Scroll to the bottom of the page and select eicar.com from the row labeled as using the standard HTTP protocol.
3 The browser attempts to download the requested file and,
   • If the file is successfully downloaded, the custom signature configuration failed at some point. Check the custom signature, the IPS sensor, and the firewall profile.
   • If the download is blocked with a high security alert message explaining that you’re not permitted to download the file, the EICAR test file was blocked by the FortiGate unit antivirus scanner before the IPS sensor could examine it. Disable antivirus scanning and try to download the EICAR test file again.
   • If no file is downloaded and the browser eventually times out, the custom signature successfully detected the EICAR test file and blocked the download.
Viewing the packet log

2. Locate the log entry that recorded the blocking of the EICAR test file block. The Message field data will be tools: EICAR.AV.Test.File.Download.
4. The packet log viewer is displayed.

Creating a custom signature to block access to example.com

In this first example, you will create a custom signature to block access to the example.com URL.

This example describes the use of the custom signature syntax to block access to a URL. To create the custom signature entry in the FortiGate unit web-based manager, see “Creating a custom IPS signature” on page 87.

1. Enter the custom signature basic format
   All custom signatures have a header and at least one keyword/value pair. The header is always the same:
   ```
   F-SBID( )
   ```
   The keyword/value pairs appear within the parentheses and each pair is followed by a semicolon.

2. Choose a name for the custom signature
   Every custom signature requires a name, so it is a good practice to assign a name before adding any other keywords.
   Use the `--name` keyword to assign the custom signature a name. The name value follows the keyword after a space. Enclose the name value in double-quotes:
   ```
   F-SBID( --name "Block.example.com"; )
   ```
   The signature, as it appears here, will not do anything if you try to use it. It has a name, but does not look for any patterns in network traffic. You must specify a pattern that the FortiGate unit will search for.

3. Add a signature pattern
   Use the `--pattern` keyword to specify what the FortiGate unit will search for:
   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; )
   ```
   The signature will now detect the example.com URL appearing in network traffic. The custom signature should only detect the URL in HTTP traffic, however. Any other traffic with the URL should be allowed to pass. For example, an email message to or from example.com should not be stopped.

4. Specify the service
   Use the `--service` keyword to limit the effect of the custom signature to only the HTTP protocol.
   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; )
   ```
   The FortiGate unit will limit its search for the pattern to the HTTP protocol. Even though the HTTP protocol uses only TCP traffic, the FortiGate will search for HTTP protocol communication in TCP, UDP, and ICMP traffic. This is a waste of system resources that you can avoid by limiting the search further, as shown below.
5 Specify the traffic type.

Use the `--protocol tcp` keyword to limit the effect of the custom signature to only TCP traffic. This will save system resources by not unnecessarily scanning UDP and ICMP traffic.

F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --protocol tcp; )

The FortiGate unit will limit its search for the pattern to TCP traffic and ignore UDP and ICMP network traffic.

6 Ignore case sensitivity

By default, patterns are case sensitive. If a user directed his or her browser to Example.com, the custom signature would not recognize the URL as a match.

Use the `--no_case` keyword to make the pattern matching case insensitive.

F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --no_case; )

Unlike all of the other keywords in this example, the `--no_case` keyword has no value. Only the keyword is required.

7 Limit pattern scans to only traffic sent from the client

The `--flow` command can be used to further limit the network traffic being scanned to only that send by the client or by the server.

F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --no_case; --flow from_client; )

Web servers do not contact clients until clients first open a communication session. Therefore, using the `--flow from_client` command will force the FortiGate to ignore all traffic from the server. Since the majority of HTTP traffic flows from the server to the client, this will save considerable system resources and still maintain protection.

8 Specify the context

When the client browser tries to contact example.com, a DNS is first consulted to get the example.com server IP address. The IP address is then specified in the URL field of the HTTP communication. The domain name will still appear in the host field, so this custom signature will not function without the `--context host` keyword/value pair.

F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --no_case; --flow from_client; --context host; )

Creating a custom signature to block the SMTP “vrfy” command

The SMTP “vrfy” command can be used to verify the existence of a single email address or to list all of the valid email accounts on an email server. A spammer could potentially use this command to obtain a list of all valid email users and direct spam to their inboxes.

In this example, you will create a custom signature to block the use of the vrfy command. Since the custom signature blocks the vrfy command from coming through the FortiGate unit, the administrator can still use the command on the internal network.

This example describes the use of the custom signature syntax to block the vrfy command. To create the custom signature entry in the FortiGate unit web-based manager, see “Creating a custom IPS signature” on page 87.
1 Enter the custom signature basic format

All custom signatures have a header and at least one keyword/value pair. The header is always the same:

F-SBID( )

The keyword/value pairs appear within the parentheses and each pair is followed by a semicolon.

2 Choose a name for the custom signature

Every custom signature requires a name, so it is a good practice to assign a name before you add any other keywords.

Use the --name keyword to assign the custom signature a name. The name value follows the keyword after a space. Enclose the name value in double-quotes:

F-SBID( --name "Block.SMTP.VRFY.CMD"; )

The signature, as it appears here, will not do anything if you try to use it. It has a name, but does not look for any patterns in network traffic. You must specify a pattern that the FortiGate unit will search for.

3 Add a signature pattern

Use the --pattern keyword to specify what the FortiGate unit will search for:

F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; )

The signature will now detect the vrfy command appearing in network traffic. The custom signature should only detect the command in SMTP traffic, however. Any other traffic with the pattern should be allowed to pass. For example, an email message discussing the vrfy command should not be stopped.

4 Specify the service

Use the --service keyword to limit the effect of the custom signature to only the HTTP protocol.

F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; --service SMTP; )

The FortiGate unit will limit its search for the pattern to the SMTP protocol.

Even though the SMTP protocol uses only TCP traffic, the FortiGate will search for SMTP protocol communication in TCP, UDP, and ICMP traffic. This is a waste of system resources that you can avoid by limiting the search further, as shown below.

5 Specify the traffic type.

Use the --protocol tcp keyword to limit the effect of the custom signature to only TCP traffic. This will save system resources by not unnecessarily scanning UDP and ICMP traffic.

F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; --service SMTP; --protocol tcp; )

The FortiGate unit will limit its search for the pattern to TCP traffic and ignore the pattern in UDP and ICMP network traffic.

6 Ignore case sensitivity

By default, patterns are case sensitive. If a user directed his or her browser to Example.com, the custom signature would not recognize the URL as a match.

Use the --no_case keyword to make the pattern matching case insensitive.
F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy";
    --service SMTP; --no_case; )

Unlike all of the other keywords in this example, the --no_case keyword has no value. Only the keyword is required.

7 Specify the context

The SMTP vrfy command will appear in the SMTP header. The --context host keyword/value pair allows you to limit the pattern search to only the header.

F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy";
    --service SMTP; --no_case; --context header; )

Configuring a Fortinet Security Processing module

The Example Corporation has a web site that is the target of SYN floods. While they investigate the source of the attacks, it’s very important that the web site remain accessible. To enhance the ability of the company’s FortiGate-620B to deal with SYN floods, the administrator will install an ASM-CE4 Fortinet Security Processing module and have all external access to the web server come through it.

The security processing modules not only accelerate and offload network traffic from the FortiGate unit’s processor, but they also accelerate and offload security and content scanning. The ability of the security module to accelerate IPS scanning and DoS protection greatly enhances the defense capabilities of the FortiGate-620B.

Assumptions

As shown in other examples and network diagrams throughout this document, the Example Corporation has a pair of FortiGate-620B units in an HA cluster. To simplify this example, the cluster is replaced with a single FortiGate-620B.

An ASM-CE4 is installed in the FortiGate-620B.

The network is configured as shown in Figure 10.

Network configuration

The Example Corporation network needs minimal changes to incorporate the ASM-CE4. Interface amc-sw1/1 of the ASM-CE4 is connected to the Internet and interface amc-sw1/1 is connected to the web server.

Since the main office network is connected to port2 and the Internet is connected to port1, a switch is installed to allow both port1 and amc-sw1/1 to be connected to the Internet.
The switch used to connect port1 and amc-sw1/1 to the Internet must be able to handle any SYN flood, all of the legitimate traffic to the web site, and all of the traffic to and from the Example Corporation internal network. If the switch cannot handle the bandwidth, or if the connection to the service provider cannot provide the required bandwidth, traffic will be lost.

**Security module configuration**

The Fortinet security modules come configured to give equal priority to content inspection and firewall processing. The Example Corporation is using a ASM-CE4 module to defend its web server against SYN flood attacks so firewall processing is a secondary consideration.

Use these CLI commands to configure the security module in ASM slot 1 to devote more resources to content processing, including DoS and IPS, than to firewall processing.

```cli
config system amc-slot
edit sw1
    set optimization-mode fw-ips
    set ips-weight balanced
    set ips-p2p disable
    set ips-fail-open enable
    set fp-disable none
    set ipsec-inb-optimization enable
    set syn-proxy-client-timer 3
    set syn-proxy-server-timer 3
end
```

These settings do not disable firewall processing. Rather, when the security module nears its processing capacity, it will chose to service content inspection over firewall processing.

**DoS sensor configuration**

Defend against anomaly-based attacks using a DoS sensor. For the SYN floods launched against the Example Corporation web site, the `tcp_syn_flood` anomaly is the best defense.
Create a DoS sensor for SYN flood protection
1. Go to UTM > Intrusion Protection > DoS Sensor.
2. Select Create New.
3. Enter Web site SYN protection for the DoS sensor name.
4. Select OK to create the sensor.

The default tcp_syn_flood threshold is 2000. This means that the configured action will be triggered when the number of TCP packets with the SYN flag set exceeds 2000 per second.

For some applications, this value will be too high, while for others it will be too low. One way to find the correct values for your environment is to set the action to Pass and enable logging. Observe the logs and adjust the threshold values until you can determine the value at which normal traffic begins to generate attack reports. Set the threshold above this value with the margin you want. Note that the smaller the margin, the more protected your network will be from DoS attacks, but your network traffic will also be more likely to generate false alarms.

Configure a DoS sensor for SYN flood protection
1. Go to UTM > Intrusion Protection > DoS Sensor.
2. Select the Web site SYN protection sensor and select the Edit icon.
3. Select Enable and Logging for the tcp_syn_flood anomaly.
4. Select the Proxy action for the tcp_syn_flood anomaly.
5. Enter the threshold value for the tcp_syn_flood anomaly.
6. Select OK.

With the action configured as Proxy, TCP packets with the SYN flag set will be passed until the threshold value is exceeded. At that point, TCP packets with the SYN flag set until their numbers fall below the threshold value.

The ASM-CE4 security module will intercept the packet, and reply to the client with a TCP packet that has the SYN and ACK flags set. If the connection request is legitimate, the client will reply with a packet that has the ACK flag set. The ASM-CE4 will then ‘replay’ this exchange to the server and allow the client and server to communicate directly.

If the client does not reply with the expected packet, the ASM-CE4 will close the connection. Therefore, if the security module receives a flood of SYN packets, they will be blocked. Only the legitimate connections will be allowed through to the server.

DoS policy configuration
Before the DoS sensor can begin examining network traffic, you must create and configure a DoS policy and specify the DoS sensor.

Create a DoS policy
1. Go to Firewall > DoS Policy.
2. Select Create New.
3. Select amc-sw1/1 for Source Interface/Zone.
4. Select all for Source Address.
5. Select all for Destination Address.
Intrusion protection IPS examples

7 Enable DoS Sensor and select the Web site SYN protection sensor from the list.
8 Select OK.

Virtual IP configuration
Traffic destined for the web server will arrive at the amc-sw1/1 interface. You must create a virtual IP mapping to have the ASM-CE4 direct the traffic to the web server.

Create a virtual IP mapping
1 Go to Firewall > Virtual IP > Virtual IP.
2 Select Create New.
3 In the Name field, enter web_server.
4 Select amc-sw1/1 as the External Interface.
5 Enter 172.20.120.212 as the External IP Address/Range.
6 Enter 10.11.201.120 as the Mapped IP Address/Range.
7 Select OK.

Firewall policy configuration
A firewall policy is required to allow traffic through to the web server. Further, the firewall policy must include the virtual IP so the traffic is directed to the web server.

Create a firewall policy
1 Go to Firewall > Policy > Policy.
2 Select Create New.
3 Select amc-sw1/1 for the Source Interface/Zone.
4 Select all for the Source Address.
5 Select amc-sw1/2 for the Destination Interface/Zone.
6 Select web_server for the Destination Address.
7 Select Enable NAT.
8 Select OK.

Attempts to connect to 172.20.120.212 will be forwarded to the web server with this firewall policy in place.

View proxy statistics
With a FortiGate security module installed, a CLI command displays the current proxy statistics.

At the CLI prompt, type execute npu-cli /dev/ce4_0 showsynproxy. The last nine lines will list the proxy statistics:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Proxied TCP Connections</td>
<td>434055223</td>
</tr>
<tr>
<td>Working Proxied TCP Connections</td>
<td>515699</td>
</tr>
<tr>
<td>Retired TCP Connections</td>
<td>433539524</td>
</tr>
<tr>
<td>Valid TCP Connections</td>
<td>0</td>
</tr>
<tr>
<td>Attacks, No Ack From Client</td>
<td>433539524</td>
</tr>
<tr>
<td>No SynAck From Server</td>
<td>0</td>
</tr>
<tr>
<td>Rst By Server (service not supported)</td>
<td>0</td>
</tr>
<tr>
<td>Client timeout setting</td>
<td>3 Seconds</td>
</tr>
<tr>
<td>Server timeout setting</td>
<td>3 Seconds</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total Proxied TCP Connections</td>
<td>The number of proxied TCP connection attempts since the FortiGate unit was restarted. This value is the sum of the working and retired connection totals.</td>
</tr>
<tr>
<td>Working Proxied TCP Connections</td>
<td>The number of TCP connection attempts currently being proxied.</td>
</tr>
<tr>
<td>Retired TCP Connections</td>
<td>The number of proxied TCP connection attempts dropped or allowed. These connection attempts are no-longer being serviced. This value is the sum of the valid and attacks totals.</td>
</tr>
<tr>
<td>Valid TCP Connections</td>
<td>The number of valid proxied TCP connection attempts.</td>
</tr>
<tr>
<td>Attacks, No Ack From Client</td>
<td>The number of proxied TCP connection attempts in which the client did not reply. These are typically attacks.</td>
</tr>
<tr>
<td>No SynAck From Server</td>
<td>The number of valid client connection attempts in which the server does not reply.</td>
</tr>
<tr>
<td>Rst By Server (service not supported)</td>
<td>The number of valid client connection attempts in which the server resets the connection.</td>
</tr>
<tr>
<td>Client timeout setting</td>
<td>The client time-out duration.</td>
</tr>
<tr>
<td>Server timeout setting</td>
<td>The server time-out duration.</td>
</tr>
</tbody>
</table>
Web filter

This section describes Fortigate web filtering for HTTP traffic. The three main parts of the web filtering function, the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service interact with each other to provide maximum control over what the Internet user can view as well as protection to your network from many Internet content threats. Web Content Filter blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic.

This section describes the Web Content Filter and URL Filter functions. For information on FortiGuard Web Filtering, see “FortiGuard Web Filter” on page 129.

The following topics are included in this section:

- Web filter concepts
- Web content filter
- URL filter
- SafeSearch
- Advanced web filter configuration
- Web filtering example

Web filter concepts

Web filtering is a means of controlling the content that an Internet user is able to view. With the popularity of web applications, the need to monitor and control web access is becoming a key component of secure content management systems that employ antivirus, web filtering, and messaging security. Important reasons for controlling web content include:

- lost productivity because employees are accessing the web for non-business reasons
- network congestion — when valuable bandwidth is used for non-business purposes, legitimate business applications suffer
- loss or exposure of confidential information through chat sites, non-approved email systems, instant messaging, and peer-to-peer file sharing
- increased exposure to web-based threats as employees surf non-business-related web sites
- legal liability when employees access/download inappropriate and offensive material
- copyright infringement caused by employees downloading and/or distributing copyrighted material.

As the number and severity of threats increase on the World Wide Web, the risk potential increases within a company’s network as well. Casual non-business related web surfing has caused many businesses countless hours of legal litigation as hostile environments have been created by employees who download and view offensive content. Web-based attacks and threats are also becoming increasingly sophisticated. Threats and web-based applications that cause additional problems for corporations include:
• spyware/grayware
• phishing
• pharming
• instant messaging
• peer-to-peer file sharing
• streaming media
• blended network attacks.

Spyware, also known as grayware, is a type of computer program that attaches itself to a user’s operating system. It does this without the user’s consent or knowledge. It usually ends up on a computer because of something the user does such as clicking on a button in a pop-up window. Spyware can track the user’s Internet usage, cause unwanted pop-up windows, and even direct the user to a host web site. For further information, visit the FortiGuard Center.

Some of the most common ways of grayware infection include:
• downloading shareware, freeware, or other forms of file-sharing services
• clicking on pop-up advertising
• visiting legitimate web sites infected with grayware.

Phishing is the term used to describe attacks that use web technology to trick users into revealing personal or financial information. Phishing attacks use web sites and email that claim to be from legitimate financial institutions to trick the viewer into believing that they are legitimate. Although phishing is initiated by spam email, getting the user to access the attacker’s web site is always the next step.

Pharming is a next generation threat that is designed to identify and extract financial, and other key pieces of information for identity theft. Pharming is much more dangerous than phishing because it is designed to be completely hidden from the end user. Unlike phishing attacks that send out spam email requiring the user to click to a fraudulent URL, pharming attacks require no action from the user outside of their regular web surfing activities. Pharming attacks succeed by redirecting users from legitimate web sites to similar fraudulent web sites that have been created to look and feel like the authentic web site.

Instant messaging presents a number of problems. Instant messaging can be used to infect computers with spyware and viruses. Phishing attacks can be made using instant messaging. There is also a danger that employees may use instant messaging to release sensitive information to an outsider.

Peer-to-peer (P2P) networks are used for file sharing. Such files may contain viruses. Peer-to-peer applications take up valuable network resources and may lower employee productivity but also have legal implications with the downloading of copyrighted or sensitive company material.

Streaming media is a method of delivering multimedia, usually in the form of audio or video to Internet users. Viewing streaming media impacts legitimate business by using valuable bandwidth.

Blended network threats are rising and the sophistication of network threats is increasing with each new attack. Attackers learn from each previous successful attack and enhance and update attack code to become more dangerous and fast spreading. Blended attacks use a combination of methods to spread and cause damage. Using virus or network worm techniques combined with known system vulnerabilities, blended threats
can quickly spread through email, web sites, and Trojan applications. Examples of blended threats include Nimda, Code Red, Slammer, and Blaster. Blended attacks can be designed to perform different types of attacks, which include disrupting network services, destroying or stealing information, and installing stealthy backdoor applications to grant remote access.

**Different ways of controlling access**

The methods available for monitoring and controlling Internet access range from manual and educational methods to fully automated systems designed to scan, inspect, rate and control web activity.

Common web access control mechanisms include:

- establishing and implementing a well-written usage policy in the organization on proper Internet, email, and computer conduct
- installing monitoring tools that record and report on Internet usage
- implementing policy-based tools that capture, rate, and block URLs.

The final method is the focus of this topic. The following information shows how the filters interact and how to use them to your advantage.

**Order of web filtering**

The FortiGate unit applies web filters in a specific order:

1. URL filter
2. FortiGuard Web Filter
3. web content filter
4. web script filter
5. antivirus scanning.

If you have blocked a FortiGuard Web Filter category but want certain users to have access to URLs within that pattern, you can use the Override within the FortiGuard Web Filter. This will allow you to specify which users have access to which blocked URLs and how long they have that access. For example, if you want a user to be able to access www.example.com for one hour, you can use the override to set up the exemption. Any user listed in an override must fill out an online authentication form that is presented when they try to access a blocked URL before the FortiGate unit will grant access to it. For more information, see “FortiGuard Web Filter” on page 129.

**Web content filter**

You can control web content by blocking access to web pages containing specific words or patterns. This helps to prevent access to pages with questionable material. You can also add words, phrases, patterns, wild cards and Perl regular expressions to match content on web pages. You can add multiple web content filter lists and then select the best web content filter list for each web filter profile.

Enabling web content filtering involves three separate parts of the FortiGate configuration:

- The firewall policy allows certain network traffic based on the sender, receiver, interface, traffic type, and time of day.
- The web filter profile specifies what sort of web filtering is applied.
- The web content filter list contains blocked and exempt patterns.
The web content filter feature scans the content of every web page that is accepted by a firewall policy. The system administrator can specify banned words and phrases and attach a numerical value, or score, to the importance of those words and phrases. When the web content filter scan detects banned content, it adds the scores of banned words and phrases in the page. If the sum is higher than a threshold set in the web filter profile, the FortiGate unit blocks the page.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create a web content filter list.
2. Add patterns of words, phrases, wildcards, and regular expressions that match the content to be blocked or exempted.
   - You can add the patterns in any order to the list. You need to add at least one pattern that blocks content.
3. In a web filter profile, enable the web content filter and select a web content filter list from the options list.

To complete the configuration, you need to select a firewall policy or create a new one. Then, in the firewall policy, enable UTM and select the appropriate web filter profile from the list.

Creating a web filter content list

You can create multiple content lists and then select the best one for each web filter profile.

To create a web filter content list

1. Go to UTM > Web Filter > Web Content Filter.
2. Select Create New.
3. Enter a Name for the new list.
4. Enter optional comments to identify the list.
5. Select OK.

Configuring a web content filter list

Once you have created the web filter content list, you need to add web content patterns to it. There are two types of patterns: Wildcard and Regular Expression.

You use the Wildcard setting to block or exempt one word or text strings of up to 80 characters. You can also use the wildcard symbols, such as "*" or "?", to represent one or more characters. For example, as a wildcard expression, forti*.com will match fortinet.com and forticare.com. The "*" represents any kind of character appearing any number of times.

You use the Regular Expression setting to block or exempt patterns of Perl expressions, which use some of the same symbols as wildcard expressions, but for different purposes. The "*" represents the character before the symbol. For example, fortii*.com will match fortinet.com and fortiicare.com. The symbol "*" represents "i" in this case, appearing any number of times.

The maximum number of web content patterns in a list is 5000.
To add a web content pattern

1. Go to UTM > Web Filter > Web Content Filter.
2. Select the web content filter list and choose Edit.
3. Select Create New.
4. Select Block or Exempt, as required, from the Action list.
5. Enter the content Pattern.
6. Select a Pattern Type from the drop-down list.
7. Select a Language for the pattern from the drop-down list if you need to change the default.
8. Enter a score for the banned pattern.
   The score can be left at the default value or set to another value. For more information, see "How content is evaluated" on page 117.
9. Select Enable.
10. Select OK.

How content is evaluated

Every time the web content filter detects banned content on a web page, it adds the score for that content to the sum of scores for that web page. You set this score when you create a new pattern to block the content. The score can be any number from zero to 99999. Higher scores indicate more offensive content. When the sum of scores equals or exceeds the threshold score, the web page is blocked. The default score for web content filter is 10 and the default threshold is 10. This means that by default a web page is blocked by a single match. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

Banned words or phrases are evaluated according to the following rules:

- The score for each word or phrase is counted only once, even if that word or phrase appears many times in the web page.
- The score for any word in a phrase without quotation marks is counted.
- The score for a phrase in quotation marks is counted only if it appears exactly as written.

The following table describes how these rules are applied to the contents of a web page. Consider the following, a web page that contains only this sentence: "The score for each word or phrase is counted only once, even if that word or phrase appears many times in the web page."
Enabling the web content filter and setting the content threshold

When you enable the web content filter, the web filter will block any web pages when the sum of scores for banned content on that page exceeds the content block threshold. The threshold will be disregarded for any exemptions within the web filter list.

To enable the web content filter and set the content block threshold
1. Go to UTM > Web Filter > Profile.
2. Select Create New to add a new web filter profile or select an existing profile and choose Edit.
3. Select Web Content Filter.
4. Select the web content list in the Option column.
5. Enter the threshold for the web content filter.
6. Select OK.

URL filter

You can allow or block access to specific URLs by adding them to the URL filter list. You add the URLs by using patterns containing text and regular expressions. The FortiGate unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message instead.

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.
When adding a URL to the URL filter list, follow these rules:

- Type a top-level URL or IP address to control access to all pages on a website. For example, `www.example.com` or `192.168.144.155` controls access to all pages at this website.

- Enter a top-level URL followed by the path and file name to control access to a single page on a website. For example, `www.example.com/news.html` or `192.168.144.155/news.html` controls access to the news page on this website.

- 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 using text and regular expressions (or wildcard characters). For example, `example.*` matches `example.com`, `example.org`, `example.net` and so on.

**Note:** URLs with an action set to exempt or pass are not scanned for viruses. If users on the network download files through the FortiGate unit from a trusted website, add the URL of this website to the URL filter list with an action to pass it so the FortiGate unit does not virus scan files downloaded from this URL.

### URL filter actions

You can select one of four actions for URL patterns you include in URL filter lists.

**Block**

Attempts to access any URLs matching the URL pattern are denied. The user will be presented with a replacement message.

**Allow**

Any attempt to access a URL that matches a URL pattern with an allow action is permitted. The traffic is passed to the remaining antivirus proxy operations, including FortiGuard Web Filter, web content filter, web script filters, and antivirus scanning.

Allow is the default action. If a URL does not appear in the URL list, it is permitted.

**Pass**

Traffic to, and reply traffic from, sites matching a URL pattern with a pass action will bypass all antivirus proxy operations, including FortiGuard Web Filter, web content filter, web script filters, and antivirus scanning.

Make sure you trust the content of any site you pass.

**Exempt**

Exempt is similar to Pass in that it allows trusted traffic to bypass the antivirus proxy operations, but it functions slightly differently. In general, if you’re not certain that you need to use the Exempt action, use Pass.

HTTP 1.1 connections are persistent unless declared otherwise. This means the connections will remain in place until closed or the connection times out. When a client loads a web page, the client opens a connection to the web server. If the client follows a link to another page on the same site before the connection times out, the same connection is used to request and receive the page data.
When you add a URL pattern to a URL filter list and apply the Exempt action, traffic sent to and replies traffic from sites matching the URL pattern will bypass all antivirus proxy operations, as with the Pass action. The difference is that the connection itself inherits the exemption. This means that all subsequent reuse of the existing connection will also bypass all antivirus proxy operations. When the connection times out, the exemption is cancelled.

For example, consider a URL filter list that includes example.com/files configured with the Exempt action. A user opens a web browser and downloads a file from the URL example.com/sample.zip. This URL does not match the URL pattern so it is scanned for viruses. The user then downloads example.com/files/beautiful.exe and since this URL does match the pattern, the connection itself inherits the exempt action. The user then downloads example.com/virus.zip. Although this URL does not match the exempt URL pattern, a previously visited URL did, and since the connection inherited the exempt action and was re-used to download a file, the file is not scanned.

If the user next goes to an entirely different server, like example.org/photos, the connection to the current server cannot be reused. A new connection to example.org is established. This connection is not exempt. Unless the user goes back to example.com before the connection to that server times out, the server will close the connection. If the user returns after the connection is closed, a new connection to example.com is created and it is not exempt until the user visits a URL that matches the URL pattern.

Web servers typically have short time-out periods. A browser will download multiple components of a web page as quickly as possible by opening multiple connections. A web page that includes three photos will load more quickly if the browser opens four connections to the server and downloads the page and the three photos at the same time. A short time-out period on the connections will close the connections faster, allowing the server to avoid unnecessarily allocating resources for a long period. The HTTP session time-out is set by the server and will vary with the server software, version, and configuration.

Using the exempt action can have unintended consequences in certain circumstances. You have a web site at example.com and since you control the site, you trust the contents and configure example.com as exempt. But example.com is hosted on a shared server with a dozen other different sites, each with a unique domain name. Because of the shared hosting, they also share the same IP address. If you visit example.com, your connection your site becomes exempt from any antivirus proxy operations. Visits to any of the 12 other sites on the same server will reuse the same connection and the data you receive is exempt from scanned.

Use of the exempt action is not suitable for configuration in which connections through the FortiGate unit use an external proxy. For example, you use proxy.example.net for all outgoing web access. Also, as in the first example, URL filter list that includes a URL pattern of example.com/files configured with the Exempt action. Users are protected by the antivirus protection of the FortiGate unit until a user visits a URL that matches the of example.com/files URL pattern. The pattern is configured with the Exempt action so the connection to the server inherits the exemption. With a proxy however, the connection is from the user to the proxy. Therefore, the user is entirely unprotected until the connection times out, no matter what site he visits.

Ensure you are aware of the network topology involving any URLs to which you apply the Exempt action.

Examples using exempt and pass actions

These examples illustrate the differences between the exempt and pass actions.
The URL filter list in use has a single entry: www.example.com/files/content/.

- With an exempt action, the user downloads the file www.example.com/files/content/eicar.com. This URL matches the URL filter list entry so the file is not scanned. Further, the connection itself inherits the exemption. The user next downloads www.example.com/virus/eicar.com. Although this does not match the URL filter list entry, the existing connection to example.com will be used so the file is not scanned.
- With a pass action, the user downloads the file www.example.com/files/content/eicar.com. This URL matches the URL filter list entry so the file is not scanned. The user next downloads www.example.com/virus/eicar.com. This does not match the URL filter entry so it will be scanned. The pass action does not affect the connection and every URL the user accesses is checked against the URL filter list.

The URL filter list in use has a single entry: www.domain.com/files/content/. The user's browser is configured to use an external web proxy. All user browsing takes advantage of this proxy.

- With an exempt action, the user downloads www.example.com/files/content/eicar.com through the proxy. This matches the URL filter list entry so the file is not scanned. Further, the connection to the proxy inherits the exemption. The user next downloads www.eicar.org/virus/eicar.com through the proxy. Although this does not match the URL filter list entry, the existing connection to the proxy will be used so the file is not scanned. In fact, until the user stops browsing long enough for the connection to time out, all the user web traffic is exempt and will not be scanned.
- With a pass action, the user downloads www.example.com/files/content/eicar.com through the proxy. This matches the URL filter list entry so the file is not scanned. The user next downloads www.eicar.org/virus/eicar.com through the proxy. This does not match the URL filter entry so it will be scanned. The pass action does not affect the connection and every URL the user accesses is checked against the URL filter list.

**General configuration steps**

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create a URL filter list.
2. Add URLs to the URL filter list.
3. Select a web filter profile or create a new one.
4. In the web filter profile, enable the **Web URL Filter** and select a URL filter list from the drop-down list.

To complete the configuration, you need to select a firewall policy or create a new one. Then, in the firewall policy, enable **UTM** and select the appropriate web filter profile from the list.

**Creating a URL filter list**

To create a URL filter list

1. Go to **UTM > Web Filter > URL Filter**.
2. Select **Create New**.
3. Enter a **Name** for the new URL filter list.
4 Enter optional comments to describe it.
5 Select OK.

Configuring a URL filter list

Each URL filter list can have up to 5000 entries. For this example, the URL www.example*.com will be used. You configure the list by adding one or more URLs to it.

To add a URL to a URL filter list

1 Go to UTM > Web Filter > URL Filter.
2 Select an existing list and choose Edit.
3 Select Create New.
4 Enter the URL, without the “http”, for example: www.example*.com.
5 Select a Type: Simple, Wildcard or Regular Expression.
   In this example, select Wildcard.
6 Select the Action to take against matching URLs: Exempt, Block, Allow, or Pass.
7 Select Enable.
8 Select OK.

SafeSearch

SafeSearch is a feature of popular search sites that prevents explicit web sites and images from appearing in search results. Although SafeSearch is a useful tool, especially in educational environments, the resourceful user may be able to simply turn it off. Enabling SafeSearch for the supported search sites enforces its use by rewriting the search URL to include the code to indicate the use of the SafeSearch feature.

Three search sites are supported:

<table>
<thead>
<tr>
<th>Search Site</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>Enforce the strict filtering level of safe search protection for Google search results by adding &amp;safe=on to search URL requests. Strict filtering removes both explicit text and explicit images from the search results.</td>
</tr>
<tr>
<td>Yahoo!</td>
<td>Enforce the strict filtering level of safe search protection for Yahoo! search results by adding &amp;vm=r to search URL requests. Strict filtering removed adult web, video, and images from search results.</td>
</tr>
<tr>
<td>Bing</td>
<td>Enforce the strict filtering level of safe search protection for Bing search results by adding adlt=strict to search URL requests. Strict filtering removes explicit text, images, and video from the search results.</td>
</tr>
</tbody>
</table>

Enabling SafeSearch — Web-based manager

1 Go to UTM > Web Filter > Profile.
2 Select the profile in which you want to enable SafeSearch and choose Edit.
3 Under the SafeSearch heading, select the check boxes for Google, Yahoo!, and Bing in the Options column.
4 Select OK.

The CLI can also be used to enable SafeSearch in a web filter profile. In this example, the safe_web web filter is configured to enable SafeSearch.
Enabling SafeSearch — CLI

```
config webfilter profile
  edit safe_web
  config web
    set safe-search bing google yahoo
  end
end
```

This enforces the use of SafeSearch in traffic controlled by the firewall policies using the web filter you configure.

Advanced web filter configuration

The Advanced Filter section of the web filter profile provides a number of advanced filtering options. The FortiGuard Web Filter options in the advance filter section are detailed in the FortiGuard Web Filter section, in "Advanced FortiGuard Web Filter configuration" on page 136.

ActiveX filter

Enable to filter ActiveX scripts from web traffic. Web sites using ActiveX may not function properly with this filter enabled.

Cookie filter

Enable to filter cookies from web traffic. Web sites using cookies may not function properly with this enabled.

Java applet filter

Enable to filter java applets from web traffic. Web sites using java applets may not function properly with this filter enabled.

Web resume download block

Enable to prevent the resumption of a file download where it was previously interrupted. With this filter enabled, any attempt to restart an aborted download will download the file from the beginning rather than resuming from where it left off.

This prevents the unintentional download of viruses hidden in fragmented files.

Note that some types of files, such as PDF, fragment files to increase download speed and enabling this option can cause download interruptions. Enabling this option may also break certain applications that use the Range Header in the HTTP protocol, such as YUM, a Linux update manager.

Block Invalid URLs

Select to block web sites when their SSL certificate CN field does not contain a valid domain name.

FortiGate units always validate the CN field, regardless of whether this option is enabled. However, if this option is not selected, the following behavior occurs:

- If the request is made directly to the web server, rather than a web server proxy, the FortiGate unit queries for FortiGuard Web Filtering category or class ratings using the IP address only, not the domain name.
• If the request is to a web server proxy, the real IP address of the web server is not known. Therefore, rating queries by either or both the IP address and the domain name is not reliable. In this case, the FortiGate unit does not perform FortiGuard Web Filtering.

HTTP POST action

Select the action to take with HTTP POST traffic. HTTP POST is the command used by your browser when you send information, such as a form you have filled-out or a file you are uploading, to a web server.

The available actions include:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Allow use of the HTTP POST command as normal.</td>
</tr>
<tr>
<td>Comfort</td>
<td>Use client comforting to slowly send data to the web server as the FortiGate unit scans the file. Use this option to prevent a server time-out when scanning or other filtering is enabled for outgoing traffic. The client comforting settings used are those defined in the protocol options profile selected in the firewall policy. For more information, see “Configuring client comforting” on page 56.</td>
</tr>
<tr>
<td>Block</td>
<td>Block the HTTP POST command. This will limit users from sending information and files to web sites. When the post request is blocked, the FortiGate unit sends the http-post-block replacement message to the web browser attempting to use the command.</td>
</tr>
</tbody>
</table>

**Web filtering example**

Web filtering is particularly important for protecting school-aged children. There are legal issues associated with improper web filtering as well as a moral responsibility not to allow children to view inappropriate material. The key is to design a web filtering system in such a way that students and staff do not fall under the same web filter profile in the FortiGate configuration. This is important because the staff may need to access websites that are off-limits to the students.

**School district**

The background for this scenario is a school district with more than 2300 students and 500 faculty and staff in a preschool, three elementary schools, a middle school, a high school, and a continuing education center. Each elementary school has a computer lab and the high school has three computer labs with connections to the Internet. Such easy access to the Internet ensures that every student touches a computer every day.

With such a diverse group of Internet users, it was not possible for the school district to set different Internet access levels. This meant that faculty and staff were unable to view websites that the school district had blocked. Another issue was the students’ use of proxy sites to circumvent the previous web filtering system. A proxy server acts as a go-between for users seeking to view web pages from another server. If the proxy server has not been blocked by the school district, the students can access the blocked website.

When determining what websites are appropriate for each school, the district examined a number of factors, such as community standards and different needs of each school based on the age of the students.

The district decided to configure the FortiGate web filtering options to block content of an inappropriate nature and to allow each individual school to modify the options to suit the age of the students. This way, each individual school was able to add or remove blocked sites almost immediately and have greater control over their students’ Internet usage.
In this simplified example of the scenario, the district wants to block any websites with the word **example** on them, as well as the website www.example.com. The first task is to create web content filter lists for the students and the teachers.

**To create a web content filter list for the students**
1. Go to *UTM > Web Filter > Web Content Filter*.
2. Select *Create New*.
3. Enter the *Name* of the new list: **Student Web Content List**.
4. Enter optional comments to identify the list.
5. Select *OK*.

**To create a web content filter list for the teachers**
1. Go to *UTM > Web Filter > Web Content Filter*.
2. Select *Create New*.
3. Enter the *Name* of the new list: **Teacher Web Content List**.
4. Enter optional comments to identify the list.
5. Select *OK*.

The next step is to configure the two web content filters that were just created. The first will be the Student Web Content List.

**To add a pattern to the student web content filter list**
1. Go to *UTM > Web Filter > Web Content Filter*.
2. Select the **Student Web Content List** and choose *Edit*.
3. Select *Create New*.
4. Enter the word **example** as the content block *Pattern*.
5. Leave the rest of the settings at their default values.
6. Select *OK*.

It might be more efficient if the Teacher Web Content List included the same blocked content as the student list. From time to time a teacher might have to view a blocked page. It would then be a matter of changing the *Action* from **Block** to **Allow** as the situation required.

**To change a pattern from Block to Exempt**
1. Go to *UTM > Web Filter > Web Content Filter*.
2. Select the **Teacher Web Content List** and choose *Edit*.
3. Select **example** from the *Pattern* list and choose *Edit*.
4. Select **Exempt** from the *Action* list.
5. Ensure that **Enable** is selected.
6. Select *OK*.

URL filter lists with filters to block unwanted web sites must be created for the students and teachers. For this example the URL **www.example.com** will be used.

**To create a URL filter for the students**
1. Go to *UTM > Web Filter > URL Filter*.
2. Select *Create New*. 
3 Enter **Student URL List** as the URL filter **Name**.
4 Enter optional comments to describe the contents of the list.
5 Select **OK**.
The URL filter for the students has been created. Now it must be configured.

**To configure the URL filter for the students**
1 Go to **UTM > Web Filter > URL Filter**.
2 Select **Student URL List** and choose **Edit**.
3 Select **Create New**.
4 Enter **www.example.com** in the **URL** field.
5 Select **Simple** from the **Type** list.
6 Select **Block** from the **Action** list.
7 Select **Enable**.
8 Select **OK**.

The teachers should be able to view the students’ blocked content, however, so an addition URL filter is needed.

**To create a URL filter for the teachers**
1 Go to **UTM > Web Filter > URL Filter**.
2 Select **Create New**.
3 Enter **Teacher URL List** as the URL filter **Name**.
4 Enter optional comments to describe the list.
5 Select **OK**.

**To configure the URL filter for the teachers**
1 Go to **UTM > Web Filter > URL Filter**.
2 Select **Teachers URL List** and choose **Edit**.
3 Select **Create New**.
4 Enter **www.example.com** in the **URL** field.
5 Select **Simple** from the **Type** list.
6 Select **Exempt** from the **Action** list.
7 Select **Enable**.
8 Select **OK**.

A web filter profile must be created for the students and the teachers.

**To create a web filter profile for the students**
1 Go to **UTM > Web Filter > Profile**.
2 Select **Create New**.
3 Enter **Students** as the **Profile Name**.
4 Enter optional comments to identify the profile.
5 Enable **Web Content Filter** and select **Student Web Content List** from the drop-down list.
6 Enable **Web URL Filter** and select **Student URL List** from the drop-down list.
7 Expand the Advanced Filter section.

8 Enable Web Resume Download Block.
Selecting this setting will block downloading parts of a file that have already been
downloaded and prevent the unintentional download of virus files hidden in fragmented
files. Note that some types of files, such as PDFs, are fragmented to increase
download speed, and that selecting this option can cause download interruptions with
these types.

9 Select OK.

To create a firewall policy for the students

1 Go to Firewall > Policy.
2 Select Create New.
3 Enable UTM.
4 Select Enable Web Filter.
5 Select Students from the web filter drop-down list.
6 Enter optional comments.
7 Select OK.

To create a web filter profile for the teachers

1 Go to UTM > Web Filter > Profile.
2 Select Create New.
3 Enter Teachers as the Profile Name.
4 Enter optional comments to identify the profile.
5 Enable Web Content Filter and select Teacher Web Content List from the list.
6 Enable Web URL Filter and select Teacher URL List from the list.
7 Expand the Advanced Filter section.
8 Enable Web Resume Download Block.
9 Select OK.

To create a firewall policy for Teachers

1 Go to Firewall > Policy.
2 Select Create New.
3 Enable UTM.
4 Select Enable Web Filter.
5 Select Teachers from the web filter drop-down list.
6 Enter optional comments.
7 Select OK.
FortiGuard Web Filter

This section describes FortiGuard Web Filter for HTTP and HTTPS traffic.

FortiGuard Web Filter is a managed web filtering solution available by subscription from Fortinet. FortiGuard Web Filter enhances the web filtering features supplied with your FortiGate unit by sorting billions of web pages into a wide range of categories users can allow or block. The FortiGate unit accesses the nearest FortiGuard Web Filter Service Point to determine the category of a requested web page, and then applies the firewall policy configured for that user or interface.

FortiGuard Web Filter includes over 45 million individual ratings of web sites that apply to more than two billion pages. Pages are sorted and rated into several dozen categories administrators can allow or block. Categories may be added or updated as the Internet evolves. To make configuration simpler, you can also choose to allow or block entire groups of categories. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

FortiGuard Web Filter ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. Users can notify the FortiGuard Web Filter Service Points if they feel a web page is not categorized correctly, so that the service can update the categories in a timely fashion.

The following topics are discussed in this section:

• Before you begin
• FortiGuard Web Filter and your FortiGate unit
• Enable FortiGuard Web Filter
• Advanced FortiGuard Web Filter configuration
• Add or change FortiGuard Web Filter ratings
• Create FortiGuard Web Filter overrides
• Customize categories and ratings
• FortiGuard Web Filter examples

Before you begin

Before you follow the instructions in this section, you should have a FortiGuard Web Filter subscription and your FortiGate unit should be properly configured to communicate with the FortiGuard servers. For more information about FortiGuard services, see the FortiGuard Center web page. You should also have a look at “Web filter concepts” on page 113.
**FortiGuard Web Filter and your FortiGate unit**

When FortiGuard Web Filter is enabled in a web filter profile, the setting is applied to all firewall policies that use this profile. When a request for a web page appears in traffic controlled by one of these firewall policies, the URL is sent to the nearest FortiGuard server. The URL category is returned. If the category is blocked, the FortiGate unit provides a replacement message in place of the requested page. If the category is not blocked, the page request is sent to the requested URL as normal.

**Order of web filtering**

The FortiGate unit applies web filters in a specific order:

1. URL filter
2. FortiGuard Web Filter
3. web content filter
4. web script filter
5. antivirus scanning.

The flowchart in Figure 11 on page 131 shows the steps involved in FortiGuard Web Filtering. Most features are included but some of the advanced options, including overrides, are not. The features appearing in the flowchart are described in this section.
Figure 11: FortiGuard Web Filter sequence of events

Start:
User attempts to load a URL

Query FortiGuard for URL category and classification

Strict Blocking?
Yes
- Is the URL category set to block or allow?
  - Yes: Deny access to the URL and stop any running quota timer
  - No: Allow access to the URL

No
- Is there a classification for this URL?
  - Yes: Is the URL classification set to block or allow?
    - Yes: Deny access to the URL and stop any running quota timer
    - No: Allow access to the URL
  - No: Deny access to the URL and stop any running quota timer

Is the URL category set to block or allow?
- Yes: Is there a classification for this URL?
  - Yes: Is the URL classification set to block or allow?
    - Yes: Deny access to the URL and stop any running quota timer
    - No: Allow access to the URL
  - No: Deny access to the URL and stop any running quota timer
- No: Is the URL category set to block or allow?
  - Yes: Is there a classification for this URL?
    - Yes: Is the URL classification set to block or allow?
      - Yes: Deny access to the URL and stop any running quota timer
      - No: Allow access to the URL
    - No: Deny access to the URL and stop any running quota timer
  - No: Deny access to the URL and stop any running quota timer

Is FortiGuard Quota exempt for the classification?
- Yes: Allow access to the URL
- No: Deny access to the URL and stop any running quota timer

Is FortiGuard Quota exempt for the category group?
- Yes: Allow access to the URL
- No: Deny access to the URL and stop any running quota timer

Is there any time remaining for this category group quota?
- Yes: Start the category group timer and allow access to the URL
- No: Deny access to the URL and stop any running quota timer

Is there any time remaining for this category quota?
- Yes: Start the category timer and allow access to the URL
- No: Deny access to the URL and stop any running quota timer

Is there any time remaining for this classification quota?
- Yes: Start the classification timer and allow access to the URL
- No: Deny access to the URL and stop any running quota timer

Is the URL category set to block or allow?
- Yes: Is there a classification for this URL?
  - Yes: Is the URL classification set to block or allow?
    - Yes: Deny access to the URL and stop any running quota timer
    - No: Allow access to the URL
  - No: Deny access to the URL and stop any running quota timer
- No: Is the URL category set to block or allow?
  - Yes: Is there a classification for this URL?
    - Yes: Is the URL classification set to block or allow?
      - Yes: Deny access to the URL and stop any running quota timer
      - No: Allow access to the URL
    - No: Deny access to the URL and stop any running quota timer
  - No: Deny access to the URL and stop any running quota timer
Enable FortiGuard Web Filter

FortiGuard Web Filter is enabled and configured within web filter profiles. Overrides, local categories, and local ratings are configured in UTM > Web Filter.

General configuration steps

1. Go to UTM > Web Filter > Profile.
2. Select the Edit icon of the web filter profile in which you want to enable FortiGuard Web Filter, or select Create New to add a new web filter profile.
3. Expand the FortiGuard Web Filtering section.
4. Under the FortiGuard Web Filtering heading, the Enable FortiGuard Web Filtering row allows you to enable the feature for HTTP and HTTPS traffic. Select either or both check boxes as required.
5. The category and classification tables allow you to block or allow access to general or more specific web site categories. Configure access as required.
6. Select OK to save the web filter profile.
7. To complete the configuration, you need to select the firewall policy controlling the network traffic you want to restrict. Then, in the firewall policy, enable UTM and select Enable Web Filter and select the appropriate web filter profile from the list.

Configuring FortiGuard Web Filter settings

FortiGuard Web Filter includes a number of settings that allow you to determine various aspects of the filtering behavior.

To configure FortiGuard Web Filter settings

1. Go to UTM > Web Filter > Profile.
2. Select the Edit icon of the web filter profile in which you want to enable FortiGuard Web Filter, or select Create New to add a new web filter profile.
3. Expand the FortiGuard Web Filtering section.
4. Select one or both of the HTTP and HTTPS check boxes in the row labeled FortiGuard Web Filtering to enable FortiGuard Web Filter for HTTP and HTTPS web traffic.

At least one of these check boxes must be selected for FortiGuard Web Filter to function for the protocol. Other web filter features, such as web content filter and URL filter, will function as configured, however.
5. Select FortiGuard Web Filtering Overrides to enable the overrides configured in UTM > Web Filter > Override. Select HTTP, HTTPS, or both to enable overrides. For more information, see “Create FortiGuard Web Filter overrides” on page 138.
6. Select OK to save your changes to the web filter profile.

Configuring FortiGuard Web Filter categories

Categories are a means to describe the content of web sites. FortiGuard Web Filter divides the web into dozens of categories in eight category groups.

Every URL and IP address is associated with one category. URLs and IP addresses that have not been rated are placed in the Unrated category so you can still apply actions, overrides, and quotas to them.
To configure the FortiGuard Web Filter categories

1. Go to UTM > Web Filter > Profile.
2. Select Create New to add a new web filter profile, or select an existing web filter profile and choose Edit to configure the FortiGuard Web Filter categories.
3. Expand the FortiGuard Web Filtering section.
4. Under the FortiGuard Web Filtering heading, the category groups are listed in a table. You can expand each category group to view and configure every category within the group. If you change the setting of a category group, all categories within the group inherit the change.
5. Select Allow to allow access to the sites within the category.
6. Select Block to restrict access to sites within the category. Users attempting to access a blocked site will receive a replacement message explaining that access to the site is blocked.
7. Select Log to record attempts to access sites in a category.
8. Select Allow Override to allow users to override blocked categories. For more information, see “Understanding administrative and user overrides” on page 138.

Before you can allow an override, you must create it (see “Create FortiGuard Web Filter overrides” on page 138) and then enable FortiGuard Web Filtering Overrides in the web filter profile.
9. Select OK.

Configuring FortiGuard Web Filter classifications

Classifications are assigned based on characteristics of the site, not the topic of the site content. For example, the cached content classification tells you the site caches content from other sites. It tells you nothing about what the content is.

Unlike categories, not every rated URL and IP address has an assigned classification.

To configure the FortiGuard Web Filter classifications

1. Go to UTM > Web Filter > Profile.
2. Select Create New to add a new web filter profile or select the web filter profile in which you want to configure the FortiGuard Web Filter categories and select Edit.
3. Expand the FortiGuard Web Filtering section.
   The classification table is listed below the category table.
4. Select Allow to allow access to the sites within the classification.
5. Select Block to restrict access to sites within the classification. Users attempting to access a blocked site will receive a replacement message explaining that access to the site is blocked.
6. Select Log to record attempts to access sites in a classification.
7. Select Allow Override to allow users to override blocked classifications.
   This option is not available unless you also:
   • select the Enable FortiGuard Web Filtering Overrides option that appears just before the table
   • create overrides in UTM > Web Filter > Override. For more information, see “Create FortiGuard Web Filter overrides” on page 138.
8. Select OK.
Configuring FortiGuard Web Filter usage quotas

In addition to using category and classification blocks and overrides to limit user access to URLs, you can set a daily timed access quota by category, category group, or classification. Quotas allow access for a specified length of time, calculated separately for each user. Quotas are reset every day at midnight.

Users must authenticate with the FortiGate unit. The quota is applied to each user individually so the FortiGate must be able to identify each user. One way to do this is to configure a firewall policy using the identity based policy feature. Apply the web filter profile in which you have configured FortiGuard Web Filter and FortiGuard Web Filter quotas to such a firewall policy.

Caution: The use of FortiGuard Web Filter quotas requires that users authenticate to gain web access. The quotas are ignored if applied to a firewall policy in which user authentication is not required.

When a user first attempts to access a URL, they’re prompted to authenticate with the FortiGate unit. When they provide their username and password, the FortiGate unit recognizes them, determines their quota allowances, and monitors their web use. The category and classification of each page they visit is checked and FortiGate unit adjusts the user’s remaining available quota for the category or classification.

Note: Editing the web filter profile resets the quota timers for all users.

To configure the FortiGuard Web Filter categories

1. Go to UTM > Web Filter > Profile.
2. Select an existing web filter profile and choose Edit to configure the FortiGuard Web Filter categories.
3. Expand the FortiGuard Web Filtering section.
4. Under the FortiGuard Web Filtering heading, the category groups are listed in a table. You can expand each category group to view and configure every category within the group.
5. Under the FortiGuard Quota heading, select Enable to activate the quota for the category, category group, or classification.
6. Select Hours, Minutes, or Seconds and enter the number of hours, minutes, or seconds. This is the daily quota allowance for each user.
7. Select OK.

Apply the web filter profile to an identity-based firewall policy. All the users subject to that policy are restricted by the quotas.

Quota hierarchy

You can apply quotas to categories, category groups, and classifications. Only one quota per user can be active at any one time. The one used depends on how you configure the FortiGuard Web Filter.
When a user visits a URL, the FortiGate unit queries the FortiGuard servers for the category and classification of the URL. From highest to lowest, the relative priority of the quotas are:

1. **Category**
2. **Classification**
3. **Category group**

So for example, the Business Oriented category group contains the Information Technology category. When a user visits a page in the Information Technology category, the FortiGate unit will check for quotas in sequence:

- Is there a quota set for the Information Technology category? If there is, the category quota timer is started and the user is allowed access to the URL. If no time remains in the category quota, the URL is blocked and the user cannot access it for the remainder of the day.

- If there is no quota set for the Information Technology category, is there a quota set for any classification that applies to the URL? If there is, the classification quota timer is started and the user is allowed access to the URL. If no time remains in the classification quota, the URL is blocked and the user cannot access it for the remainder of the day.

- If no quota is set, or no classification exists for the URL, is there a quota set for the Business Oriented category group? If there is, the category group quota timer is started and the user is allowed access to the URL. If no time remains in the category group quota, the URL is blocked and the user cannot access it for the remainder of the day.

- If there is no category group quota, the user is allowed to access the URL. Getting to this point means there are no quotas set for the page. The FortiGate unit will stop any running quota timer because the current URL has no quota.

Only one quota timer can be running at any one time for a single user. Whenever a quota timer is started or a page is blocked, the timer running, because of the previous URL access, is stopped. Similarly, a URL with no quotas will stop a quota timer still running because of the URL the user previously accessed.

**Quota exempt**

The quota checking sequence occurs for every URL the user accesses. This is true for every web page, and every element of the web page that is loaded. For example, if a user loads a web page, the quota is checked for the web page as soon as it is loaded. If there is a photo on the page, it is also checked and the quota is adjusted accordingly.

This can cause unexpected behavior. For example, if the web page a user loads is in the Information Technology category and it has a quota, the quota timer is started. The web page includes a number of graphics, so as these are loaded, each is checked and the appropriate quota is started. If they all share the same category rating, which they often will, there is no problem. However, if the last graphic or page element loaded comes from another site, the quota may not work as you expect. If the last graphic is an ad, loaded from a site categorized as Advertising, the Information Technology category quota timer will stop almost as soon as it is started because the FortiGate unit sees the ad URL and finds that it belongs to the Advertising category. If Advertising has a quota, its timer will start. If it is blocked or allowed, the Information Technology category quota timer is stopped and the user can view the page without using the quota set to limit the Information Technology category.
To solve this problem, you can configure a category, category group, or classification as exempt. This effectively allows the quota system to ignore it entirely. Any quota timer running when an exempt URL is encountered continues to run. An exempt category, category group, or classification can not have a quota. This may sound the same as simply disabling the quota and setting the FortiGuard Web Filter action to allow, but there is a difference. This difference is that the allow and block actions stop an already running quota timer, while the exempt action does not.

The exempt action is generally used for commonly accessed web pages that load elements from other sites that have different category ratings. Pages that load ads from advertising sites are the most common example.

### Checking quota usage

With quotas enabled, the FortiGate unit keeps track of quota usage for each user in each web filter profile. You can check the amount of quota usage for each user and their remaining time for each individual quota on the FortiGuard Quota page.

**To view FortiGuard Web Filter quota usage**

1. Go to **UTM > Web Filter > FortiGuard Quota**.
2. The table shows the users who have used some or all of their quota allowance. The total time used is listed by web filter profile for each user.
3. Select the **View** icon in any row to view the remaining quota for each category, category group, and classification. A category, category group, or classification displayed in bold type indicates the quota currently in use.

Quotas are reset every day at midnight.

### Advanced FortiGuard Web Filter configuration

The *Advanced Filter* section of the web filter profile provides a number of advanced filter options. The web filter options in the advance filter section unrelated to FortiGuard Web Filter are detailed in the web filter section, in "Advanced web filter configuration" on page 123.

**Provide Details for Blocked HTTP 4xx and 5xx Errors**

Enable to have the FortiGate unit display its own replacement message for 400 and 500-series HTTP errors. If the server error is allowed through, malicious or objectionable sites can use these common error pages to circumvent web filtering.

**Rate Images by URL (blocked images will be replaced with blanks)**

Enable to have the FortiGate retrieve ratings for individual images in addition to web sites. Images in a blocked category are not displayed even if they are part of a site in an allowed category.

Blocked images are replaced on the originating web pages with blank place-holders. Rated image file types include GIF, JPEG, PNG, BMP, and TIFF.

**Allow Websites When a Rating Error Occurs**

Enable to allow access to web pages that return a rating error from the FortiGuard Web Filter service.
If your FortiGate unit cannot contact the FortiGuard service temporarily, this setting determines what access the FortiGate unit allows until contact is re-established. If enabled, users will have full unfiltered access to all web sites. If disabled, users will not be allowed access to any web sites.

**Strict Blocking**

This setting determines when the FortiGate unit blocks a site. Enable strict blocking to deny access to a site if any category or classification assigned to the site is set to *Block*. Disable strict blocking to deny access to a site only if all categories and classifications assigned to the site are set to *Block*.

All rated URLs are assigned one or more categories. URLs may also be assigned a classification. If *Rate URLs by domain and IP address* is enabled, the site URL and IP address each carry separately assigned categories and classifications. Depending on the FortiGuard rating and the FortiGate configuration, a site could be assigned to at least two categories and up to two classifications.

**Rate URLs by Domain and IP Address**

Enable to have the FortiGate unit request the rating of the site by URL and IP address separately, providing additional security against attempts to bypass the FortiGuard Web Filter.

*Note:* FortiGuard Web Filter ratings for IP addresses are not updated as quickly as ratings for URLs. This can sometimes cause the FortiGate unit to allow access to sites that should be blocked, or to block sites that should be allowed.

**Block HTTP Redirects by Rating**

Enable to block HTTP redirects.

Many web sites use HTTP redirects legitimately but in some cases, redirects may be designed specifically to circumvent web filtering, as the initial web page could have a different rating than the destination web page of the redirect.

This option is not supported for HTTPS.

**Daily log of remaining quota**

Enable to log daily quota use.

As part of the quota reset at midnight, the FortiGate unit will record a log entry for every quota each user consumed during the day. These log entries are labeled with the sub-type *ftgd_quota*. Each entry includes the VDOM, user name, web filter profile name, category description, quota used (in seconds), and quota (in seconds). You can use log filtering to quickly limit the displayed entries to those you want, and generate reports from the logs.

**Add or change FortiGuard Web Filter ratings**

The FortiGuard Center web site allows you to check the current category assigned to any URL.

**To check the category assigned to a URL**

2. Enter the URL as directed.
3 Select Search.
4 If the URL has been rated by the FortiGuard web filter team, the category is displayed.
If a URL has not been rated, or you believe it is incorrectly rated, you can suggest the appropriate category and classification.

**To add or change the category for a URL**
1 Check the category assigned to the URL as described in the previous procedure.
2 Below the rating, select **Check to submit the URL**.
3 Enter your name, company, and email address.
4 Optionally, you may enter a comment.
5 Select the most appropriate category and classification for the URL.
6 Select **Submit** to send your submission to the FortiGuard web filter team.

---

**Create FortiGuard Web Filter overrides**

You can configure FortiGuard Web Filter to allow or deny access to web sites by category and classification. You may want to block a category but allow your users temporary access to one site within the blocked category. You may need to allow only some users to temporarily access one site within a blocked category. Do these things by using administrative and user overrides.

**Understanding administrative and user overrides**

The administrative overrides are backed up with the main configuration. The administrative overrides are not deleted when they expire and you can reuse them by extending their expiry dates. You can create administrative overrides either through the CLI or the web-based manager.

The user overrides are not backed up as part of the main configuration. These overrides are automatically deleted when they expire. You can only view and delete the user override entries. Users create user overrides using the authentication form opened from the block page when they attempt to access a blocked site, if override is enabled.

**To create an administrative override**
1 Go to **UTM > Web Filter > Override**.
2 Select **Administrative Overrides** and choose **Edit**.
3 Select **Create New**.
4 Using the **Type** selection, choose the type of override to create:
   - A **Directory** override will allow access to a particular directory on a blocked site.
   - An **Exact Domain** override will allow access to a blocked domain.
   - A **Categories** override will allow access to a blocked category.
5 If you select a directory or domain override, enter the directory or domain in the **URL** field.
   If you select a category override, select the categories and classifications you want to allow.
6 Using the Scope selection, choose how the override will be applied:
   • A User scope limits the override to a single user. Enter the user ID in the User field.
   • A User Group scope limits the override to the users you have included in a user group. Using the User Group selection, choose the user group.
   • An IP scope limits the override to an IPv4 address. Enter the address in the IP field.
   • An IPv6 scope limits the override to an IPv6 address. Enter the address in the IPv6 field.

7 Select whether to Allow or Deny content from Off-site URLs.
   This option defines whether the web page that is displayed as the result of an override will display the images and other contents from other blocked offsite URLs. For example, if all FortiGuard categories are blocked, but you want to allow access to a web site, you can create a domain override for the site and view the page. If the images on the site are served from a different domain and Off-site URLs is set to Deny, all the images on the page will appear broken because they come from a domain that the existing override rule does not apply to. If Off-site URLs is set to Allow, the images on the page will appear properly.

8 Select when the override expires by entering the exact time and date.

9 Select OK to save the override rule.

Customize categories and ratings

The FortiGuard Web Filter rating categories are general enough that virtually any web site can be accurately categorized in one of them. However, the rigid structure of the categories can create complications. For example, your company uses a web-based email provider. If you select the Web-based Email category, all sites categorized as web-based email providers, including the one your company uses, are blocked.

Local categories and local ratings allow you to assign sites to any category you choose. You can even create new categories. These settings apply only to your FortiGate unit. The changes you make are not sent to the FortiGuard Web Filter Service.

Creating local categories

Categories are labels that describe web site content. Creating your own category allows you to customize how the FortiGuard Web Filter service works.

Local categories appear in the web filter profile, under the FortiGuard Web Filter category list, in the Local Categories group. Local categories are empty when created. To populate local categories with web sites, see “Customizing site ratings” on page 139.

To create a local category
1 Go to UTM > Web Filter > Local Categories.
2 Enter the name of the new local category in the field above the local category list.
3 Select Add.
   The new local category is added to the list, but will remain empty until you add a web site to it.

Customizing site ratings

You may find it convenient to change the rating of a site. For example, if you want to block all the sites in a category except one, you can move the one site to a different category.
To customize a site rating
1. Go to UTM > Web Filter > Local Ratings.
2. Select Create New.
3. In the URL field, enter the URL of the site you want to change.
4. In the Category Rating table, select the category or categories to apply to the site.
   If you created any local categories, a Local Categories group will appear.
5. In the Classification Rating table, select a classification to apply to the site.
6. Select OK.

FortiGuard Web Filter examples

FortiGuard Web Filter can provide more powerful filtering to your network because you can use it to restrict access to millions of sites by blocking the categories they belong to.

Configuring simple FortiGuard Web Filter protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable FortiGuard Web Filter protection on a FortiGate unit located in a satellite office.

Creating a web filter profile

Most FortiGuard Web Filter settings are configured in a web filter profile. Web filter profiles are selected in firewall policies. This way, you can create multiple web filter profiles, and tailor them to the traffic controlled by the firewall policy in which they are selected. In this example, you will create one web filter profile.

To create a web filter profile — web-based manager
1. Go to UTM > Web Filter > Profile.
2. Select Create New.
3. In the Name field, enter basic_FGWF.
4. Select the FortiGuard Web Filtering check boxes for the HTTP and HTTPS traffic types.
5. Select the FortiGuard Web Filtering expand arrow.
7. Select OK to save the web filter profile.
To create a web filter profile — CLI

```
config webfilter profile
  edit basic_FGWF
    config http
      set options fortiguard-wf
    end
    config https
      set options fortiguard-wf
    end
    config ftgd-wf
      set deny g01 g02 g05
    end
end
```

Applying the web filter profile to a firewall policy

A web filter profile directs the FortiGate unit to scan network traffic only when it is selected in a firewall policy. When a web filter profile is selected in a firewall policy, its settings are applied to all the traffic the firewall policy handles.

To select the web filter profile in a firewall policy — web-based manager

1. Go to Firewall > Policy > Policy.
2. Select a policy and choose the Edit icon.
3. Enable UTM.
4. Select default from the Protocol Options list.
   
   UTM can not be enabled without selecting a protocol options profile. A default profile is provided.
5. Select the Enable Web Filter option.
6. Select the basic_FGWF profile from the list.
7. Select OK to save the firewall policy.

To select the web filter profile in a firewall policy — CLI

```
config firewall policy
  edit 1
    set utm-status enable
    set profile-protocol-options default
    set webfilter-profile basic_FGWF
  end
```

HTTP and HTTPS traffic handled by the firewall policy you modified will be monitored for attempts to access the blocked sites. A small office may have only one firewall policy configured. If you have multiple policies, consider enabling web filter scanning for all outgoing policies.

**Note:** If you have multiple policies, consider enabling web filter scanning for all outgoing policies.

**School district**

Continuing with the example in the Web filter section, you can use FortiGuard Web Filter to protect students from inappropriate material. For the first part of this example, see "Web filtering example" on page 124.
To enable FortiGuard Web Filter

1. Go to UTM > Web Filter > Profile.
2. Select the web filter profile named Students and choose Edit.
3. In the FortiGuard Web Filtering row, select both the HTTP and HTTPS options.
4. Select OK.

The Students web filter profile has FortiGuard Web Filter enabled, but all the categories are set to Allow. With this configuration, no sites are blocked.

To configure the sites to block

1. Go to UTM > Web Filter > Profile.
2. Select the web filter profile named Students and choose Edit.
3. Expand the FortiGuard Web Filter section.
4. In the category table, select Block for these categories: Potentially Liable, Controversial, and Potentially Non-productive.
5. Select OK to save the web filter profile.

The students will not be able to access any of the web sites in those three general categories or the categories within them.
Data leak prevention

The FortiGate data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. When you define sensitive data patterns, data matching these patterns will be blocked, logged, and archived, or any combination of these three actions, when passing through the FortiGate unit. You configure the DLP system 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 FortiGate unit.

This section describes how to configure the DLP settings.

The following topics are included:

- Data leak prevention concepts
- Enable data leak prevention
- DLP archiving
- DLP examples

Data leak prevention concepts

Data leak prevention examines network traffic for data patterns you specify. You define whatever patterns you want the FortiGate unit to look for in network traffic. The DLP feature is broken down into a number of parts.

DLP sensor

A DLP sensor is a package of DLP rules and DLP compound rules. To use DLP you must enable it in a firewall policy and select the DLP sensor to use. The traffic controlled by the firewall policy will be searched for the patterns defined in the DLP sensor. Matching traffic will be passed or blocked according to how you configured the DLP sensor and rules. You can also log the matching traffic.

DLP rule

Each DLP rule includes a single condition and the type of traffic in which the condition is expected to appear.

For example, the FortiGate DLP system includes a modifiable default rule consisting of a regular expression that you can use to find messages matching U.S. Social Security numbers (SSN). You can apply this sample DLP rule, called Email-US-SSN, to have the FortiGate unit examine the Email protocols SMTP, IMAP, and POP3 for messages in which the Body has Matches of the ASCII formatted Regular Expression of \b(?i000)([0-6]d[2]7(\[0-6]d\[7\{012\}\]\([-]0\)?(?!00) \d\d\3(?!0000)\d\4(\b|)W).

DLP rules allow you to specify various conditions depending on the type of traffic for which the rule is created. Table 17 on page 144 lists the available conditions by traffic type.
Table 17: Conditions available by traffic type for DLP rules

<table>
<thead>
<tr>
<th>Field</th>
<th>Email</th>
<th>HTTP</th>
<th>HTTPS</th>
<th>FTP</th>
<th>NNTP</th>
<th>IM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Body</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Subject</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sender</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>yes</td>
</tr>
<tr>
<td>Receiver</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Attachment Size</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Attachment type</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Attachment text</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Transfer size</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Binary file pattern</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Authenticated User</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>User group</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>File is/is not encrypted</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>URL</td>
<td>-</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Cookie</td>
<td>-</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>CGI parameters</td>
<td>-</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HTTP header</td>
<td>-</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Hostname</td>
<td>-</td>
<td>yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>File type</td>
<td>-</td>
<td>yes</td>
<td>-</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>File text</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Server</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
</tr>
</tbody>
</table>

The HTTPS protocol is only available on FortiGate units that do not support SSL content scanning and inspection. Units with SSL content scanning and inspection support include HTTPS GET and HTTPS POST as options within the HTTP protocol.

DLP compound rule

Compound rules allow you to require that all the conditions specified in multiple DLP rules are true before the action is taken. In this way, you can configure the FortiGate unit to search for very specific conditions. For example, you can create a DLP sensor containing two DLP rules, one that checks all email traffic for messages that have the word "credit" in the subject, and one that checks all email traffic for messages from the sender user43@example.com.

Multiple DLP rules in a DLP sensor are connected with a Boolean “or” operation. The FortiGate unit will find a match in network traffic if the word “credit” appears in the message subject, or if the message is from user43@example.com. If either condition is true, a match is found.

If the same rules are added to a compound rule, and the compound rule is added to the sensor, the rules in the compound are connected with a Boolean “and” operation. The FortiGate unit will find a match in network traffic if the word “credit” appears in the message subject and if the message is from user43@example.com. Both conditions must be true before a match is found.
Enable data leak prevention

DLP examines your network traffic for data patterns you specify. You must configure DLP in sequence.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1 Create one or more DLP rules.

DLP rules are the foundation of the data leak prevention feature. Each rule describes the attributes of a type of sensitive data. The DLP feature uses this information to detect sensitive data in network traffic.

2 Optionally, combine rules into compound rules.

When using individual rules, any matching rule triggers the action assigned to the rule. Combining rules into a compound rule and using the compound rule changes their behavior in that all the rules included in the compound rule must be true for the assigned action to be triggered.

3 Create a DLP sensor.

New DLP sensors are empty. DLP sensors allow you to combine the DLP rules you've created for different purposes.

4 Add one or more DLP rules and compound rules to the DLP sensor.

New sensors contain no rules and therefore will match no traffic. You must add one or more rules and compound rules to a DLP sensor.

5 Add the DLP sensor to one or more firewall policies that control the traffic to be examined.

Creating a DLP rule

The DLP rules define the data to be protected so the FortiGate unit can recognize it. For example, the FortiGate default sensor rules include one that uses regular expressions to describe the U.S. Social Security Number:

```
\b(?i000)\([0-6]\d(2)\|7([0-6]\d|7[012])\)\(\s-\)?(?i00)
\d\d\d(?i0000)\d(4)\(\s\|\W
```

Rather than having to list every possible Social Security Number, this regular expression describes the structure of a Social Security Number. With the pattern, the FortiGate unit recognizes any numbers that follow the pattern.

To create a DLP rule

1 Go to UTM > Data Leak Prevention > Rule.

2 Select Create New.

3 In the Name field, enter the name of the new DLP rule.

4 Use the Protocol selection to choose the type of network traffic the FortiGate unit will examine for the presence of the conditions in the DLP rule.

Changing the protocol can change the available sub-protocol and rule options.

If your FortiGate unit does not support SSL content scanning and inspection, HTTPS will still be an available protocol selection. Although the contents of HTTPS traffic cannot be examined, HTTPS traffic can be detected, allowed or denied, and logged. If
your FortiGate unit does support SSL content scanning and inspection, HTTPS POST and HTTPS GET appear in the HTTP protocol. For more information, see “SSL content scanning and inspection” on page 27.

5 Below the protocol selection, select the sub-protocols the FortiGate unit will examine for the presence of the conditions in the DLP rule:

**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 and your FortiGate 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.

**HTTP POST, HTTP GET**
When you select the HTTP protocol, you can configure the rule to apply to HTTP post traffic, HTTP get traffic, or both traffic types.

**HTTPS POST, HTTPS GET**
When you select the HTTP protocol and your FortiGate unit supports SSL content scanning and inspection, you can also configure the HTTP rule to apply to HTTPS get traffic, HTTPS post traffic, or both traffic types. To scan these encrypted traffic types, you must select *Enable Deep Scanning* in the HTTPS section of the protocol options profile. If *Enable Deep Scanning* is not 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 traffic, FTP get traffic, or both traffic types.

**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.

6 If you select file or attachment rules in a protocol that supports it, you can select various *File options* to configure how the DLP rule handles archive files, MS Word files, and PDF files found in content traffic.

**Scan archive contents**
When selected, files within archives are extracted and scanned in the same way as files that are not archived.

**Scan archive files whole**
When selected, archives are scanned as a whole. The files within the archive are not extracted and scanned individually.

**Scan MS-Word text**
When selected, the text contents of MS Word DOC documents are extracted and scanned for a match. All metadata and binary information is ignored.  
*Note:* Office 2007/2008 DOCX files are not recognized as MS-Word by the DLP scanner. To scan the contents of DOCX files, select the *Scan archive contents* option.

**Scan MS-Word file whole**
When selected, MS Word DOC files are scanned. All binary and metadata information is included.  
If you are scanning for text entered in a DOC file, use the *Scan MS-Word* option. Binary formatting codes and file information may appear within the text, causing text matches to fail.  
*Note:* Office 2007/2008 DOCX files are not recognized as MS-Word by the DLP scanner. To scan the contents of DOCX files, select the *Scan archive contents* option.
### Scan PDF text
When selected, the text contents of PDF documents are extracted and scanned for a match. All metadata and binary information is ignored.

### Scan PDF file whole
When selected, PDF files are scanned. All binary and metadata information is included.
If you are scanning for text in PDF files, use the **Scan PDF Text** option. Binary formatting codes and file information may appear within the text, causing text matches to fail.

7 Select the **Rule** that defines the condition the FortiGate unit will search for.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>This option will cause an automatic match of the selected protocol and sub-protocols, regardless of the contents of the network traffic itself.</td>
<td>Email, HTTP, HTTPS, FTP, NNTP, IM, Session Control</td>
</tr>
<tr>
<td>Attachment size</td>
<td>Check the attachment file size.</td>
<td>Email</td>
</tr>
<tr>
<td>Attachment text</td>
<td>Search email attachments for the specified text.</td>
<td>Email</td>
</tr>
<tr>
<td>Attachment type</td>
<td>Search email attachments for file types or file patterns as specified in the selected file filter.</td>
<td>Email</td>
</tr>
<tr>
<td>Authenticated User</td>
<td>Search for traffic from the specified authenticated user.</td>
<td>Email, HTTP, FTP, NNTP, IM</td>
</tr>
<tr>
<td>Binary file pattern</td>
<td>Search for the specified binary string in network traffic.</td>
<td>Email, HTTP, FTP, NNTP, IM</td>
</tr>
<tr>
<td>Body</td>
<td>Search for the specified string in the message or page body.</td>
<td>Email, HTTP, NNTP</td>
</tr>
<tr>
<td>CGI parameters</td>
<td>Search for the specified CGI parameters in any web page with CGI code.</td>
<td>HTTP</td>
</tr>
<tr>
<td>Cookie</td>
<td>Search the contents of cookies for the specified text.</td>
<td>HTTP</td>
</tr>
<tr>
<td>File is/not encrypted</td>
<td>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 FortiGate unit cannot scan their contents.</td>
<td>Email, HTTP, FTP, NNTP, IM</td>
</tr>
<tr>
<td>File text</td>
<td>Search for the specified text in transferred text files.</td>
<td>FTP, NNTP, IM</td>
</tr>
<tr>
<td>File type</td>
<td>Search for the specified file patterns and file types. The patterns and types are configured in file filter lists, and a list is selected in the DLP rule.</td>
<td>HTTP, FTP, NNTP, IM</td>
</tr>
<tr>
<td>Hostname</td>
<td>Search for the specified host name when contacting an HTTP server.</td>
<td>HTTP</td>
</tr>
<tr>
<td>HTTP header</td>
<td>Search for the specified string in HTTP headers.</td>
<td>HTTP</td>
</tr>
<tr>
<td>Receiver</td>
<td>Search for the specified string in the message recipient email address.</td>
<td>Email</td>
</tr>
<tr>
<td>Sender</td>
<td>Search for the specified string in the message sender user ID or email address. For email, the sender is determined by the “From:” address in the email header. For IM, all members of an IM session are senders, and the senders are determined by finding the IM user IDs in the session.</td>
<td>Email, IM</td>
</tr>
<tr>
<td>Server</td>
<td>Search for the server’s IP address in a specified address range.</td>
<td>FTP, NNTP</td>
</tr>
<tr>
<td>Subject</td>
<td>Search for the specified string in the message subject.</td>
<td>Email</td>
</tr>
</tbody>
</table>
Enable data leak prevention

<table>
<thead>
<tr>
<th>Transfer size</th>
<th>Check the total size of the information transfer. For email traffic, for example, the transfer size includes the message header, body, and any encoded attachment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Search for the specified URL in HTTP traffic.</td>
</tr>
<tr>
<td>User group</td>
<td>Search for traffic from any user in the specified user group.</td>
</tr>
</tbody>
</table>

8 Select the required rule operators, if applicable:

matches/does not match This operator specifies whether the FortiGate unit is searching for the presence or absence of a 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.

is/is not This operator specifies if the rule is triggered when a condition is true or not true.
  - is: The rule will be triggered if the rule is true.
  - is not: The rule will be triggered if the rule is not true.
  - For example, if a rule specifies that a file type is found within a specified file type list, all matching files will trigger the rule. Conversely, if the rule specifies that a file type is not found in a file type list, only the file types not in the list would trigger the rule.

==/>=/<=/!= These operators allow you to compare the size of a transfer or attached file to an entered value.
  - == is equal to the entered value.
  - >= is greater than or equal to the entered value.
  - <= is less than or equal to the entered value.
  - != is not equal to the entered value.

9 Enter the data pattern, if the rule type you selected requires it.

Most rules types end with a field or selection of the data pattern to be matched, whether it is a file size, text string, email address, or file name.

10 Select OK.

Understanding the default DLP rules

A number of default DLP rules are provided with your FortiGate unit. You can use these as provided, or modify them as required.

Note: These rules affect only unencrypted traffic types. If you are using a FortiGate unit that can decrypt and examine encrypted traffic, you can enable those traffic types in these rules to extend their functionality if required.

Caution: Before using the rules, examine them closely to ensure you understand how they will affect the traffic on your network.
Creating a compound DLP rule

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 condition. When this condition 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 condition, but the conditions of every included rule must be detected before the compound rule is activated.

If only some of the conditions specified in the rules within a compound rule are detected, the compound rule is not triggered.

To create a compound DLP rule

1. Go to UTM > Data Leak Prevention > Compound.
2. Select Create New.
3. In the Name field, enter the name of the new DLP compound rule.
4. Use the Protocol selection to filter the available DLP rules based on their protocol settings. For example, if you select the Email protocol, only the DLP rules configured with the email protocol will appear for you to select.
5. Below the protocol selection, select the required sub-protocols to further restrict which rules will appear for you to choose.
6. Select the first DLP rule to include in the compound rule from the Rule drop-down list.
7. Select the blue “plus” icon to add a second rule. Each subsequent rule will allow you to add another so you can add as many DLP rules as you require. Similarly, the blue “minus” icon allows you to delete the last added rule.
8. Select OK.

Creating a DLP sensor

DLP sensors are collections of DLP rules and DLP compound rules. You must also specify an action for the rule or compound rule when you add it to a sensor. Once a DLP sensor is configured, it can be selected in a firewall policy profile. Any traffic handled by the firewall policy will be examined according to the DLP sensor configuration.
To create a DLP sensor

1. Go to UTM > Data Leak Prevention > Sensor.
2. Select Create New.
3. In the Name field, enter the name of the new DLP compound rule.
4. Optionally, you may also enter a comment. The comment appears in the DLP sensor list and can remind you of the details of the sensor.
5. Select OK.

The DLP sensor is created and the sensor configuration window appears.

6. Select Enable Logging to have the FortiGate unit record details of DLP operation to the DLP log.
7. Select Enable NAC Quarantine Logging to have the FortiGate unit record details of DLP operation involving the ban and quarantine actions to the event log. This allows you to be notified about NAC quarantine events by alert email if necessary. For this to function correctly, the event log must be enabled with the NAC Quarantine event option enabled.
8. Select OK.

A newly created sensor is empty, containing no rules or compound rules. Without rules, the DLP sensor will do nothing.

Adding rules to a DLP sensor

Once you have created a DLP sensor, you need to add DLP rules.

To add rules to a DLP sensor

1. Go to UTM > Data Leak Prevention > Sensor.
2. Select the DLP sensor to which you want to add the rule and choose Edit.
3. Select Create New.
4. Select the Action the FortiGate unit will take against network traffic matching the rule. A number of actions are available:
Data leak prevention

Enable data leak prevention

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>The FortiGate unit will take no action on network traffic matching a rule with this action. Other matching rules in the same sensor and other sensors may still operate on matching traffic.</td>
</tr>
<tr>
<td>Block</td>
<td>Traffic matching a rule with the block action will not be delivered. The matching message or download is replaced with the data leak prevention replacement message.</td>
</tr>
<tr>
<td>Exempt</td>
<td>The exempt action prevents any DLP sensors from taking action on matching traffic. This action overrides the action assigned to any other matching sensors.</td>
</tr>
<tr>
<td>Ban</td>
<td>If the user is authenticated, this action blocks all traffic to or from the user using the protocol that triggered the rule and adds the user to the Banned User list. If the user is not authenticated, this action blocks all traffic of the protocol that triggered the rule from the user’s IP address. If the banned user is using HTTP, FTP, or NNTP (or HTTPS if the FortiGate unit supports SSL content scanning and inspection) the FortiGate unit displays the “Banned by data leak prevention” replacement message for the protocol. If the user is using IM, the IM and P2P “Banned by data leak prevention” message replaces the banned IM message and this message is forwarded to the recipient. If the user is using IMAP, POP3, or SMTP (or IMAPS, POP3S, SMTPS if your FortiGate unit supports SSL content scanning and inspection) the Mail “Banned by data leak prevention” message replaces the banned email message and this message is forwarded to the recipient. These replacement messages also replace all subsequent communication attempts until the user is removed from the banned user list.</td>
</tr>
<tr>
<td>Ban Sender</td>
<td>This action blocks email or IM traffic from the sender of matching email or IM messages and adds the sender to the Banned User list. This action is available only for email and IM protocols. For email, the sender is determined by the From: address in the email header. For IM, all members of an IM session are senders and the senders are determined by finding the IM user IDs in the session. Similar to Ban, IM or Mail “Banned by data leak prevention” message replaces the banned message and this message is forwarded to the recipient. These replacement messages also replace all subsequent communication attempts until the user is removed from the banned user list.</td>
</tr>
<tr>
<td>Quarantine IP address</td>
<td>This action blocks access for any IP address that sends traffic matching a sensor with this action. The IP address is added to the Banned User list. The FortiGate unit displays the “NAC Quarantine DLP Message” replacement message for all connection attempts from this IP address until the IP address is removed from the banned user list.</td>
</tr>
<tr>
<td>Quarantine Interface</td>
<td>This action blocks access to the network for all users connecting to the interface that received traffic matching a sensor with this action. The FortiGate unit displays the “NAC Quarantine DLP Message” replacement message for all connection attempts to the interface until the interface is removed from the banned user list.</td>
</tr>
</tbody>
</table>

*Caution*: If you have configured DLP to block IP addresses and if the FortiGate unit receives sessions that have passed through a NAT device, all traffic from that NAT device—not just traffic from individual users—could be blocked. You can avoid this problem by implementing authentication or, where possible, select Ban Sender. 

Ban, Ban Sender, Quarantine IP, and Quarantine Interface provide functionality similar to NAC quarantine. However, these DLP options block users and IP addresses at the application layer while NAC quarantine blocks IP addresses and interfaces at the network layer.
Enable data leak prevention

Tip: To view or modify the replacement message text, go to System > Config > Replacement Message.

5 Select how traffic matching the rule will be archived.

- **Disable**: Do not archive network traffic matching the rule.
- **Summary Only**: Archive a summary of matching network traffic.
  - For example, if applied to a rule governing email, the information archived includes the sender, recipient, message subject, message size, and other details.
- **Full**: Archive the matching network traffic in addition to the summary information.
  - For example, full archiving of email traffic includes the email messages and any attached files.

Note: Archiving requires a FortiAnalyzer device or a subscription to the FortiGuard Analysis and Management Service.

6 If you selected one of the ban or quarantine actions, the Expires setting allows you to choose how long the offending user/address/interface will remain on the banned user list.

- Select **Indefinitely** to keep the banned user entry in place until it is manually deleted.
- Select **After** to enter the number of minutes, hours, or days, after which the banned user entry is automatically deleted.

7 Choose the **Severity** rating to be attached to log entries created when network traffic matches any rules in the sensor.

The severity setting has no effect on how DLP functions. It only affects DLP log entries and the reports generated from the logs.

8 Select the type of rule you want to add to the DLP sensor using the **Member type** drop-down list. You may choose either **Rule** or **Compound rule**, and the list below your selection will display only the type you choose.

9 From the table, select the rule or compound rule to add to the DLP sensor.

10 Select **OK**.

The rule is added to the sensor. You may select **Create New** to add more rules, or select **OK** to return to the DLP sensor list.

### Understanding default DLP sensors

A number of default DLP sensors are provided with your FortiGate unit. You can use these as provided, or modify them as you require.

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.

Note: DLP prevents duplicate action. Even if more than one rule in a sensor matches some content, DLP will not create more than one content archive entry, quarantine item, or ban entry from the same content.
DLP archiving

DLP is typically used to prevent sensitive information from getting out of your company network, but it can also be used to record network use. This is called DLP archiving. The DLP engine examines email, FTP, IM, NNTP, and web traffic. Enabling archiving for rules when you add them to sensors directs the FortiGate unit to record all occurrences of these traffic types when they are detected by the sensor.

Since the archive setting is configured for each rule in a sensor, you can have a single sensor that archives only the things you want.

DLP archiving comes in two forms: Summary Only, and Full.

Summary archiving records information about the supported traffic types. For example, when an email message is detected, the sender, recipient, message subject, and total size are recorded. When a user accesses the Web, every URL the user visits recorded. The result is a summary of all activity the sensor detected.

For more detailed records, full archiving is necessary. When an email message is detected, the message itself, including any attachments, is archived. When a user accesses the Web, every page the user visits is archived. Far more detailed than a summary, full DLP archives require more storage space and processing.

Because both types of DLP archiving require additional resources, DLP archives are saved to a FortiAnalyzer unit or the FortiGuard Analysis and Management Service (subscription required).

Two sample DLP sensors are provided with DLP archiving capabilities enabled. If you select the Content_Summary sensor in a firewall policy, it will save a summary DLP archive of all traffic the firewall policy handles. Similarly, the Content_Archive sensor will save a full DLP archive of all traffic handled the firewall policy you apply it to. These two sensors are configured to detect all traffic of the supported types and archive them.
DLP examples

Configuring DLP content archiving

This example details how to enable DLP content archiving on a FortiGate unit located in a satellite office. With this DLP sensor selected in a firewall policy, all email, FTP, HTTP, IM, and NNTP traffic controlled by the policy is saved to your FortiAnalyzer unit. This example assumes the FortiGate unit is configured to send all logs to a FortiAnalyzer unit or to the FortiGuard Analysis and Management Service.

Using the DLP content archive sensor

DLP sensors are created by selecting DLP rules. Each rule specifies a condition and an action. When the condition is true, the action is taken.

Your FortiGate unit comes with a sample DLP sensor that generates a DLP content archive of all email, FTP, HTTP, IM, and NNTP traffic.

Selecting the DLP sensor in a firewall policy

A DLP sensor directs the FortiGate unit to scan network traffic only when it is selected in a firewall policy. When a DLP sensor is selected in a firewall policy, its settings are applied to all the traffic the firewall policy handles.

To select the DLP content archive sensor in a firewall policy — web-based manager

1. Go to Firewall > Policy > Policy.
2. Select a policy and choose the Edit icon.
3. Enable UTM.
4. Select the Enable DLP Sensor option.
5. Select default from the Protocol Options list.
   DLP can not be enabled without selecting a protocol options profile. A default profile is provided.
6. Select the Content_Archive sensor from the list.
7. Select OK to save the firewall policy.

To select the antivirus profile in a firewall policy — CLI

```
config firewall policy
    edit 1
        set utm-status enable
        set profile-protocol-options default
        set dlp-sensor Content_Archive
    end
```

All email, FTP, HTTP, IM, and NNTP traffic handled by the firewall policy you modified will be archived. A small office may have only one firewall policy configured. If you have multiple policies, select the Content_Archive sensor in every policy you want archived.

Blocking sensitive email messages

Someone in the Example.com corporation has been sending copies of the company president’s monthly update email messages to the press. These messages have included the full header. Rather than try to block them, the IT department at Example.com will find out who is sending the messages using DLP.
All messages include the text From: president@example.com and Subject: XYZ Monthly Update where XYZ is the month the update applies to.

You will create a rule for the email address and a rule for the subject, combine them in a compound rule, and add the compound rule to a DLP sensor. You will then add the DLP sensor to the firewall policy that controls outgoing email traffic.

To create the “address” rule
1. Go to UTM > Data Leak Prevention > Rule.
2. Select Create New.
3. In the Name field, enter President address.
4. In the Comments field, enter Finds “president@example.com” in email.
5. For Protocol, select Email.
6. Select the SMTP, IMAP, and POP3 check boxes.
7. Select the Body rule.
8. For the three drop-down menus in the Body row, select, matches, ASCII, and Wildcard.
9. In the final field in the Body row, enter president@example.com
10. Select OK to save the rule.

To create the “subject” rule
1. Go to UTM > Data Leak Prevention > Rule.
2. Select Create New.
3. In the Name field, enter President subject.
4. In the Comments field, enter Finds “XYZ Monthly Update” in email.
5. For Protocol, select Email.
6. Select the SMTP, IMAP, and POP3 check boxes.
7. Select the Body rule.
8. For the three drop-down menus in the Body row, select, matches, ASCII, and Wildcard.
9. In the final field in the Body row, enter * Monthly Update
   The asterisk (“*”) can represent any characters so the rule will match any monthly update.
10. Select OK to save the rule.

Adding these two rules to a DLP sensor may generate a large number of false positives because any rule in a sensor will trigger the action. If the action were to log messages matching the address and subject rules in this example, then left as individual rules, the DLP sensor would log Monthly Updates from any employee and log all the president’s email messages. In this case, you only want to know when both rules are true for a single message. To do this, you must first add the rules to a compound rule.

To create the “president + subject” compound rule.
1. Go to UTM > Data Leak Prevention > Compound.
2. Select Create New.
3. In the Name field, enter President + subject.
4. For Protocol, select Email.
5. Select the SMTP, IMAP, and POP3 check boxes.
6  In the Rules drop-down menu, select President address.
7  Select the blue Add Rule button.
8  In the second Rules drop-down menu, select President subject.
9  Select OK to save this compound rule.

To create the “president” DLP sensor

1  Go to UTM > Data Leak Prevention > Sensor.
2  Select Create New.
3  In the Name field, enter president.
4  In the Comments field, enter Finds “president@example.com” and “XYZ Monthly Update” in email.
5  Select OK to save the new sensor.
6  Select Enable Logging so the activity of this sensor will be logged.
7  Select Create New to add a rule to the sensor.
8  Set the Action to None.
9  Set Member type to Compound rule.
10 Select the President + subject rule.
11 Select OK.

With the DLP sensor ready for use, you need to select it in the firewall policy.

To select the DLP sensor in the firewall policy

1  Go to Firewall > Policy > Policy.
2  Select the firewall policy that controls outgoing email traffic.
3  Select the Edit icon.
4  Enable UTM.
5  Select default from the Protocol Options list.
   UTM can not be enabled without selecting a protocol options profile. A default profile is provided.
6  Select the Enable DLP Sensor option.
7  Select the president sensor from the list.
8  Select OK to save the firewall policy.

With the DLP sensor specified in the correct firewall policy, any email message with both president@example.com and Monthly Update in the message body will trigger the sensor and a DLP log entry will be created. The sender IP address is recorded and this will indicate which computer was used to send the message.
Application control

Using the application control UTM feature, your FortiGate unit can detect and take action against network traffic depending on the application generating the traffic. Based on FortiGate Intrusion Protection protocol decoders, application control is a user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the FortiGate 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 FortiGate unit can recognize the network traffic generated by a large number of applications. You can create application control 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, and then add application control lists to the firewall policies that control the network traffic you need to monitor.

This section describes how to configure the application control settings.

If you enable virtual domains (VDOMs) on the Fortinet unit, you need to configure application control separately for each virtual domain.

The following topics are included in this section:

- Application control concepts
- Enable application control
- Application traffic shaping
- Application control monitor
- Application control packet logging
- Application considerations
- Application control examples

Application control concepts

You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the firewall policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.

Updated and new application signatures are delivered to your FortiGate unit as part of your FortiGuard Application Control Service subscription. Fortinet is constantly increasing the number 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.

To view the version of the application control database installed on your FortiGate unit, go to the License Information dashboard widget and find the IPS Definitions version.
To see the complete list of applications supported by FortiGuard Application Control go to the FortiGuard Application Control List. This web page lists all of the supported applications. You can select any application name to see details about the application.

Enable application control

Application control examines your network traffic for traffic generated by the applications you want it to control.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create an application control list.
2. Configure the list to include the signatures for the application traffic you want the FortiGate unit to detect. Configure each entry to allow or pass the traffic, and optionally log the traffic.
3. Enable UTM and application control in a firewall policy and select the application control list.

Creating an application control list

You need to create an application control list before you can enable application control.

To create an application control list

1. Go to UTM > Application Control > Application Control List.
2. Select Create New.
3. In the Name field, enter the name of the new application control list.
4. Optionally, you may also enter a comment.
5. Select OK.

The application control list is created and the list configuration window appears. A newly created application control list is empty. Without applications, the application control list will have no effect.

Adding applications to an application control list

Once you have created an application control list, you need to define the applications that you want to control.

To add applications to an application control list

1. Go to UTM > Application Control > Application Control List.
2. Select an application control list and choose Edit.
3. Select Create New.
4. Using the Category selection, choose the type of application you want to add. For example, if you want to add Facebook chat, choose im.

The Category selection displays only the options available in the Application selection. If you want to see all the applications listed, leave Category set to All Categories.
5 Using the Application selection, choose the application you want to add.
   The application available to you will be limited to those in the category you selected. If you want to include all the applications in a category, leave Application set to All Applications.

6 Select the Action the FortiGate unit will take when it detects network traffic from the application:
   - Block will stop all traffic from the application.
   - Pass allows the application traffic to flow normally.
   If you set the action to Pass, you have the option of enabling traffic shaping for the application or applications specified in this application list entry. For more information about application control traffic shaping, see "Application traffic shaping" on page 160.

7 Enable Session TTL to specify a time-to-live value for the session, in seconds. If this option is not enabled, the TTL defaults to the setting of the CLI command config system session-ttl.

8 Select Enable Logging to have the FortiGate unit log the occurrence and action taken when traffic from the application is detected.

9 Select Enable Packet Log to have the FortiGate unit save the packets that application control used to determine the traffic came from the application.

10 Some applications have additional options:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM Options (for example AIM)</td>
<td></td>
</tr>
<tr>
<td>Block Login</td>
<td>Select to prevent users from logging in to the selected IM system.</td>
</tr>
<tr>
<td>Block File Transfers</td>
<td>Select to prevent the sending and receiving of files using the selected IM system.</td>
</tr>
<tr>
<td>Block Audio</td>
<td>Select to prevent audio communication using the selected IM system.</td>
</tr>
<tr>
<td>Inspect Non-standard Port</td>
<td>Select to allow the FortiGate unit to examine nonstandard ports for the IM client traffic.</td>
</tr>
<tr>
<td>Display DLP meta-information on the system dashboard</td>
<td>Select to include meta-information detected for the IM system on the FortiGate unit dashboard.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Some traffic types include a command option. These include FTP.Command, NNTP.Command, POP3.Command, and SMTP.Command. Specify a command that appears in the traffic that you want to block or pass.</td>
</tr>
<tr>
<td></td>
<td>For example, enter GET as a command in the FTP.Command application to have the FortiGate unit examine FTP traffic for the GET command. Multiple commands can be entered.</td>
</tr>
<tr>
<td>Method</td>
<td>A method option is available for HTTP, RTSP, and SIP protocols. Specify a method that appears in the traffic that you want to block or pass.</td>
</tr>
<tr>
<td></td>
<td>For example, enter POST as a method in the HTTP.Method application to have the FortiGate unit examine HTTP traffic for the POST method. Multiple methods can be entered.</td>
</tr>
<tr>
<td>Program Number</td>
<td>Enter the program number appearing in Sun Remote Procedure Calls (RPC) that you want to block or pass. Multiple program numbers can be entered.</td>
</tr>
<tr>
<td>UUID</td>
<td>Enter the UUID appearing in Microsoft Remote Procedure Calls (MSRPC) that you want to block or pass. Multiple UUIDs can be entered.</td>
</tr>
</tbody>
</table>
Understanding the default application control lists

A number of default application control lists are provided with your FortiGate unit. You can use these as provided, or modify them as required.

Caution: Before using the default application control lists, examine them closely to ensure you understand how they will affect the traffic on your network.

<table>
<thead>
<tr>
<th>List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>block-p2p</td>
<td>This list blocks the applications in the P2P category and allow all other application traffic.</td>
</tr>
<tr>
<td>monitor-all</td>
<td>This list allows all application traffic and enables the application control monitoring for all traffic. Only FortiGate units with a hard drive support application monitoring.</td>
</tr>
<tr>
<td>monitor-p2p-and-media</td>
<td>This list allows all application traffic, and enables the application control monitoring for the applications in the P2P and media categories. Only FortiGate units with a hard drive support application monitoring.</td>
</tr>
</tbody>
</table>

Application traffic shaping

You can apply traffic shaping for application list entries you configure to pass. Traffic shaping enables you to limit or guarantee the bandwidth available to the application or applications specified in an application list entry. You can also prioritize traffic by using traffic shaping.

When the action is set to Pass, two options appear: Traffic Shaping and Reverse Direction Traffic Shaping. When enabled, you can select traffic shapers configured in Firewall > Traffic Shaper.

You can create or edit traffic shapers by going to Firewall > Traffic Shaper > Shared. Per-IP traffic shapers are not available for use in application control traffic shaping.

For more information about traffic shaping, see the Traffic Shaping User Guide.

Enabling application control traffic shaping

Enabling traffic shaping in an application control list entry involves selecting the required shaper. You can create or edit shapers in Firewall > Traffic Shaper > Shared.

To enable traffic shaping

1. Go to UTM > Application Control > Application Control List.
2. Select the application control list and choose Edit.
3. Select the application control list entry and choose Edit.
4. Select Traffic Shaping and choose the required traffic shaper from the list.
   - If the action is set to Block, the traffic shaping option is not available. Only allowed traffic can be shaped.
5. Select Reverse Direction Traffic Shaping and choose the required traffic shaper from the list if traffic flowing in the opposite direction also requires shaping.
6. Select OK.

Any firewall policy with this application control list selected will shape application traffic according to the applications specified in the list entry and the shaper configuration.
Reverse direction traffic shaping

To enable traffic shaping, you must set the action to Pass, enable Traffic Shaping and then choose the shaper. This will apply the shaper configuration to the application traffic specified in the entry, but only in the direction as specified in the firewall policy in which the application control list is selected. To shape traffic travelling in the opposite direction, enable Reverse Direction Traffic Shaper.

For example, if you find that your network bandwidth is being overwhelmed by streaming HTTP video, one solution is to limit the bandwidth by applying a traffic shaper to an application control entry that allows the HTTP:Video application. Your users access the Web using a firewall policy that allows HTTP traffic from the internal interface to the external interface. Firewall policies are required to initiate communication so even though web sites respond to requests, a policy to allow traffic from the external interface to the internal interface is not required for your users to access the Web. The internal to external policy allows them to open communication sessions to web servers, and the external servers can reply using the existing session.

If you enable Traffic Shaping and select the shaper in an application control list specified in the firewall policy, the problem will continue. The reason is the shaper you select for Traffic Shaping is applied only to the application traffic moving in the direction stated in the firewall policy. In this case, that is from the internal interface to the external interface. The firewall policy allows the user to visit the web site and start the video, but the video itself is streamed from the server to the user, or from the external interface to the internal interface. This is the reverse of the direction specified in the firewall policy. To solve the problem, you must enable Reverse Direction Traffic Shaping and select the shaper.

Shaper re-use

Shapers are created independently of firewall policies and application control lists so you are free to reuse the same shapers in multiple list entries and policies. Shared shapers can be configured to apply separately to each firewall policy or across all policies. This means that if a shaper is configured to guaranteed 1000 KB/s bandwidth, each firewall policy using the shaper will have its own 1000 KB/s reserved, or all of the policies using the shaper will share a pool if 1000 KB/s, depending on how it is configured.

The same thing happens when a shaper is used in application control list entries. If an application control list using a shaper is applied to two separate policies, how the bandwidth is limited or guaranteed depends on whether the shaper is set to apply separately to each policy or across all policies. In fact, if a shaper is applied directly to one firewall policy, and it is also included in an application control list that is applied to another firewall policy, the same issue occurs. How the bandwidth is limited or guaranteed depends on the shaper configuration.

If a shaper is used more than once within a single application control list, all of the applications using the shaper are restricted to the maximum bandwidth or share the same guaranteed bandwidth.

For example, you want to limit the bandwidth used by Skype and Facebook chat to no more than 100 KB/s. Create a shaper, enable Maximum Bandwidth, and enter 100. Then create an application control list with and entry for Skype and another entry for Facebook chat. Apply the shaper to each entry and select the application control list in the firewall policy that allows your users to access both services.

This configuration uses the same shaper for each entry, so Skype and Facebook chat traffic are limited to no more than 100 KB/s in total. That is, traffic from both applications is added and the total is limited to 100 KB/s. If you want to limit Skype traffic to 100 KB/s and Facebook chat traffic to 100 KB/s, you must use separate shapers for each application control entry.
Application control monitor

The application monitor enables you to gain an insight into the applications generating traffic on your network. When monitor is enabled in an application control list entry and the list is selected in a firewall policy, all the detected traffic required to populate the selected charts is logged to the SQL database on the FortiGate unit hard drive. The charts are available for display in the executive summary section of the log and report menu.

Note: Because the application monitor relies on a SQL database, the feature is available only on FortiGate units with an internal hard drive.

While the monitor charts are similar to the top application usage dashboard widget, it offers several advantages. The widget data is stored in memory so when you restart the FortiGate unit, the data is cleared. Application monitor data is stored on the hard drive and restarting the system does not affect old monitor data.

Application monitor allows you to choose to compile data for any or all of three charts: top ten applications by bandwidth use, top ten media users by bandwidth, and top ten P2P users by bandwidth. Further, there is a chart of each type for the traffic handled by each firewall policy with application monitor enabled. The top application usage dashboard widget shows only the bandwidth used by the top applications since the last system restart.

Enabling application control monitor

Once you have configured and enabled application control, you can enable application monitor. There are three steps, as detailed below: enabling application monitor in an application control list, selecting the charts in the firewall policy, and displaying the charts in the Executive Summary.

To enable application control monitor in an application control list

1. Go to UTM > Application Control > Application Control List.
2. Select the application control list and choose Edit.
3. Select Enable Monitoring.
4. Select OK.

With application control monitoring enabled, the FortiGate unit begins collecting data for the applications specified in the application control list from the traffic handled by all policies using the list. If you require monitoring in other application control lists, follow the same procedure to enable it in each list.

To configure the charts for which data is collected

1. Go to Firewall > Policy > Policy.
2. Select the firewall policy in which the application control list is selected and choose Edit. Note the firewall policy ID number.
3. Under UTM, the Enable Application Control selection has three new options, one for each chart type. Select one or more chart types.
4. Select OK.
5. If you have the application control list specified in multiple firewall policies, repeat this procedure for each policy.

For more information about executive summary charts, see the Logging and Reporting User Guide.
To display the application monitor charts
2. Select Add Widget.
3. Select the chart you want from the Widgets list.
   The three application monitor charts correspond to the three chart selections in the firewall policy. They are listed in the list as:
   - top10-application-bw-X-0
   - top10-media-user-X-0
   - top10-p2p-user-bw-X-0
   If you have application monitor enabled in multiple firewall policies, one chart of each type per policy will be available for you to choose. The ‘X’ in the chart name is the firewall policy number.
4. Select a Daily or Weekly schedule. The chart will display the data collected from only the current day or current week, depending on the setting. The chart will be reset daily on the hour specified, or weekly on the hour and day specified.
5. Select OK.

Application control packet logging
Packet logging saves the network packets that application control identifies application traffic with. These packets can be used to trouble-shoot false positives or for forensic investigation. The FortiGate unit saves the logged packets to the attack log, wherever the logs are configured to be stored, whether memory, internal hard drive, a FortiAnalyzer unit, or the FortiGuard Analysis and Management Service.

You can enable packet logging in individual application list entries. Use caution in enabling packet logging. Application control list entries configured with few restrictions can contain hundreds of applications, potentially resulting in a flood of saved packets. This would take up a great deal of space, require time to sort through, and consume considerable system resources to process. Packet logging is designed as a focused diagnostic tool and is best used with a narrow scope.

Caution: Although logging to multiple FortiAnalyzer units is supported, packet logs are not sent to the secondary and tertiary FortiAnalyzer units. Only the primary unit receives packet logs.

To enable application control packet logging
1. Create an entry in an application control list. For more information, see “Adding applications to an application control list” on page 158.
2. Before saving the entry, select Enable Packet Log.
3. Select the application control list in the firewall policy that allows the network traffic the FortiGate unit will examine for the application or applications.

For information on viewing and saving logged packets, see “Viewing and saving logged packets” on page 31.
Application considerations

Some applications behave differently from most others. You should be aware of these differences before using application control to regulate their use.

IM applications

Application control regulates most instant messaging applications by preventing or allowing user access to the service. Selecting Block Login will not disconnect users who are logged in when the change is made. Once they log themselves out, however, they will not be able to log in again.

Skype

Based on the NAT firewall type, Skype takes advantage of several NAT firewall traversal methods, such as STUN (Simple Traversal of UDP through NAT), ICE (Interactive Connectivity Establishment) and TURN (Traversal Using Relay NAT), to make the connection.

The Skype client may try to log in with either UDP or TCP, on different ports, especially well-known service ports, such as HTTP (80) and HTTPS (443), because these ports are normally allowed in firewall settings. A client who has previously logged in successfully could start with the known good approach, then fall back on another approach if the known one fails.

The Skype client could also employ Connection Relay. This means if a reachable host is already connected to the Skype network, other clients can connect through this host. This makes any connected host not only a client but also a relay server.

Application control examples

Blocking all instant messaging

Instant messaging use is not permitted at the Example Corporation. Application control helps enforce this policy.

First you will create an application control list with a single entry that includes all instant messaging applications. You will set the list action to block.

To create the application control list

1. Go to UTM > Application Control > Application Control List.
2. Select Create New.
3. In the Name field, enter no IM for the application control list name.
4. Select OK.
5. Select Create New to add a new list entry.
6. For Category, select im.
7. For Action, select Block.
8. Select OK to save the new list entry.
9. Select OK to save the list.

Next you will enable application control and select the list.
To enable application control and select the application control list

1. Go to Firewall > Policy > Policy.
2. Select the firewall policy that allows the network users to access the Internet and choose Edit.
3. Enable UTM.
4. Select Enable Application Control.
5. Select the no IM application control list.
6. Select OK.

No IM use will be allowed by the firewall policy. If other firewall policies handle traffic that users could use for IM, enable application control with the no IM list for those as well.

Allowing only software updates

Some departments at Example Corporation do not require access to the Internet to perform their duties. Management therefore decided to block their Internet access. Software updates quickly became an issue because automatic updates will not function without Internet access and manual application of updates is time-consuming.

The solution is configuring application control to allow only automatic software updates to access the Internet.

To create an application control list — web-based manager

1. Go to UTM > Application Control > Application Control List.
2. Select Create New.
3. In the Name field, enter Updates_Only as the application control list name.
4. Select OK.
5. Select Create New.
6. Select update from the Category list.
7. Select Pass from the Action list.
8. Select OK to save the entry.

This application list entry will allow all software update application traffic.

9. Select the All Other Known Applications entry.
10. Select Edit.
11. Select Block from the Action list.
12. Select OK.

This application list entry will block all traffic from recognized applications that are not specified in this application control list.

13. Select the All Other Unknown Applications entry.
15. Select Block from the Action list.
16. Select OK.

This application list entry will block all traffic from applications that are not recognized by the application control feature.

17. Select OK.
18. Select OK to save the application control list.
To create an application control list — CLI

```bash
config application list
  edit Updates_Only
    config entries
      edit 1
        set category 17
        set action pass
      end
      set other-application-action block
      set unknown-application-action block
    end
end
```

Selecting the application control list in a firewall policy

An application control list directs the FortiGate unit to scan network traffic only when it is selected in a firewall policy. When an application control list is selected in a firewall policy, its settings are applied to all the traffic the firewall policy handles.

**To select the application control list in a firewall policy — web-based manager**

1. Go to **Firewall > Policy > Policy**.
2. Select a policy.
3. Select the **Edit** icon.
4. Enable **UTM**.
5. Select the **Enable Application Control** option.
6. Select the **Updates_only** list.
7. Select **default** from the **Protocol Options** list.
   - Application control can not be enabled without selecting a protocol options profile. A default profile is provided.
8. Select **OK**.

**To select the application control list in a firewall policy — CLI**

```bash
config firewall policy
  edit 1
    set utm-status enable
    set profile-protocol-options default
    set application-list Updates_Only
  end
end
```

Traffic handled by the firewall policy you modified will be scanned for application traffic. Software updates are permitted and all other application traffic is blocked.
DoS policy

Denial of Service (DoS) policies are primarily used to apply DoS sensors to network traffic based on the FortiGate interface it is entering as well as the source and destination addresses. DoS sensors are a traffic anomaly detection feature to identify network traffic that does not fit known or common traffic patterns and behavior. A common example of anomalous traffic is the denial of service attack. A denial of service 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 that legitimate users can no longer use it.

This section describes how to create and configure DoS sensors and policies to protect the publicly accessible servers on your network.

The following topics are included in this section:

- DoS policy concepts
- Enable DoS
- DoS example

DoS policy concepts

DoS policies are similar to firewall policies except that instead of defining the way traffic is allowed to flow, they keep track of certain traffic patterns and attributes and will stop traffic displaying those attributes. Further, DoS policies affect only incoming traffic on a single interface. You can further limit a DoS policy by source address, destination address, and service.

DoS policies examine network traffic very early in the sequence of protective measures the FortiGate unit deploys to protect your network. Because of this early detection, DoS policies are a very efficient defense that uses few resources. Denial of service attacks, for example, are detected and its packets dropped before requiring firewall policy look-ups, antivirus scans, and other protective but resource-intensive operations. For more information about DoS attacks, see "Defending against DoS attacks" on page 39.

Enable DoS

A DoS policy examines network traffic arriving at an interface for anomalous patterns usually indicating an attack. Enable DoS sensors to protect your FortiGate unit from attack. To apply a DoS policy, you must follow the steps below in sequence:

1. Create a DoS sensor.
2. Create a DoS policy
3. Apply the DoS sensor to the DoS policy.

Creating and configuring a DoS sensor

Because an improperly configured DoS sensor can interfere with network traffic, no DoS sensors are present on a factory default FortiGate unit. You must create your own and then enable them 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.
To create a DoS sensor
1. Go to UTM > Intrusion Protection > DoS Sensor.
2. Select Create New.
3. In the Name field, enter the name of the DoS sensor.
4. Optionally, enter a description of the DoS sensor in the Comment field.
5. Select OK.

The DoS sensor is created and the sensor configuration window appears. However, a newly created DoS sensor contains default values which may not be appropriate for your network. You can adjust these values by configuring the DoS sensor thresholds.

To configure a DoS sensor
1. Go to UTM > Intrusion Protection > DoS Sensor.
2. Select the DoS sensor you want to configure and choose Edit.
3. The DoS sensor configuration window appears.

The Anomalies Configuration table lists 12 types of network 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 of new TCP connections, including retransmission, to one destination IP address exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.</td>
</tr>
<tr>
<td>tcp_port_scan</td>
<td>If the SYN packet rate of new TCP connections, including retransmission, 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>tcp_src_session</td>
<td>If the number of concurrent TCP connections from one source IP address 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 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 threshold value, the action is executed. 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 exceeds the configured threshold value, the action is executed. 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 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 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 exceeds the configured threshold value, the action is executed. The threshold is expressed in packets per second.</td>
</tr>
<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>
</tbody>
</table>
Select Enable to have the FortiGate unit examine traffic for the anomaly.

5 Select Logging to create an entry in the attack log if the anomaly is detected.

6 Select an Action for the anomaly. By default, the action is Pass, which allows the traffic containing the anomaly to pass uninterrupted. If set to Block, the anomalous traffic is blocked and will not flow through the FortiGate unit.

With a Fortinet security processing module installed, FortiGate units that support these modules offer a third action for the tcp_syn_flood threshold. In addition to Block and Pass, you can choose to Proxy connect attempts when their volume exceeds 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 FortiGate unit will intercept incoming SYN packets with a hardware accelerated SYN proxy to determine whether the connection attempts are legitimate or a SYN flood attack. Legitimate connections are allowed while an attack is blocked.

Note: Because DoS sensors are configured before being applied to an interface, you can assign a DoS sensor with the Proxy action to an interface that does not have hardware SYN proxy support. In this circumstance, the Proxy action is invalid and a Pass action will be applied.

7 Set the Threshold value for the anomaly. See the table in step 3 for details about the threshold values for each anomaly.

8 Select OK.

Creating a DoS policy

DoS policies examine network traffic entering an interface. The DoS sensor specified in the DoS policy allows you to limit certain anomalous traffic to protect against attacks.

To create a DoS policy

1 Go to Firewall > Policy > DoS Policy and select Create New.

2 For Source Interface/Zone, select the interface on which the DoS policy will examine incoming traffic.

3 For Source Address, select the address or address group that defines the source addresses of the traffic the DoS policy will examine. Network traffic from addresses not included in the selected address group is ignored by this DoS policy.

4 For Destination Address, select the address or address group that defines the destination addresses of the traffic the DoS policy will examine. Network traffic to addresses not included in the selected address group is ignored by this DoS policy.

5 For Service, select the type of network traffic the DoS policy will examine. Protocols not included in the selected service or service group are ignored by this DoS policy.

6 Select the DoS Sensor check box and choose the required sensor from the list.

7 Select OK.
**Apply an IPS sensor to a DoS policy**

Although IPS sensors are usually applied to firewall policies, you can also apply them to DoS policies by using CLI commands. There are two reasons you might want to apply an IPS sensor to a DoS policy:

- If you want to have all traffic coming into one FortiGate unit interface checked for the signatures in an IPS sensor, it is simpler to apply the IPS sensor once to a DoS policy. In a complex configuration, there could be many policies controlling the traffic coming in on a single interface.

- The operations in a DoS policy occur much earlier in the sequence of operations performed on incoming traffic. This means that IPS examination of traffic occurs much sooner if the IPS sensor is applied to a DoS policy. Fewer system resources are used because signatures set to block traffic will take effect before firewall policy checking and all of the scans specified in the firewall policy.

The CLI command for configuring DoS policies is `config firewall interface-policy`. The following command syntax shows how to add an example IPS sensor called `all_default_pass` to a DoS policy with policy ID 5 that was previously added from the web-based manager.

```
config firewall interface-policy
edit 5
set ips-sensor-status enable
set ips-sensor all_default_pass
end
```

**DoS example**

The Example.com corporation installed a web server and connected it to Port5 on its FortiGate unit. To protect against denial of service attacks, you will configure and apply a DoS sensor to protect the web server.

**To create the DoS sensor**

1. Go to **UTM > Intrusion Protection > DoS Sensor**.
2. Select **Create New**.
3. Enter **Web Server** in the **Name** field.
4. In the **Anomalies Configuration** table, select the **Enable** check box in the table heading. This enables all the anomalies with a single selection.
5. Select **OK** to save the new DoS policy.

As suggested in “Defending against DoS attacks” on page 39, the IT administrators will run the DoS policy with logging enabled and the anomaly actions set to **Pass** until they determine the correct threshold values for each anomaly.

**To create a DoS policy**

1. Go to **Firewall > Policy > DoS Policy**.
2. Select **Create New**.
3. In the **Source Interface/Zone** field, select **Port1** which is the interface connected to the Internet.
4. In the **Source Address** field, select **all**.
5 In the *Destination Address* field, select *all*.
   If there were more than one publicly accessible server connected to the FortiGate unit,
   you would specify the address of the web server in this field.
6 In the *Service* field, select *ANY*.
7 Select the *DoS Sensor* check box and choose *Web Server* from the list.
8 Select *OK* to save the DoS policy.

The DoS policy will monitor all network traffic entering Port1 and log the violations if the
thresholds in the *Web Server* DoS sensor are exceeded.
Sniffer policy

Sniffer policies are used to configure a physical interface on the FortiGate unit as a one-arm intrusion detection system (IDS). Traffic sent to the interface is examined for matches to the configured IPS sensor and application control list. Matches are logged and then all received traffic is dropped. Sniffing only reports on attacks. It does not deny or otherwise influence traffic.

This section describes how to configure your network topology to use the FortiGate unit as a one-arm intrusion detection system. It also describes how to configure and enable a sniffer policy.

The following topics are included in this section:

- Sniffer policy concepts
- Before you begin
- Enable one-arm sniffing
- Sniffer example

Sniffer policy concepts

Using the one-arm intrusion detection system (IDS), you can configure a FortiGate unit to operate as an IDS appliance by sniffing network traffic for attacks without actually processing the packets.

To configure one-arm IDS, you enable sniffer mode on a FortiGate interface and connect the interface to a hub or to the SPAN port of a switch that is processing network traffic. Then you add DoS policies for that FortiGate interface. Each policy can include a DoS sensor, an IPS sensor, and an application control list to detect attacks and application traffic in the network traffic that the FortiGate interface receives from the hub or switch SPAN port.

The sniffer policy list

The sniffer policy list shows all of the sniffer policies you have created. The policies are listed by sniffer interface. This is important because multiple sniffer policies can be applied to sniffer interfaces. Traffic entering a sniffer interface is checked against the sniffer policies for matching source and destination addresses and for service. This check against the policies occurs in listed order, from top to bottom. The first sniffer policy matching all three attributes then examines the traffic. Once a policy matches the attributes, checks for policy matches stop. If no sniffer policies match, the traffic is dropped without being examined.

Once a policy match is detected, the matching policy compares the traffic to the contents of the DoS sensor, IPS sensor, and application list specified in the policy. If any matches are detected, the FortiGate unit creates an entry in the log of the matching sensor/list. If the same traffic matches multiple sensors/lists, it is logged for each match. When this comparison is complete, the network traffic is dropped.

Figure 12 illustrates this process.
Before you begin

Traffic entering an interface in sniffer mode is examined for DoS sensor violations, IPS sensor matches, and application control matches. After these checks, all network traffic is dropped. To avoid losing data, you must direct a copy of the network traffic to the FortiGate unit interface configured to sniff packets.

The easiest way to do this is to either use a hub or a switch with a SPAN port. A hub is the easiest solution to implement but carries a downside. Connecting the FortiGate unit interface configured with the sniffer policy to a hub will deliver all traffic passing through the hub to the interface. However, if the network carries a heavy traffic load, the hub could slow the network because every hub interface sends out all the traffic the hub received on every interface.

A better solution is a switch with a SPAN port. Network switches receive traffic on all interfaces but they only send traffic out on the interface connected to the destination. Network slowdowns are less common when using switches instead of hubs.

Figure 12: How the intrusion detection system uses sniffer policies to examine traffic
Connecting the sniffer interface to a regular switch interface will not work because no traffic is addressed to the sniffer interface. A SPAN port is a special-purpose interface that mirrors all the traffic the switch receives. Traffic is handled normally on every other switch interface, but the SPAN port sends a copy of everything. If you connect your FortiGate unit sniffer interface to the switch SPAN port, all the network traffic will be examined without any being lost because of the examination.

Figure 13: A network configured for intrusion detection using a sniffer policy

Enable one-arm sniffing

Sniffer policies examine network traffic for anomalous patterns that usually indicate an attack. Since all traffic entering a sniffer interface is dropped, you need to first add a switch or hub to your network as described in "Before you begin" on page 174. The following steps are based on the assumption that you have added the switch or hub.

General configuration steps

The interface first must be designated as the sniffer interface, then the sniffer policy can be configured to use the sniffer interface.

1. Add a switch or hub to your network as described in "Before you begin" on page 174. This configuration will send a copy of your network traffic to the sniffer interface.

   Caution: When an interface is configured as a sniffer interface, all traffic received by the interface is dropped after being examined by the sniffer policy.

2. Designate a physical interface as a sniffer interface.
3. Create a sniffer policy that specifies the sniffer interface.
4. Specify a DoS sensor, IPS sensor, application control list, or any combination of the three to define the traffic you want logged.
Designating a sniffer interface

An interface must be designated as a sniffer interface before it can be used with a sniffer policy. Once an interface is designated as a sniffer interface, it functions differently from a regular network interface in two ways:

- A sniffer mode interface accepts all traffic and drops it. If a sniffer policy is configured to use the sniffer interface, traffic matching the attributes configured in the policy will be examined before it is dropped. No traffic entering a sniffer mode interface will exit the FortiGate unit from any interface.

- A sniffer mode interface will be the only available selection in sniffer policies. The sniffer interface will not appear in firewall policies, routing tables, or anywhere else interfaces can be selected.

Designating a sniffer interface

1. Go to System > Network > Interface.
2. Select the interface.
3. Select the Edit icon.
4. Select the Enable one-arm sniffer check box.
   If the check box is not available, the interface is in use. Ensure that the interface is not selected in any firewall policies, routes, virtual IPs or other features in which a physical interface is specified.
5. Select OK.

Caution: When an interface is configured as a sniffer interface, all traffic received by the interface is dropped after being examined by the sniffer policy.

Creating a sniffer policy

Sniffer interfaces accept all traffic. To examine the traffic before it is dropped, a sniffer policy is required.

To create a sniffer policy

1. Go to Firewall > Policy > Sniffer Policy and select Create New.
2. For Source Interface/Zone, select the interface configured as the sniffer interface. If no interfaces are available for selection, no interfaces have been defined as sniffer interfaces. For more information, see “Designating a sniffer interface” on page 176.
3. For Source Address, select the address or address group that defines the source addresses of the traffic the sniffer policy will examine. Network traffic from addresses not included in the selected address group is ignored by this sniffer policy.
4. For Destination Address, select the address or address group that defines the destination addresses of the traffic the sniffer policy will examine. Network traffic to addresses not included in the selected address group is ignored by this sniffer policy.
5. For Service, select the type of network traffic the sniffer policy will examine. Protocols not included in the selected service or service group are ignored by this sniffer policy.
6. To have the sniffer policy log violations specified in a DoS sensor, select the DoS Sensor check box and choose the sensor from the list.
7. To have the sniffer policy log signatures appearing in an IPS sensor, select the IPS Sensor check box and choose the sensor from the list.
8 To have the sniffer policy log traffic from applications specified in an application control list, select the **Application Black/White List** check box and choose the application control list.

9 Select **OK**.

DoS sensors, IPS sensors, and application control lists all allow you to choose actions and log traffic. When included in a sniffer sensor, these settings are ignored. Actions in these other settings do not apply, and all matches are logged regardless of the logging setting.

### Sniffer example

**An IDS sniffer configuration**

The Example.com Corporation uses a pair of FortiGate-620B units to secure the head office network. To monitor network attacks and create complete log records of them, the network administrator has received approval to install a FortiGate-82C to record all IPS signature matches in incoming and outgoing network traffic using a sniffer policy. This example details the set-up and execution of this network configuration.

Although this example uses a separate FortiGate unit for sniffer-mode operation, the sniffer traffic can be sent to the FortiGate unit protecting the network. The switch must still be configured to create a copy of the data because the sniffer interface drops all incoming traffic. In this case, the administrator requested a FortiGate-82C for this purpose because sniffer-mode operation is resource intensive, and using a separate FortiGate unit frees the FortiGate-620B cluster from this task. The FortiGate-82C unit also has four internal hard drives, making it ideal for storing large log files.

**Configuring the network**

Connect the Port1 interface of the FortiGate-82C to the Port8 interface of the switch. You must configure your network to deliver a copy of the traffic to be examined to the sniffer interface because all network traffic entering a sniffer interface is dropped after examination.

Since the corporate network uses a pair of FortiGate units in an HA cluster, a switch is already in place connecting the Internet to Port1 of both FortiGate units.

**Figure 14: Switch configuration**
The company Internet feed is connected to Port1 of the switch. The FortiGate units are connected to Port2 and Port3 of the switch. Since they are configured as an HA cluster, they must both have access to the Internet in the event of a failure.

To allow a FortiGate unit sniffer interface to examine the network traffic, the switch must be configured to create a copy of all network traffic entering or leaving Port2 and Port3 and send it out Port8. When configured this way, the switch port sending the duplicate traffic is called a mirror port or a SPAN port.

Consult the switch documentation for instructions on how to configure a SPAN port.

**Note:** The traffic between Port1 and Port2/Port3 is not modified or diverted in any way by the creation of a SPAN port. The traffic is duplicated with the copy being sent out of the SPAN port.

**Configuring the FortiGate sniffer interface**

No sniffer interfaces are included in the default configuration of any FortiGate unit. A copy of all of the network traffic is being sent to Port1 of the FortiGate-82C so you must configure Port1 as a sniffer-mode interface.

**Caution:** All network traffic entering a sniffer-mode interface is dropped after examination and logging according to the configured sniffer policy.

**To configure the sniffer mode interface — web-based manager**

1. Log in to the FortiGate-82C web-based manager.
2. Go to **System > Network > Interface**.
3. Select the Port1 interface.
4. Select **Edit**.
5. Select **Enable one-arm sniffer**.
6. Select **OK**.

**To configure the sniffer mode interface — CLI**

```
config system interface
  edit port1
    set ips-sniffer-mode enable
  end
```

**Creating an IPS sensor**

A sniffer policy allows you to select an IPS sensor, a DOS sensor, and an application control list. Any conditions these sensors and list are configured to detect and log are saved to the appropriate log.

For this example, create an IPS sensor that detects and logs the occurrence of all the predefined IPS signatures.

**To create an IPS sensor — web-based manager**

1. Go to **UTM > Intrusion Protection > IPS Sensor**.
2. Select **Create New**.
3. In the **Name** field, enter **IPS_sniffer**.
4. In the **Comments** field, enter **IPS sensor for use in the sniffer policy**.
In the Filters section, select Create New.

In the name field, enter All signatures, logged.

For the Logging setting under Signatures Settings, select Enable all.

Select OK to save the filter.

Ensure Enable Logging is selected in the sensor.

Select OK to save the IPS sensor.

To create an IPS sensor — CLI

```
config ips sensor
  edit IPS_sniffer
    set comment "IPS sensor for use in the sniffer policy."
  config filter
    edit "All signatures, logged"
      set log enable
  end
end
```

Creating the sniffer policy

The sniffer policy allows us to choose

To create the sniffer policy — web-based manager

1. Go to Firewall > Policy > Sniffer Policy.
2. Select Create New.
3. Select Port1 for the Source Interface/Zone.
4. Enable IPS Sensor and select the IPS_sniffer sensor.
5. Select OK to save the sniffer policy.

To create the sniffer policy — web-based manager

```
config firewall sniff-interface-policy
  edit 0
    set interface port1
    set srcaddr all
    set dstaddr all
    set service ANY
    set ips-sensor-status enable
    set ips-sensor IPS_sniffer
  end
```

With this configuration, all traffic entering the sniffer port is checked for matching signatures. Matches are logged and the traffic is dropped.

To examine the network traffic for more issues, you can create a DoS sensor and select it in the sniffer policy to log traffic anomalies. You can also create an application list with the specific application you’d like to check for and select it in the sniffer policy.
Index

A
allow
pattern, 59
anomaly protection
DoS, 24
antispan, see email filtering and FortiGuard, AntiSpam
antivirus, 47
archive scan depth, 55
change default database, 53
concepts, 47
databases, 50
enabling scanning, 52
example, 61
file filtering, 23
flow-based scanning, 48
FortiAnalyzer, 23
HTTPS, IMAPS, POP3S, SMTPS, 29
maximum file size, 55
override default database, 53
proxy-based scanning, 47
scan buffer size, 54
scanning order, 48
antivirus quarantine
HTTPS, IMAPS, POP3S, SMTPS, 30
application control, 25
monitor, 162
packet logging, 163
application monitor, 162
archive antivirus scan depth, 55
archiving
DLP, 153
B
black list, 24
block
pattern, 59
buffer size
IPS, 98
C
CA certificate, 28
certificate
key size, 28
SSL, 28
certification, 21
CLI syntax conventions, 17
comments, documentation, 21
concepts
antivirus, 47
web filtering, 24
conserve mode, 26
content scanning
SSL, 27
conventions, 13
Cross-Site Scripting
protection from, 19
custom signature
adding, 87
customer service, 21
D
data leak prevention (DLP), see DLP
deep scan, 29
DLP, 143
archiving, 153
default rules, 148
default sensors, 152
NAC quarantine logging, 150
DLP archive
displaying on dashboard, 31
HTTPS, IMAPS, POP3S, SMTPS, 31
document conventions
CLI syntax, 17
documentation, 21
commenting on, 21
conventions, 13
Fortinet, 21
DoS
anomaly protection, 24
E
EICAR, 61
email filtering
IMAPS, POP3S, SMTPS, 30
email filtering, see also FortiGuard, AntiSpam, 24
engine algorithm
IPS, 97
engine count
IPS, 97
F
fail-open
IPS, 98
FAQ, 21
file filtering, 59
antivirus, 23
enabling, 60
general configuration steps, 59
file pattern, 48, 51, 59
creating, 60
file quarantine
configuring, 57
general configuration steps, 57
file size, 48, 51
file type, 48, 51, 59
creating, 60
filter
IPS, 85
firewall policy, 54
FortiAnalyzer
antivirus, 23
quarantine, 57
FortiGate documentation
commenting on, 21
FortiGate-ASM-S08 module, 57
FortiGate-ASM-SAS module, 57
FortiGuard
AntiSpam, 24
Antivirus, 20, 52, 57
services, 20
Web Filtering, 24, 30
HTTPS, 30
FortiGuard Center, 52
FortiGuard Web Filter quota, 134
FortiGuard, Distribution Network, 51
Fortinet
Knowledge Center, 21
Technical Documentation, 21
Technical Documentation, conventions, 13
Technical Support, 21
Technical Support, registering with, 20
Technical Support, web site, 20
Training Services, 21
Fortinet customer service, 21
Fortinet documentation, 21
Fortinet Knowledge Center, 21

G
general configuration steps
file filtering, 59
file quarantine, 57
glossary, 21
grayware, 48, 51
scanning, 61

H
HA
IPS processing, 96
heuristics, 48, 51
how-to, 21
HTTPS
antivirus, 29
antivirus quarantine, 30
data leak prevention, 30
DLP archive, 31
FortiGuard Web Filtering, 30
protocol recognition, 29
web filtering, 30

I
IDS
one-armed IDS, 24

IM, 25
IMAPS
antivirus, 29
antivirus quarantine, 30
data leak prevention, 30
DLP archive, 31
email filtering, 30
predefined firewall services, 29
protocol recognition, 29
inspection
SSL, 27
introduction
Fortinet documentation, 21
intrusion detection system, see IDS
intrusion prevention system, see IPS
intrusion protection system, see IPS
IP address
private network, 13
IPS
adding custom signatures, 87
buffer size, 98
concepts, 83
custom signature keywords, 88
custom signature syntax, 87
engine algorithm, 97
engine count, 97
fail-open, 98
filter, 85
in an HA cluster, 96
overview, 24
packet logging, 99
protocol decoders, 98
scanning, 85
sensor, 85
session count accuracy, 98
signature override, 86

K
key size
certificate, 28
keywords
IPS custom signatures, 88
Knowledge Center, 21

M
maximum file size
antivirus, 55
monitor
application control, 162

O
one-armed IDS, 24
override
IPS signature, 86

P
P2P, 25
packet logging
  application control, 163
  IPS, 99
  settings, 31
  viewing and saving logged packets, 31
pattern, 59
  allow, 59
  block, 59
  creating, 60
POP3S
  antivirus, 29
  antivirus quarantine, 30
  data leak prevention, 30
  DLP archive, 31
  email filtering, 30
  predefined firewall services, 29
  protocol recognition, 29
predefined firewall services
  IMAPS, POP3S, SMTPS, 29
product registration, 20
protocol decoders, 98
protocol recognition
  HTTPS, IMAPS, POP3S, SMTPS, 29
Q
quarantine, 57
quota
  FortiGuard Web Filter, 134
R
regex, 32
registering
  with Fortinet Technical Support, 20
regular expressions, 32
RFC
  1918, 13
S
scan buffer size
  antivirus, 54
scanning order
  antivirus, 48
security processing modules
  configuring, 99
  example configuration, 108
  proxy statistics, 111
sensor
  IPS, 85
session count accuracy, 98
signature
  adding custom IPS signatures, 87
  signature override
    IPS, 86
SMTPS
  antivirus, 29
  antivirus quarantine, 30
  data leak prevention, 30
  DLP archive, 31
  email filtering, 30
  predefined firewall services, 29
  protocol recognition, 29
sniffer policies, 24
SSL
  antivirus, 29
  antivirus quarantine, 30
  certificate, 28
  content inspection, 27
  content scanning, 27
  data leak prevention, 30
  DLP archive, 31
  email filtering, 30
  example, 61
  FortiGuard Web Filtering, 30
  HTTPS, 30
  inspection, 27
  predefined firewall services, 29
  protocol recognition, 29
  settings, all, 29
  supported FortiGate models, 27
  web filtering, 30
syntax
  IPS custom signatures, 87
T
technical
  documentation, 21
  documentation conventions, 13
  notes, 21
  support, 21
technical support, 21
  Training Services, 21
U
Unified Threat Management, see UTM
URL filtering, 24
UTM
  overview, 23
  VDOM, 25
UTM profiles, 25
V
VDOM
  UTM, 25
virus database, 52
virus scan, 48, 51
vulnerability
  Cross-Site Scripting, 19
  XSS, 19
W
web content filtering, 24
web filter
  quota, 134
web filtering, 24
HTTPS, 30
wildcard, 59
wildcards, 32

X

XSS vulnerability
protection from, 19